MULTIPURPOSE INVISIBLE AND VISIBLE DIGITAL IMAGE WATERMARKING SCHEMES

Ph. D. THESIS

by

HIMANSHU AGARWAL

DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY ROORKEE
ROORKEE- 247 667 (INDIA)
JULY, 2014

MULTIPURPOSE INVISIBLE AND VISIBLE DIGITAL IMAGE WATERMARKING SCHEMES

A THESIS

Submitted in partial fulfilment of the requirements for the award of the degree of

DOCTOR OF PHILOSOPHY
in

MATHEMATICS

by

HIMANSHU AGARWAL

DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY ROORKEE
ROORKEE- 247 667 (INDIA)
JULY, 2014

INDIAN INSTITUTE OF TECHNOLOGY ROORKEE
ROORKEE

CANDIDATE'S DECLARATION

I hereby certify that the work which is being presented in the thesis entitled **MULTIPURPOSE INVISIBLE AND VISIBLE DIGITAL IMAGE WATERMARKING SCHEMES** in partial fulfilment of the requirements for the award of the Degree of Doctor of Philosophy and submitted in the Department of Mathematics of the Indian Institute of Technology Roorkee, Roorkee is an authentic record of my own work carried out during a period from July, 2009 to July, 2014 under the supervision of Dr. R. Balasubramanian, Associate Professor, Department of Computer Science and Engineering, Indian Institute of Technology Roorkee, Roorkee.

The matter presented in this thesis has not been submitted by me for the award of any other degree of this or any other Institute.

(HIMANSHU AGARWAL)

This is to certify that the above statement made by the candidate is correct to the best of my knowledge.

(R. Balasubramanian)
Supervisor

Date: July , 2014

The Ph.D. Viva-Voce Examination of **Mr. Himanshu Agarwal,** Research Scholar, has been held on……

Signature of Supervisor Chairman, SRC Signature of External Examiner

Head of the Department/Chairman, ODC

Abstract

Watermarking is an advanced research topic in multimedia community. It is used for various applications such as broadcast monitoring, piracy, owner identification, copyright protection, copy deterrence, proof of ownership, media authentication, fingerprint/transaction tracking, copy control, legacy enhancement, security of biometric system etc. The requirements of an efficient watermarking system depend on the application scenario. Nowadays, the main research issues in watermarking are development of new watermarking schemes, developing the testing tools for new and developed watermarking schemes, analysis of a watermarking system and broaden the usefulness of watermarking to multimedia applications.

In this thesis, we have examined the solutions of five watermarking related problems.

The first problem has been discussed in Chapter 2. Here, the digital image watermarking and biometrics have been combined to improve the owner identification/verification technology. This problem is related to broaden the watermarking application. For the solution, we have developed four watermarking schemes. Two watermarking schemes operate on discrete wavelet transform domain and rest two schemes operate on redundant discrete wavelet transform domain. One watermarking scheme in each transform domain incorporates a weighted binary coding. We have observed that the discrete wavelet transform based watermarking scheme coupled with the weighted binary coding provides the best solution for the first problem.

Both non-blind and blind watermarking schemes in the real oriented wavelet transform domain are proposed in the second problem (chapter 3). One challenge in this problem arises due to the fact that the product of the left inverse of real oriented wavelet transform followed by the real oriented wavelet transform (ROWT) is not the identity transform. A key contribution towards the solution is that we have obtained a product of left inverse of ROWT followed by the ROWT itself. This product has been used in both the proposed schemes. Further, derived mathematical properties based on the quotient-remainder-theorem have been used in the proposed blind watermarking scheme.

The third problem (Chapter 4) is to provide a solution to improve the security/integrity of a compromised biometric system. In the solution of the third problem, we have proposed a spatial domain and a discrete cosine transform based watermarking schemes. The spatial domain based watermarking scheme is blind, reversible and fragile while the discrete cosine transform based watermarking scheme is blind and robust.

The fourth problem (Chapter 5) is motivated by the fact that visible watermark is embedded at predefined positions in an image/video frame, which leads occlusion of important portion of multimedia objects by the visible watermark, for instance, TV channel logo used for television broadcasting. As a solution, we have proposed a visible watermarking technique that embeds a binary logo watermark at N non-overlapping positions in an image such that important portions of the image are not occluded.

In the last problem of the thesis (Chapter 6), we have analysed watermarking systems of binary watermarks. The analysis is based on an assumption that negative paired images provide same information, which is the basic fundamental of information theory. We have analysed watermarking systems with respect to five comparators. These five comparators are based on the normalized Hamming

similarity (NHS), the normalized correlation coefficient (NCC/NC), the mean subtracted NCC (MSNCC), symmetric NHS (SNHS, a version derived from NHS), absolute MSNCC (AMSNCC, a version derived from MSNCC). A main observation of this analysis is that SNHS and AMSNCC based comparators treat negative of watermark same as itself.

The solution of each problem has been tested against several signal distortions such as Geometric attacks, filtering, format conversion and noise addition.

Acknowledgements

I thank GOD for providing me the opportunity to pursue PhD under the supervision of Dr. R. Balasubramanian, Associate Professor in the Indian Institute of Technology (IIT) Roorkee, India. I sincerely thank to my PhD supervisor for suggesting me the problem of digital watermarking, and providing me a very rewarding research and teaching experience. It is impossible to get a supervisor better than him.

I feel privileged to express my sincere regards and gratitude to Dr. Pradeep K. Atrey, Associate Professor for providing me an outstanding research training during my six months research visit programme in the Applied Computer Science Department of the University of Winnipeg of Canada. Further, during this programme, he never made me feel that I am away from home.

My sincere thanks go out to Prof Mohan Kankanhalli, Dr. Debashis Sen (from National University of Singapore) and Dr. Ibrahim Venkat (from Universiti Sains Malaysia) with whom I have collaborated during my PhD. Their conceptual and technical insights into my thesis work are invaluable.

I would like to acknowledge all my teachers, who motivated me for quality in education, research and life. My sincere regards and gratitude must go out to Prof M. L. Mittal, Dr. D. P. Goyal, Dr. Punita Verma, Sh. Ramesh Agarwal, Sh. Harikant Yadav and Sh. Deepak Jangra.

I thank Department of Mathematics, IIT Roorkee for providing the infrastructure and all necessary facilities for my research. I am thankful to Prof R. C. Mittal, Head

of Department, Prof R. Bhargava and Prof S. P. Sharma (former HODs), Prof P. N. Agrawal, DRC chairperson, Prof T. R. Gulati and Prof G. S. Srivastava (former DRC chairpersons) for their encouragement, support and timely help. I sincerely thank to my internal supervisor Prof N. Sukavanyam and external supervisor Prof R. P. Maheshwari for their valuable feedbacks to improve the quality of this thesis. I would like to thank all staff members of the Department for their friendly behavior.

I am highly thankful to Computer Vision Graphics & Image Processing (CVGIP) Laboratory, Department of Mathematics, IIT Roorkee for the facilities that I have availed for my research work. I am thankful to all its members for their help.

I am thankful to my seniors and friends Dr. Gaurav Gupta, Dr. Sanjay Rawat, Dr. Sanoj Kumar, Dr. Asha Rani, Dr. Sanjeev Kumar, Dr. Mohit Kumar, Dr. Gaurav Bhatnagar, Dr. Manoj Kumar, Pushpendra, Amit, Manisha and many more for their constant help, support and encouragement. The friendship with my fellow researcher, Sandeep Kumar Mogha is unforgettable. I am grateful to my friends Nishant, Ankita, Vinay, Shreelatha, Kasun and Harmeet for their help, hospitality, and research discussions during my stay in Canada. I thank all research scholars of the Department of Mathematics for wonderful memories.

I acknowledge the University Grant Commission (UGC) of India, the Ministry of Human Resource Development (MHRD) of India, the IIT Roorkee of India, the Council of Scientific & Industrial Research (CSIR) of India and the Canadian Bureau for International Education (CBIE) of Canada for providing financial assistance for research during my PhD tenure.

Last, but not least, I dedicate this thesis to my parents Smt. Shashi Bala and Sh. Raj Kumar. I am thankful to my extended family for their unconditional wishes and love. Special thanks and gratitude are for my taiji Smt. Chanda Devi, tauji Sh. Kamal Prasad, didi Smt. Kusum Gupta, jijaji Sh. Lalit Gupta, Rekha bhabhiji, Ashok bhaiya, brothers Sumanshu and Paras, and friend Pooja.

Table of Contents

Abstract **i**

Acknowledgements **v**

Table of Contents **vii**

List of Figures **xv**

List of Tables **xxiii**

List of Acronyms **xxvii**

1 Introduction **1**

1.1 Watermarking 2

1.2 Modeling of Watermarking System 3

1.2.1 Sender Side 3

1.2.2 Communication Channel 5

1.2.3 Receiver Side 5

1.3 Classification of Watermarking Schemes 6

1.3.1 Visibility of Watermark 6

1.3.2 Information Required in Watermark Extraction 9

1.3.3 Transformation Used in Watermarking 10

1.3.4 Type of Watermarks 11
1.3.5 Reversible Watermarking Scheme 12
1.3.6 Real Time Watermarking Scheme 12
1.3.7 Miscellaneous 12
1.4 Watermarking System Evaluation 13
1.4.1 Perceptibility 13
1.4.2 Capacity 13
1.4.3 Reliability 14
1.4.4 Robustness of Watermark Against Attack 14
1.5 Biometrics 16
1.5.1 Applications of Biometrics 16
1.5.2 How a Biometric System Works? 17
1.6 Problems and Contributions 19
1.7 Organization of Thesis 22

2 Blind Reliable Invisible Watermarking Scheme in Wavelet Domain for Face Image Watermark 23

2.1 Related Work 25
2.2 Watermarking Schemes and Weighted Binary Coding 29
2.2.1 Extended Watermarking Scheme of Vatsa et al. [221] in RDWT Domain 29
2.2.2 Extended Watermarking Scheme of Vatsa et al. [221] in DWT Domain 32
2.2.3 Weighted Binary Coding for a Face Image 34
2.2.4 Extended Watermarking Scheme of Kundur et al. [113] in DWT Domain 39

2.2.5 Extended Watermarking Scheme of Kundur et al. [113] in RDWT Domain 42
2.3 Experiments, Results and Analysis 45
2.3.1 Experiment 1: Performance of Watermarking Schemes with Watermark Embedding Strength 47
2.3.2 Experiment 2: Cropping from Center 57
2.3.3 Experiment 3: Gaussian Filtering 60
2.3.4 Experiment 4: Gaussian Noise 64
2.3.5 Experiment 5: Salt and Pepper Noise 67
2.3.6 Experiment 6: Rotation 70
2.3.7 Experiment 7: JPEG Compression 73
2.3.8 Experiment 8: Resize 76
2.3.9 Comparison of PSNR and NC of Extracted Watermarks . . . 78
2.4 Conclusions 79

3 Image Watermarking in Real Oriented Wavelet Transform Domain 81
3.1 Motivation and Related Work 82
3.2 ROWT and its Observed Property 84
3.2.1 ROWT 84
3.2.2 Observed Property of ROWT 90
3.3 Watermarking Schemes 92
3.3.1 Non-blind Watermarking Schemes 92
3.3.2 Blind Watermarking Schemes 100
3.4 Experiments, Results and Analysis 110
3.4.1 Experiment 1: Testing of Proposed Watermarking Schemes and Effect of Embedding Strength and Error Controller 112

3.4.2 Experiment 2: What if the Observed Property of ROWT is Not Utilized ? 114
3.4.3 Experiment 3: The Effect of Embedding Strength and Error Controller on Formatted Watermarked Images 117
3.4.4 Experiment 4: Attack Analysis 124
3.4.5 Experiment 5: Comparison Without any Attack 128
3.4.6 Experiment 6: Robustness Comparison 129
3.5 Conclusions 135

4 Watermarking Schemes to Secure the Face Database and Test Images in a Biometric System 137
4.1 Overview of the Problem and its Solution 138
4.2 Related Work 143
4.3 Spatial Domain Based Watermarking Scheme 144
4.4 DCT Domain Based Watermarking Scheme 148
4.5 Experiments, Results and Analysis 150
4.5.1 Performance Metric 150
4.5.2 Data Set 152
4.5.3 Discussion on Results 154
4.6 Conclusions 160

5 Visible Watermarking Based on Importance and Just Noticeable Distortion of Image Regions 161
5.1 Background 162
5.1.1 Related Work 162
5.1.2 Problem 165
5.1.3 Overview of Solution 166
5.1.4 Contributions 167

5.2 Solutions of Three Main Issues 168
5.2.1 Overview of Solution of Issue $\mathcal{I}1$ 168
5.2.2 Overview of Solution of Issue $\mathcal{I}2$ 168
5.2.3 Overview of Solution of Issue $\mathcal{I}3$ 170
5.3 Visible Watermarking of an Image Using a Watermark at N Positions 174
5.4 Experiments, Results and Discussion 177
5.4.1 Experiment 1 179
5.4.2 Experiment 2 185
5.4.3 Experiment 3 189
5.4.4 Experiment 4 190
5.4.5 Experiment 5 196
5.5 Conclusions 198

6 Study of Comparators for Binary Watermarks 199
6.1 Comparators 200
6.1.1 Normalized Hamming Similarity (NHS) 200
6.1.2 Normalized Correlation Coefficient (NCC/NC) 201
6.1.3 Mean Subtracted Normalized Correlation Coefficient (MSNCC) 202
6.1.4 Absolute Mean Subtracted Normalized Correlation Coefficient (AMSNCC) 203
6.1.5 Symmetric Normalized Hamming Similarity (SNHS) 204
6.2 Receiver Operating Characteristic (ROC) 204
6.3 Theoretical Analysis of SNHS Based Comparator 209
6.3.1 Condition for Avoiding Duplicate Watermarks in a Set of Watermarks 210
6.3.2 Sufficient Condition for the Existence of (FPR, FNR)=(0,0) . 211
6.3.3 Threshold Interval Corresponds to (FPR, FNR)=(0,0) 211

6.3.4 Proof for Each Extracted Watermark is Correctly Matched if Sufficient Condition Holds . . . 212
6.3.5 Proof for Each Extracted Watermark is Uniquely Matched if Sufficient Condition Holds . . . 212
6.4 Experiments, Results and Analysis . . . 215
6.4.1 Experiment 1: Comparison of Comparators . . . 221
6.4.2 Experiment 2: Verification of Analytic Formula of Threshold Interval Determination that Corresponds to (FPR, FNR)=(0,0) 235
6.5 Conclusions . . . 240

7 Conclusions and Future Scope 241
7.1 Conclusions . . . 241
7.2 Further Scope . . . 243
7.2.1 Real Time Watermarking . . . 243
7.2.2 Video Watermarking . . . 243
7.2.3 Cloud Computing . . . 244

A PSNR and Capacity 245
A.1 PSNR . . . 245
A.2 Capacity of Watermarking Scheme . . . 246

B Mathematical Preliminary 247
B.1 Convolution . . . 247
B.2 Discrete Convolution . . . 247
B.2.1 Discrete Cosine Transformation (DCT) . . . 248
B.3 Wavelet . . . 249
B.3.1 Wavelet Transform . . . 250
B.3.2 Wavelet Series . . . 250

B.3.3 Discrete Wavelet Transformation (DWT) 251
B.3.4 Fast Wavelet Transform (FWT) 251
B.3.5 Redundant Discrete Wavelet Transform (RDWT) 252
B.3.6 2D-DWT 253
B.3.7 2D-RDWT 254

Bibliography **257**

List of Figures

1.1 Modeling of a generic watermarking system 4
1.2 Invisible watermarking example 7
1.3 Visible watermarking example 7
1.4 Enrollment in a biometric system 17
1.5 Verification in a biometric system 17
1.6 Identification in a biometric system 18

2.1 Original/host images. 45
2.2 Original watermarks. 46
2.3 Performance of watermarking schemes with respect to watermark embedding strength for first combination of host image and watermark 49
2.4 Watermarked images of the first combination 53
2.5 Watermarked images of the second combination 54
2.6 Extracted watermarks of the both combinations 55
2.7 Performance of watermarking schemes with respect to cropping attack on the watermarked images 58
2.8 Performance of watermarking schemes with respect to Gaussian filtering on the watermarked images 61
2.9 Performance of watermarking schemes with respect to Gaussian noise addition in the watermarked images 65

2.10 Performance of watermarking schemes with respect to salt and pepper noise addition in the watermarked images 68
2.11 Performance of watermarking schemes with respect to rotation attack on the watermarked images 71
2.12 Performance of watermarking schemes with respect to JPEG compression of the watermarked images 74
2.13 Performance of watermarking schemes with respect to resize attack on the watermarked images 77

3.1 An analysis filter bank of ROWT 85
3.2 A synthesis filter bank of ROWT 86
3.3 ROWT of an image 87
3.4 Illustration of the observed property of the ROWT using numerical example 91
3.5 A numerical example to illustrate a traditional non-blind watermarking algorithms 95
3.6 Overview of proposed non-blind watermarking scheme. 95
3.7 A numerical example to illustrate the proposed non-blind watermarking scheme in the ROWT domain 98
3.8 A numerical example to illustrate a traditional blind watermarking algorithms 102
3.9 Overview of proposed blind watermarking scheme. 105
3.10 A numerical example to illustrate the proposed blind watermarking scheme in the ROWT domain 109
3.11 Data set. 111
3.12 Result of the proposed non-blind watermarking scheme 112
3.13 Result of the proposed blind watermarking scheme 113

3.14 Result of a traditional non-blind watermarking scheme in the ROWT domain without the observed property 116
3.15 Result of a traditional blind watermarking scheme in the ROWT domain without the observed property 116
3.16 Quantitative performance of the proposed non-blind watermarking scheme with respect to embedding strength for a formatted watermarked image 117
3.17 Visual results of the proposed non-blind watermarking scheme for a formatted watermarked image 119
3.18 Quantitative performance of the proposed blind watermarking scheme for a formatted watermarked image with respect to embedding strength and error controller 120
3.19 Visual result of the proposed blind watermarking scheme for a formatted watermarked image 122
3.20 NHS curves after cropping of formatted watermarked images 124
3.21 NHS curves after Gaussian filtering of formatted watermarked images 125
3.22 NHS curves after adding Gaussian noise in formatted watermarked images 126
3.23 NHS curves after adding salt & pepper noise in formatted watermarked images 127
3.24 Comparison of robustness of different watermarking schemes after a formatting operation 129
3.25 Comparison of robustness of different watermarking schemes after cropping the formatted watermarked images 130
3.26 Comparison of robustness of different watermarking schemes after Gaussian filtering the formatted watermarked images 131

3.27 Comparison of robustness of different watermarking schemes after adding Gaussian noise in the formatted watermarked images 132
3.28 Comparison of robustness of different watermarking schemes after adding salt & pepper noise in the formatted watermarked images . . 133

4.1 A partially compromised and proposed watermarking based secure biometric systems 139
4.2 Core idea of spatial domain based watermarking scheme 145
4.3 Training face database 152
4.4 Test face images 153
4.5 Recognition accuracy vs. ratio of number of eigen-faces to the total number of face images in the training database 154
4.6 Watermarked training face images 155
4.7 Reconstructed face images 156
4.8 Watermarked test face images 156
4.9 Comparison of the proposed DCT based watermarking scheme with existing watermarking schemes 159

5.1 Block diagram of watermark embedding strategy for a sub-image. . . 170
5.2 Block diagram for watermarking of an image 174
5.3 Sample original images 177
5.4 Sample binary watermarks 177
5.5 Visual results of proposed watermarking scheme 179
5.6 Quantitative results corresponding to several watermarked image . . . 180
5.7 Watermarking results based on user-study on several watermarked images 182
5.8 Watermarked images corresponding to the original image Im_1 (Fig. 5.3) and watermark W_3 (Fig. 5.4) 185

5.9 Watermarked images corresponding to original image Im_3 (Fig. 5.3) and watermark W_2 (Fig. 5.4) 186
5.10 Watermarked images corresponding to original image Im_{10} (Fig. 5.3) and watermark W_2 (Fig. 5.4) 187
5.11 Watermarked images to describe effects of miscellaneous watermarking parameters 189
5.12 Comparison between proposed watermark embedding strategy and watermark embedding strategy of Liu et al. [132] 191
5.13 Quantitative results for comparison between proposed and existing [132] watermark embedding strategies 193
5.14 Watermarking results based on user-study for comparison between proposed and existing [132] watermark embedding strategies 194
5.15 Attack analysis and comparison between proposed and existing [132] watermark embedding strategies 197

6.1 ROC curve of a watermarking system 205
6.2 Explanation of sets of watermarks X_1 and X_1'. 215
6.3 Explanation of sets of watermarks X_2 and X_2'. 216
6.4 Explanation of sets of watermarks X_3 and X_3'. 216
6.5 Explanation of sets of watermarks X_4 and X_4'. 216
6.6 Explanation of sets of watermarks X_5 and X_5'. 217
6.7 Explanation of sets of original images H_1 and H_1'. 217
6.8 Explanation of sets of original images H_2, H_3, H_2' and H_3' 217
6.9 Explanation of sets of original images H_4 and H_4'. 218
6.10 Explanation of sets of original images H_5 and H_5'. 219
6.11 ROC curves of watermarking systems under no attack/negative attack. Data set is D_1, watermarking scheme is of Wong et al. [235]. 221

6.12 ROC curves of watermarking systems under no attack/negative attack. Data set is D_2, watermarking scheme is of [235]. 222

6.13 ROC curves of watermarking systems under no attack/negative attack. Data set is D_3, watermarking scheme is of [235]. 222

6.14 ROC curves of watermarking systems under no attack/negative attack. Data set is D_4, watermarking scheme is of [235]. 223

6.15 ROC curves of watermarking systems under no attack/negative attack. Data set is D_5, watermarking scheme is of [235]. 223

6.16 ROC curves of watermarking systems under no attack/negative attack. Data set is D'_1, watermarking scheme is of Bhatnagar et al. [15]. . . . 224

6.17 ROC curves of watermarking systems under no attack/negative attack. Data set is D'_2, watermarking scheme is of [15]. 225

6.18 ROC curves of watermarking systems under no attack/negative attack. Data set is D'_3, watermarking scheme is of [15]. 225

6.19 ROC curves of watermarking systems under no attack/negative attack. Data set is D'_4, watermarking scheme is of [15]. 226

6.20 ROC curves of watermarking systems under no attack/negative attack. Data set is D'_5, watermarking scheme is of [15]. 226

6.21 ROC curves of watermarking systems after attacks. Data set is D_4, watermarking scheme is of [235]. 228

6.22 ROC curves of watermarking systems after attacks. Data set is D_4, watermarking scheme is of [235]. 229

6.23 ROC curves of watermarking systems after attacks. Data set is D_4, watermarking scheme is of [235]. 230

6.24 ROC curves of watermarking systems after attacks. Data set is D'_4, watermarking scheme is of [15]. 231

6.25 ROC curves of watermarking systems after attacks. Data set is D'_4, watermarking scheme is of [15]. 232

A.1 Watermarking as a communication channel. 246

B.1 Comparison between DWT and RDWT 256

List of Tables

1.1 Classification of watermarking schemes based on visibility of embedded watermark 8

1.2 Classification of watermarking schemes based on required information of original data in watermark extractor 9

1.3 Classification of watermarking schemes based on different transformation 10

1.4 Classification of watermarking schemes based on type of embedded watermark 11

2.1 Comparison of biometric based watermarking schemes from different aspects. 24

2.2 Comparison of watermarking schemes in wavelet domain from different aspects 26

2.3 Number of embedding locations available for a watermark bit of given significance 36

2.4 Quantitative performance of the watermarking schemes with respect to watermark embedding strength. 48

2.5 Quantitative results of the proposed watermarking schemes. 51

2.6 Comparison of the proposed watermarking schemes with Lin et al. [124] and Ma et al. [135]. 56

2.7 Cropping results for first combination of host image and watermark . 57

2.8 Gaussian filter results for the first combination 60
2.9 Gaussian noise results for the first combination 64
2.10 Salt & pepper noise results for the first combination 67
2.11 Rotation results for the first combination 70
2.12 JPEG compression results for the first combination 73
2.13 Resize results for the first combination 76
2.14 Performance ranking of watermarking schemes 79

3.1 Features of watermarking schemes with respect to transformed domain. 82
3.2 List of symbols used in section 3.2. 84
3.3 List of symbols used in section 3.3. 93
3.4 Quantitative results of proposed non-blind watermarking scheme based on ROWT after formatting operation 118
3.5 Quantitative results of proposed blind watermarking scheme based on ROWT after formatting operation 121
3.6 Comparison of different watermarking schemes based on CWT 128

4.1 A summary of different watermarking schemes from different aspects 142
4.2 Performance of proposed spatial domain based watermarking scheme 158

5.1 Detail of results corresponding to Fig. 5.5. 183

6.1 List of symbols used in chapter 6. 206
6.2 Explanation of data-sets $D_1, D_2, D_3, D_4, D_5, D'_1, D'_2, D'_3, D'_4$, and D'_5 used in experiments 215
6.3 Threshold interval that corresponds to (FPR, FNR)=(0,0) of various watermarking systems of watermarking scheme of Wong et al. [235] . 224
6.4 Threshold interval that corresponds to (FPR, FNR)=(0,0) of various watermarking systems of watermarking scheme of Bhatnagar et al. [15] 227

6.5 Threshold interval that corresponds to (FPR, FNR)=(0,0) of various watermarking systems of data set D_1 227
6.6 Threshold interval that corresponds to (FPR, FNR)=(0,0) of various watermarking systems of data set D_1' 233
6.7 Verification of analytic formula for threshold interval determination that corresponds to (FPR, FNR)=(0,0) for watermarking systems of watermarking scheme of Wong et al. [235] 235
6.8 Verification of analytic formula for threshold interval determination that corresponds to (FPR, FNR)=(0,0) for watermarking systems of watermarking scheme of Bhatnagar et al. [15] 236
6.9 Verification of analytic formula for threshold interval determination that corresponds to (FPR, FNR)=(0,0) for watermarking systems of data set D_1 237
6.10 Verification of analytic formula for threshold interval determination that corresponds to (FPR, FNR)=(0,0) for watermarking systems of data set D_1' 238

List of Acronyms

AMSNCC	Absolute Mean Subtracted Normalized Correlation Coefficient
ATM	Automated Teller Machine
BTC	Block Truncation Coding
CSF	Contrast Sensitive Function
CWT	Complex Wavelet Transform
DCT	Discrete Cosine Transform
DTCWT	Dual Tree Complex Wavelet Transform
DWT	Discrete Wavelet Transform
FNR	False Negative Rate
FPGA	Field Programmable Gate Array
FPR	False Positive Rate
FWT	Fast Wavelet Transform
GPU	Graphics Processing Unit
HVS	Human Visual System
IC	Integrated Circuit
ID	Identification Detail
INF	Infinity (∞)
IQA	Image Quality Assessment
IW-SSIM	Information Weighted Structural Similarity Index Measure

JND	Just Noticeable Distortion
JPEG	Joint Photographic Experts Group
LSB	Least Significant Bit
MATLAB	MATrix LABoratory
MFCC	Mel Frequency Cepstral Coefficieent
MSNCC	Mean Subtracted Normalized Correlation Coefficient
MSNHS	Maximum Symmetric Normalized Hamming Similarity
NC/NCC	Normalized Correlation Coefficient
NHS	Normalized Hamming Similarity
PDA	Personal Digital Assistant
PSNR	Peak Signal to Noise Ratio
RDWT	Redundant Discrete Wavelet Transform
ROWT	Real Oriented Wavelet Transform
TV	TeleVision
SNHS	Symmetric Normalized Hamming Similarity
VSS	Visual Secret Sharing
XOR	Exclusive OR

Chapter 1

Introduction

Digital watermarking is an important tool in multimedia that provides solution for digital rights such as broadcast monitoring, piracy, owner identification, copyright protection, copy deterrence, proof of ownership, media authentication, fingerprint/transaction tracking, copy control, legacy enhancement, etc. [13, 31, 38, 40, 115, 140, 141, 154, 169, 244, 253]. Recently, digital watermarking has been also used to enhance security of biometric systems [104, 135].

Nowadays, watermarking and biometrics are essential part in our daily life digital technology. The scope of digital watermarking and biometrics are wide in digital technology and will increase with time. Development of new watermarking schemes, upgrading the existing watermarking systems with respect to change in technology at minimal cost, analysis of watermarking systems with respect to different combinations of available tools in watermarking and broaden the usefulness of watermarking to multimedia applications are the research opportunities in watermarking.

This thesis provides watermarking state of the art, general working of biometric system and its limitations, new watermarking schemes, applications of watermarking and analysis of several watermarking systems.

Rest of the chapter is organized as follows. In section 1.1, overview of watermarking and its technical goal are discussed. Section 1.2 models a generic watermarking system and explains working of a generic watermarking system using the model. Classification of watermarking schemes based on literature survey is provided in section 1.3. Measures and tools to evaluate the performance of watermarking schemes and watermarking systems are discussed in section 1.4. An overview of biometrics and working of a biometric system are discussed in section 1.5. Overview of problems which are addressed in this thesis and our contribution to find their solution are discussed in section 1.6. Organization of the thesis is discussed in section 1.7.

1.1 Watermarking

The main idea in digital watermarking is that a watermark (which may be a binary image, a gray scale image, a signature, etc.) is embedded into a multimedia (which may be an image, a video, an audio, etc.) to obtain a watermarked media. The watermarked media is made available in public domain. To solve a problem of digital right claims associated with a watermarked media available in public domain, a watermark is extracted/detected from the watermarked media and the extracted watermark is compared with all possible embedded watermarks using a comparator to identify an embedded watermark. A comparator consists of two main components: a similarity measure function and a threshold value. A similarity measure function returns a similarity value between two watermarks. If the similarity value is greater than the threshold then watermarks are matched, otherwise not. The mathematical formulation of a general comparator is as follows:

$$C_{(\tau,\ \mathrm{sim})}(x_1, x_2) = \begin{cases} \text{match} & \text{if} \quad \mathrm{sim}(x_1, x_2) \geq \tau \\ \text{no match} & \text{otherwise} \end{cases}, \tag{1.1}$$

where, x_1 and x_2 are two watermarks, $\text{sim}(x_1, x_2)$ is an arbitrary function that measures similarity between two watermarks and τ is a threshold value.

Maximization of accurate identification rate (which directly depends on the capacity/size/length of watermark) is a common goal in all watermarking applications. If a very intelligent adversary with an aim to defeat a watermarking system is available in public domain, then watermarking problems are very challenging [140].

1.2 Modeling of Watermarking System

A typical watermarking system consists of three units namely sender side, communication channel and receiver side. Fig. 1.1 shows a block diagram to explain the structure and working of a generic watermarking system.

1.2.1 Sender Side

The main function of the sender side is to produce a watermarked media and to hand-over the watermarked media to the communication channel. The main components of a sender side are as follows:

1. Set of watermarks $X = \{x_1, x_2, \cdots x_{|X|}\}$.
2. Set of host data $H = \{h_1, h_2, \cdots h_{|H|}\}$.
3. Watermark embedding algorithm M_{emb}.
4. Watermarking algorithm key K.

The step-wise details of working at sender side are as follows:

1. Select a random watermark $x \in X$ and host multimedia $h \in H$.

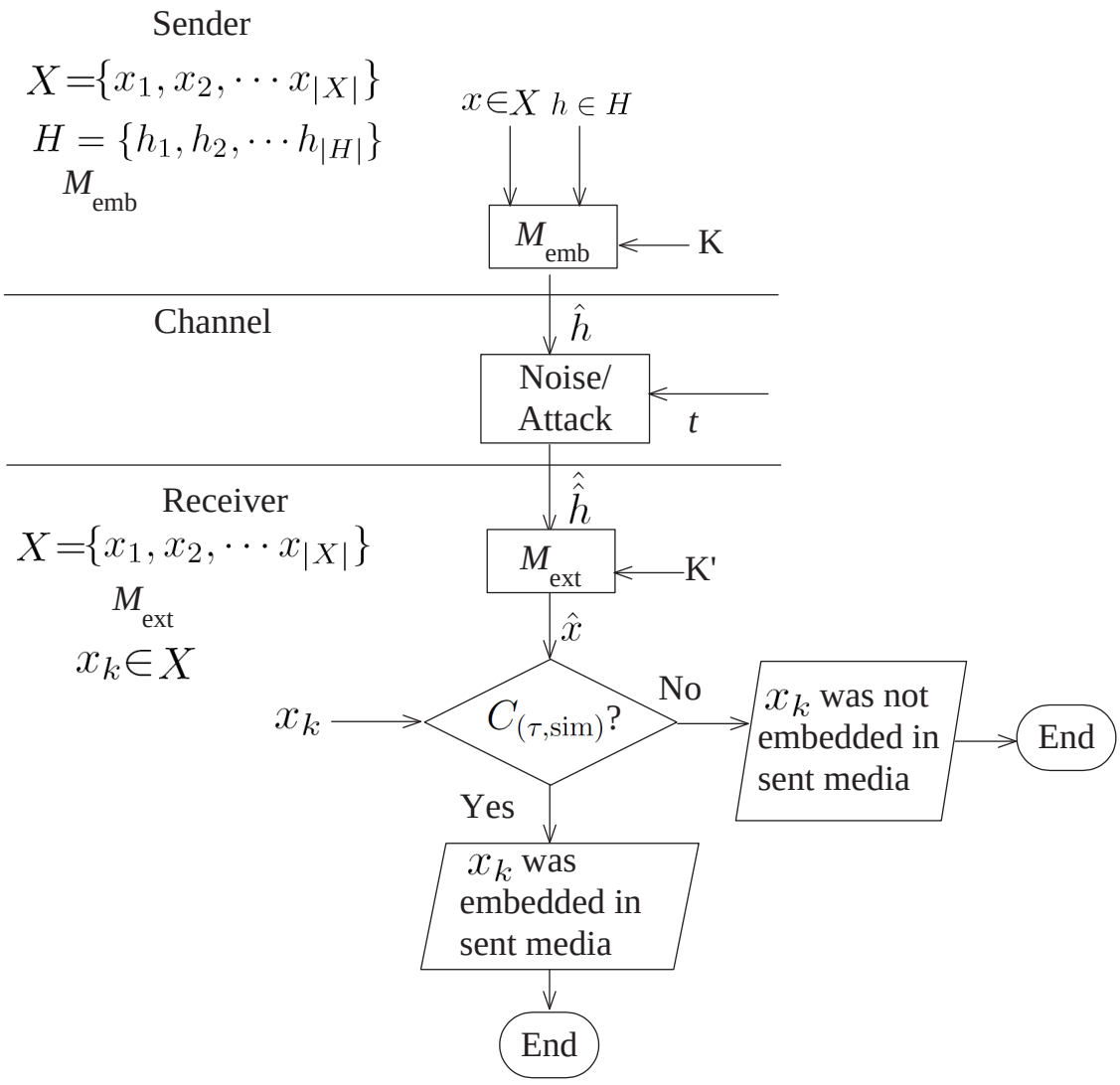


Figure 1.1: Modeling of a generic watermarking system

2. Embed x into h using the watermark embedding algorithm M_{emb} and watermark embedding algorithm key K to obtain a watermarked media $\hat{h}$.

3. The watermarked media $\hat{h}$ is transmitted to communication channel.

1.2.2 Communication Channel

The functions of an ideal communication channel are to receive a watermarked media from the sender side and to deliver the received watermarked media as such to the receiver side. In practice, ideal communication channels are rare. Some noise (t) may be added in the watermarked media or some intentional/unintentional attack (t) may be launched on the watermarked media before its delivery to the receiver. The step-wise details of working at communication channel are as follows:

1. A watermarked media $\hat{h}$ is received from the sender side.

2. The noise/attack t is applied on the watermarked media $\hat{h}$. The resultant media is temporarily stored as h_{temp}.

3. If the communication channel is ideal, then $\hat{\hat{h}} = \hat{h}$ is delivered to the receiver side. Else $\hat{\hat{h}} = h_{\text{temp}}$ is delivered to the receiver side.

1.2.3 Receiver Side

The main functions of a receiver side are to receive a watermarked media, to extract the watermark from the received watermarked media and to identify the extracted watermark. The main components of a receiver side are as follows:

1. Set of watermarks $X = \{x_1, x_2, \cdots x_{|X|}\}$ or a claimed watermark $x_k \in X$.

2. Watermark extraction algorithm M_{ext}.

3. Watermark extraction algorithm key K'.

4. Comparator $C_{(\tau,\text{sim})}$ with a threshold value τ.

Step-wise details of working at the receiver side are as follows:

1. A media $\hat{\hat{h}}$ is received from the communication channel.

2. Watermark is extracted from $\hat{\hat{h}}$ using the watermark extraction algorithm M_{ext} and its key K'. The extracted watermark is stored as $\hat{x}$.

3. The extracted watermark $\hat{x}$ is compared with all watermark of X or with x_k using the comparator $C_{(\tau,\text{sim})}$ to take a decision for the extracted watermark $\hat{x}$. The decision of $C_{(\tau,\text{sim})}$ is used by the administrator of the watermarking system.

1.3 Classification of Watermarking Schemes

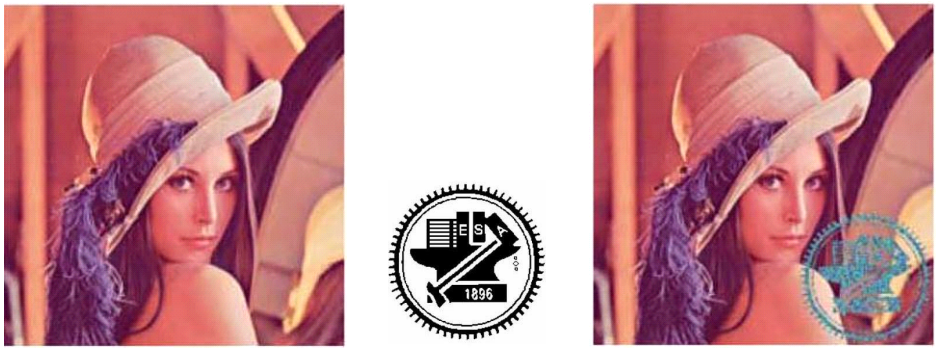
Watermarking is an advanced research topic. Several kind of watermarking schemes are available in literature. This section describes various classes of watermarking schemes based on their several important properties.

1.3.1 Visibility of Watermark

Based on visibility of the embedded watermark, watermarking schemes are divided into two categories- invisible watermarking and visible watermarking. In invisible watermarking, the embedded watermark is not visible by human perception, while in visible watermarking the embedded watermark is visible by human perception. Fig. 1.2 gives an example of invisible watermarking and Fig. 1.3 gives an example of visible watermarking schemes.

(a) (b) (c) (d)

Figure 1.2: Invisible watermarking example [124]. (a): original image. (b): original watermark. (c): watermarked image. Watermark is not visible. (d): extracted watermark.



(a) (b) (c)

Figure 1.3: Visible watermarking example [132]. (a): original image. (b): original watermark. (c): watermarked image. Watermark is visible.

Table 1.1: The following reference papers provide classification of watermarking schemes based on visibility of embedded watermark.

Invisible	[2], [5], [6], [7], [10], [11], [12], [15], [16], [17], [18], [19], [20], [21], [22], [26], [27], [28], [30], [32], [33], [35], [37], [39], [43], [44], [45], [46], [47], [49], [55], [56], [57], [58], [60], [61], [62], [66], [69], [70], [72], [74], [76], [79], [81], [82], [85], [89], [90], [91], [92], [93], [94], [95], [97], [99], [100], [102], [103], [104], [107], [113], [114], [117], [116], [118], [119], [121], [123], [125], [124], [126], [127], [130], [131], [132], [133], [137], [145], [146], [147], [148], [149], [152], [156], [157], [159], [160], [161], [162], [163], [164], [165], [166], [170], [173], [174], [175], [177], [178], [184], [187], [188], [193], [195], [196], [198], [199], [200], [202], [204], [205], [206], [207], [208], [209], [210], [211], [211], [213], [214], [215], [222], [221], [228], [229], [231], [232], [234], [235], [236], [239], [240], [243], [246], [247], [248], [249], [251], [252], [254]
Visible	[77], [78], [80], [96], [132], [151], [217] [219], [235], [238], [241], [245]
Dual	[43], [103], [150], [193]

An invisible watermarking technique/method/scheme consists of two algorithms: the watermark embedding algorithm and the watermark extraction algorithm. The purpose of watermark embedding algorithm is to embed/hide the watermark (may be text, image, logo, etc.) into the given media (image, video, audio) to obtain the watermarked data/media. Later watermark extraction algorithm extracts the watermark from the watermarked media. In visible watermarking, since the embedded watermark is visible by human perception, therefore watermark extraction algorithm is not necessary in visible watermarking.

There is one more class of watermarking known as *dual watermarking*. *Dual watermarking* is a combination of two watermarking schemes. In these schemes, two watermarks are embedded in a host media. Both the embedded watermarks may be invisible or one is visible and other is invisible. Table 1.1 provides the examples of invisible, visible and dual watermarking schemes.

Table 1.2: The following reference papers provide classification of watermarking schemes based on required information of original data in watermark extractor

Non-blind	[7], [12], [20], [60], [61], [74], [76], [91], [102], [114], [147], [159], [170], [184], [193], [213]
Semi-blind	[15], [18], [19], [145], [178], [221], [239]
Blind	[2], [5], [10], [11], [27], [37], [44], [47], [49], [50], [51], [52], [54], [57], [58], [59], [62], [66], [69], [70], [72], [79], [85], [89], [90], [98], [99], [104], [113], [118], [119], [123], [125], [124], [127], [130], [133], [135], [137], [149], [156], [161], [163], [164], [177], [188], [196], [204], [205], [210], [229], [231], [239], [240], [246], [247], [249], [254]

1.3.2 Information Required in Watermark Extraction

Depending on the required information of original data (original media/cover work and original watermark) in watermark extractor, watermarking schemes are divided into three categories, namely blind (oblivious or public), non-blind (non-oblivious or private) and semi-blind watermarking schemes [4]. Watermarking schemes that do not require the information of original data in their watermark extractor are called blind watermarking schemes. Non-blind watermarking schemes require complete information of original data in their watermark extractor while, semi-blind watermarking schemes need a part of information of original data in their watermark extractor. Non-blind watermarking schemes are applicable in those scenarios, where automated search of original media is possible [114]. However, blind watermarking schemes are more attractive, since, in many watermarking applications, original media cannot be made available at watermark extractor [4, 71, 119, 146]. Table 1.2 provides the examples of non-blind, semi-blind and blind watermarking schemes.

Table 1.3: The following reference papers provide classification of watermarking schemes based on different transformation.

Spatial	[66], [85], [103], [104], [125], [132], [150], [156], [173], [177], [189], [235], [241]
Wavelet	[2], [5], [27], [44], [47], [53], [54], [58], [62], [69], [72], [74], [76], [78], [80], [82], [89], [91], [93], [97], [102], [103], [113], [114], [123], [124], [126], [127], [130], [135], [137], [157], [161], [164], [178], [179], [184], [196], [202], [204], [205], [207], [211], [221], [229], [232], [240], [246], [249], [250], [252]
DCT	[12], [11], [39], [56], [70], [92], [95], [96], [107], [118], [146], [147], [149], [151], [152], [173], [187], [188], [199], [207], [209], [236], [250]
Fourier transform	[17], [99], [160], [165], [175], [210]
SVD	[116], [145], [30], [32]
Complex Wavelet	[37], [213], [239], [242]
Fractional domain	[43], [46], [57], [193], [248]
Wavelet+SVD	[7], [10], [15], [16], [18], [55], [61], [60], [94], [117], [121], [159]
Hybrid	[18], [19], [20], [90], [170]

1.3.3 Transformation Used in Watermarking

According to a transformed domain in which watermark is embedded, watermarking schemes are classified into two broad categories: spatial-domain and transformed-domain schemes. In spatial domain watermarking schemes, the watermark is embedded by directly modifying the pixel values of an original media. The main idea in transformed-domain watermarking schemes is that an original media is transformed, transformed coefficients of the original media are modified and the inverse transform is applied on the updated transformed coefficients to obtain the watermarked media. Table 1.3 provides the examples of watermarking schemes using different transformations. In table 1.3, hybrid implies that two or more than two transforms are used.

Table 1.4: The following reference papers provide classification of watermarking schemes based on type of embedded watermark.

Binary	[5], [6], [10], [26], [30], [32], [37], [43], [55], [76], [77], [79], [80], [81], [89], [90], [92], [93], [94], [97], [103], [113], [114], [119], [123], [125], [124], [126], [127], [130], [131], [132], [133], [137], [146], [150], [151], [152], [162], [163], [177], [178], [184], [188], [193], [195], [196], [200], [204], [211], [213], [214], [219], [228], [229], [231], [232], [235], [239], [240], [241], [245], [246], [247], [251]
Biometric	[35], [45], [58], [66], [69], [85], [98], [99], [118], [147], [157], [160], [171], [174], [221]
Random Sequence	[39], [12], [47], [50], [102], [131]
Gray Scale Image	[7], [15], [16], [18], [19], [20], [58], [60], [61], [69], [74], [114], [116], [117], [121]

1.3.4 Type of Watermarks

Different kind of watermarks have been used in watermarking. Few popular watermarks are binary watermark, gray scale image watermark, biometric watermark and random sequence watermark. Table 1.4 provides the examples of watermarking schemes of different type of watermarks.

Binary watermarks consist of random binary sequence, binary logo, etc. Class of biometric watermarks consist of any biometric feature such as fingerprint minutiae [85], eigen-face coefficients [85, 118], iris code [222], Mel-frequency-cepstral-coefficients (MFCCs) [221]. Random Gaussian sequence and random sequence of real numbers are two main watermarks in the class of random sequence watermark.

1.3.5 Reversible Watermarking Scheme

In these schemes, the exact original multimedia is recovered from the watermarked media. Few popular examples of reversible watermarking schemes are given in [53, 77, 82, 100, 197, 214, 219, 227, 238, 241, 245].

1.3.6 Real Time Watermarking Scheme

In real time watermarking, watermark is embedded in an original multimedia at the same time when it is captured. The real time watermarking schemes are applicable for real-time broadcasting, video authentication, secure camera system for courtroom evidence, etc. Mostly, real time watermarking schemes are designed on hardware such as field programmable gate array (FPGA) processor board, digital signal processor (DSP) board, or custom IC and graphics processing unit (GPU) [108]. Few examples of hardware based watermarking schemes are given in [6, 26, 91, 139, 146, 147, 149, 187, 199].

1.3.7 Miscellaneous

Recently, chaotic map and visual cryptography have been used as a powerful tool in watermarking.

Chaotic maps are very sensitive to initial conditions and their orbits outspread over the entire space. These properties are used to increase the security in digital watermarking. Some examples of watermarking schemes based on the chaotic maps are given in [44, 99, 153, 182].

In 1995, Naor and Shamir [155] have proposed the concept of (k, n) visual secret sharing (VSS) scheme. This is a concept of visual cryptography. This scheme splits a binary image into n different shares. The image can be retrieved with $k, (k \leq n)$ or more than k shares but any $k-1$ shares give absolutely no information about the

image. A good literature on application of visual cryptography in the watermarking is provided by Weir et al. [233]. Few more examples of watermarking schemes based on visual cryptography are given in [183, 200].

1.4 Watermarking System Evaluation

Performance of a watermarking system is evaluated using a series of measures. Some measures are perceptibility, capacity, reliability, and robustness of watermark against attacks [112, 167].

1.4.1 Perceptibility

This measures the perceptual quality of watermarked media with respect to original media. For invisible watermarking schemes, watermarked media and original media should be indistinguishable. For visible watermarking schemes, artist value in the watermarked media should be maintained. We have used peak-signal-to-noise-ratio (PSNR, see appendix A.1 and [112, 113]) and information-weighted-structural-similarity-index-measure (IW-SSIM) [230] to measure the quality of watermarked media. A higher value of PSNR and IW-SSIM ensure less degradation in watermarked media. The unit of PSNR is decibel (dB).

1.4.2 Capacity

It measures the amount of information hidden in a media. We have used the size of watermark and capacity (see appendix A.2 and [176]) to measure the capacity of a watermarking schemes and the unit is computed as bit. Higher capacity is a common demand in all watermarking scenarios.

1.4.3 Reliability

It measures the successful identification of the embedded watermark. Several similarity index measure such as normalized Hamming similarity (NHS, see section 6.1.1), normalized correlation coefficient (NC/NCC, see section 6.1.2) and PSNR are used to measure the reliability of watermarking system. If extracted watermark corresponds to a reference watermark, then similarity index should be high, otherwise it should be low.

For large scale scenarios, reliability is measured using false positive rate and false negative rate [40, 112]. False positive rate (FPR) is defined as the ratio of false positive decision to the total positive decision, whereas, false negative rate (FNR) is defined as the ratio of false negative decision to the total negative decision. Simultaneous low values of false positive rate and false negative rate is a common goal in all watermarking scenarios.

1.4.4 Robustness of Watermark Against Attack

A watermarked media may be subjected to some attack(s). Some common benchmark attacks are removal attacks, geometric attacks, cryptographic attacks, and protocol attacks [68, 181, 223, 224].

Removal attacks try to remove the watermark information from the watermarked media without cracking the key used in watermark embedding. Examples of removal attacks are linear and non-linear filtering, sharpening, contrast enhancement, gamma correction, compression, collusion attack, mosaic attacks and other media processing operations.

Geometric attacks apply some geometric operation on a watermarked media. Examples of Geometric attacks are translation, rotation, mirroring, scaling, shearing, cropping, line or column removal, etc.

Cryptographic attacks try to remove the embedded watermark or embed misleading watermarks.

Protocol attack was proposed by Carver et al. [41]. The main idea in this attack is that the presence to unauthorized watermark is proved. This creates an ambiguous situation that who is the rightful owner.

All attacks affect the presence of watermark in the watermarked media. Based on the presence of the watermark in the watermarked media after attack(s), watermarking schemes are divided into three categories: fragile, semi-fragile, and robust.

Fragile: Watermark is undetected after any kind of attack on the watermarked media. Such watermarking schemes are helpful in the tamper detection scenario [40].

Semi-fragile: Watermark is detected after permissible attacks on the watermarked media and undetected after un-permissible attacks on the watermarked media.

Robust: Watermark is detected after any attack on the watermarked media. Such watermarking schemes are helpful in proof of ownership, copyright protection, transaction tracking, etc. [40].

Four benchmarks namely, *stirmark*, *unzign*, *checkmark*, and *certimark* [108, 128] have been developed that combine various attacks in a unified framework. These benchmarks are used as standardization and testing tools for watermarking systems.

1.5 Biometrics

"Biometric recognition or, simply, biometrics refers to the automatic recognition of individuals based on their physiological and/or behavioral characteristics " [87]. The physiological and/or behavioral characteristics associated with an individual is/are called biometric trait. The common examples of biometric trait are face, fingerprint, iris, voice, ear, facial thermogram, hand thermogram, hand vein, gait, hand geometry, palm-print, retina, DNA and signature [87]. Biometrics offers several advantages over traditional identification/verification methods such as password or i-card. The traditional password/i-card can be lost/stolen, can be forgotten and can be shared. On the other hand, biometric traits are permanently associated with an individual. Therefore, sharing/stealing of biometric trait is very difficult. Moreover, biometrics is the only way to detect duplicate identities [84].

1.5.1 Applications of Biometrics

Biometrics has wide applications in commercial community, society and government sectors around the world [84].

Commercial applications include computer network login, electronic data security, e-commerce, internet access, ATM, credit card, physical access control, cellular phone, PDA, medical records management, and distance learning.

Government applications include national ID card, correctional facility, driver's license, social security, welfare disbursement, border control [1] (in USA, UK, Singapore and other countries), passport control and Aadhar [158].

Forensic applications include corpse identification, criminal investigation, terrorist identification, parenthood determination and missing children.

Social applications include homeland security and surveillance.

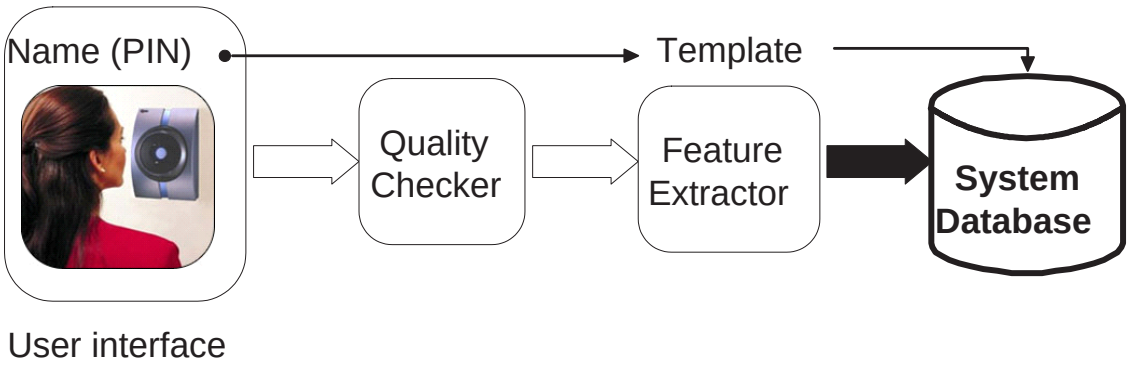


Figure 1.4: Enrollment in a biometric system

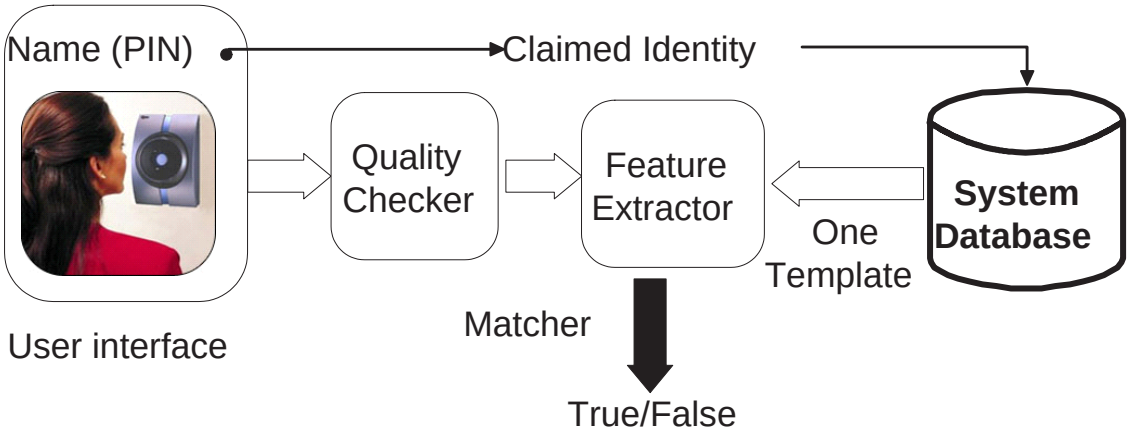


Figure 1.5: Verification in a biometric system

1.5.2 How a Biometric System Works?

In general, a biometric system has two working phase – enrollment and verification/identification phases [87].

Enrollment: During enrollment, a sample of a user's biometric trait is recorded using an appropriate sensor – for example, a face image is recorded by a camera. Then salient characteristics (such as eigen-face coefficients [220]) from the recorded biometric trait sample (sample face image) are extracted

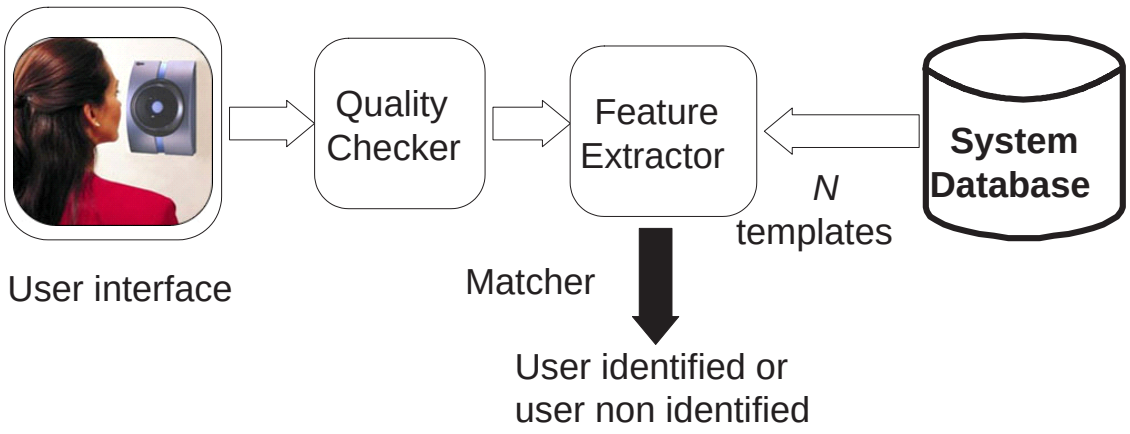


Figure 1.6: Identification in a biometric system

using a software algorithm called a feature extractor. Then these extracted salient characteristics (eigen-face coefficients) also called features are stored as a template in a database with other identifiers such as name or an identification number of the user.

Fig. 1.4 describes graphically the enrollment procedure.

Verification: In verification, an user presents his/her biometric trait (face image) at the sensor (camera) and submits identifier (name/identification number) to the biometric system. Feature extractor extracts features (eigen-face coefficients) from the biometric trait (face image) received from the sensor. The extracted features are called query features. At the matcher, the query features are compared with the features of the claimed identity stored in the database.

Fig. 1.5 describes the verification procedure graphically.

Verification procedure is an one to one comparison. The claim associated with biometric trait that has two disjoint values defined as, either claim is true or it is not true.

Identification: It is similar to verification procedure except the following:

- The user need not submit identifier.
- The query feature (query biometric trait) is compared with all the templates stored in the database.
- Identification is one to N comparison, where, N is the number of identities enrolled in the system. In identification mode, the query image is classified as one class among $N + 1$ disjoint classes, where N classes correspond to the enrolled identities and one class corresponds to no suitable enrolled identity.

Fig. 1.6 describes the identification procedure graphically.

1.6 Problems and Contributions

In this thesis, we have discussed the solution of five watermarking related problems. In the following, we have highlighted the overview of each problem and contributions towards the solution of each problem.

1. In the first problem, digital image watermarking and biometrics have been combined to improve the owner identification/verification technology. We have extended the base watermarking schemes of Kundur et al. [113] and Vatsa et al. [221]. We have proposed four blind-invisible-watermarking-schemes in wavelet domain that use a face image as watermark and a digital image as cover work. We have proposed weighted binary coding. One extended watermarking scheme of each base watermarking scheme incorporates the weighted binary coding. We have observed that extended version of Kundur et al. [113] coupled with weighted binary coding provides the best solution.

2. Recently, transforms of complex wavelet family are emerged as very important multimedia processing tools. An important transform of this family is the real oriented wavelet transform (ROWT). Developing the watermarking scheme of high capacity watermark in the ROWT domain is an important research opportunity in watermarking. However, unlike DCT, DWT, etc., left inverse of the real oriented wavelet transform followed by the real oriented wavelet transform is not the identity transform. This makes reliable watermark extraction of high capacity watermark in the ROWT domain a challenging problem, which is our second problem.

   We have obtained a product of left inverse of ROWT followed by the ROWT itself. Based on this product, we have developed non-blind and blind watermarking schemes of high capacity watermark in the ROWT domain. Further, exploring the observed relation to develop an efficient blind watermarking scheme was another challenge. This challenge has been solved by a deep investigation of the quotient-remainder theorem for the real numbers.

3. Recently, researchers have used watermarking to provide solution of security/integrity related issues of a compromised biometric system. Unfortunately, a foolproof biometric system is not developed so far. In the third problem, we have used watermarking to improve security/integrity of a compromised biometric system. We have considered a face biometric system, whose working procedure is based on the ideas of Turk et al. [220]. We have proposed spatial domain and discrete cosine transform based watermarking schemes. Spatial domain based watermarking scheme is blind, reversible and fragile which improves the integrity of the training face database in a biometric system. Discrete cosine transform based watermarking scheme is blind and robust which improves the integrity of test images.

4. Fourth problem is to develop a visible watermarking technique to embed a binary logo watermark at N non-overlapping positions in an image such that important portions of the image are not occluded. This problem is motivated by the fact that visible watermark is embedded at predefined positions in image/video frame, which leads occlusion of important portion of multimedia objects by the visible watermark, for instance, TV channel logo used for television broadcasting.

   In the proposed technique, the areas for watermark embedding in an image are found through visual saliency computation [83] or available human eye fixation density maps. In the proposed visible watermarking, just noticeable distortion [34, 173] is used to adaptively filter the watermark embedding energy based on the image content. A mathematical model in terms of information-content-weighted-structural-similarity-index [230] and visual importance is proposed to find optimal watermark embedding strength.

5. Last problem analyses the effect of different comparators on the performance of watermarking systems in case of binary watermarks. We have analysed the normalized Hamming similarity (NHS) [112], the normalized correlation coefficient (NCC) [42], the mean subtracted NCC (MSNCC) [19, 159], symmetric NHS (SNHS, a version derived from NHS), absolute MSNCC (AMSNCC, a version derived from MSNCC) based comparators under the assumption that negative of binary watermark is treated same as itself, since negative pair of binary watermarks provides same information.

   We have evaluated the performance of watermarking systems using receiver operating characteristic curve (ROC curve is defined as FNR versus FPR plot). A generic algorithm has been discussed to plot ROC curve for a generic watermarking system. We have concluded that SNHS and AMSNCC based

comparators treat negative of watermark same as itself. A formula has been derived using analytical proof to find the threshold interval corresponds to (FPR, FNR)=(0,0) for SNHS based comparator for a given watermarking system. We have verified the derived formula for several watermarking systems.

1.7 Organization of Thesis

This thesis is divided into seven chapters. The first chapter is meant for the introduction. Next five chapters are related to five problems. Each chapter among these five chapters discusses a problem, related work, contributions, algorithms, methodology used, experiments, observations and conclusions. Chapter 7 concludes the thesis and suggests open avenues for further study.

Chapter 2

Blind Reliable Invisible Watermarking Scheme in Wavelet Domain for Face Image Watermark

In this chapter, digital image watermarking and biometrics are combined to improve the owner identification/verification technology. Four blind-invisible watermarking schemes namely S_1, S_2, S_3, and S_4 are presented. S_1 and S_2 are extended version of Vatsa et al. [221], and S_3 and S_4 are extended version of Kundur et al. [113]. S_1 and S_4 operate in the redundant discrete wavelet transform (RDWT) domain and, S_2 and S_3 operate in the discrete wavelet transform (DWT) domain. In all these schemes, a common novelty is that a face thumbnail is used as watermark. Further, we have proposed a weighted binary coding. Weighted binary coding is used to convert a face image into a binary string and to reconstruct the face image from the binary string. The watermark embedding and extraction algorithms of schemes S_3 and S_4 incorporate the proposed weighted binary coding.

Table 2.1: Comparison of biometric based watermarking schemes from different aspects.

Scheme	Domain	Type of watermark	Information required during watermark extraction	Length of watermark	Is watermark biometric ?	Other remarks
[179]	Wavelet	A string	–	Small	No	–
[85]	Spatial	Fingerprint minutiae, eigen-face coefficients	Blind	Small	Yes	–
[222]	Spatial, DCT, [179]	Binary iris code	Blind	Small	Yes	Existing schemes
[35]	Spatial, [66]	Fingerprint minutiae, eigen-face coefficients	Blind	Small	Yes	Degradation in watermarked face image
[103]	Spatial+wavelet, [66], [47]	Binary	Blind	Small	No	–
[249]	Wavelet, [113]	Fingerprint minutiae	Blind	Small	Yes	–
[69]	Wavelet, [113]	Fingerprint minutiae	Blind	Small	Yes	–
[99]	Wavelet	Encrypted iris code	Blind	Small	Yes	–
[98]	Fourier transform	Fingerprint features	Blind	Small	Yes	–
[160]	Fourier transform	Iris features	Blind	Small	Yes	Detector
[157]	Wavelet	Face + binary text	Blind	Large	Yes	High error in extracted watermarks
[250]	DCT+DWT	Binary	Blind	Small	No	–
[33]	DCT	Binary logo	–	Small	No	–
[221]	RDWT	MFCC (voice feature)	Semi-blind	Large	Yes	–
[118]	DCT + [66]	Eigen-face coefficients	Blind	Small	Yes	–
[104]	Spatial	Face	Blind	Small	Yes	Small size of watermark
[174]	Correlation analysis	Palm print and iris	Non-blind	Large	Yes	Heavily rely on watermark and original image
[58]	Wavelet+LSB	Binary iris feature	Blind	Small	Yes	–
[196]	Wavelet	Binary logo	Blind	Small	No	–
[45]	DCT	Eigen-face coefficients	Blind	Small	Yes	–

This chapter is organized as follows. In section 2.1, the detailed literature survey has been done on the related work. Watermarking algorithms and weighted binary coding are presented in section 2.2. In section 2.3, experimental environment and the results are discussed. Finally, conclusions are drawn in section 2.4.

2.1 Related Work

Table 2.1 gives a summary of biometric watermarking scheme (in biometric watermarking scheme, host image/watermark is/are a biometric trait) and Table 2.2 gives a summary of wavelet based watermarking schemes from different aspects. The main highlights of the literature survey are as follows.

1. For biometric related applications, mostly blind watermarking schemes are popular.

2. In biometric watermarking schemes, binary sequence/binary image, features of biometric trait (iris code, Eigen-face coefficients, fingerprint minutiae, MFC coefficients or face image) are used as watermark.

3. In most of the biometric watermarking schemes, length of the watermark is considered as small.

4. Noore et al. [157] and Kim et al. [104] have used face image as a watermark. In Noore et al. [157], high value of error is observed in extracted face watermark. In Kim et al. [104], size of the watermark is considered as small.

5. The watermarking scheme proposed by Gunsel et al. [66] is the most popular in biometric application. It operates in spatial domain and the length of the watermark is considered very small.

Table 2.2: Comparison of watermarking schemes in wavelet domain from different aspects.

Scheme	Extractor/ detector	Information required during watermark extraction	Watermark	Length of watermark	Other remarks
[232]	–	Semi-blind	Random binary sequence	< 236	–
[170]	Detector	Non-blind	Random Gaussian sequence	$<$ Size of original image	–
[76]	Extractor	Non-blind	Binary logo	–	–
[47]	Detector	Blind	Random uniform distributed sequence	–	–
[113]	Extractor	Blind	A binary sequence	–	Modification required to embed biometric watermark
[102]	Extractor	Non-blind	Random Gaussian sequence	–	–
[11]	Detector	–	Random binary sequence	–	–
[72]	Extractor	Blind	Function of original image	–	User defined watermark can't be used

to be continued in the next page

Table 2.2 – continued from previous page

Scheme	Extractor/ detector	Information required during watermark extraction	Watermark	Length of watermark	Other remarks
[74]	Extractor	Non-blind	Binary, gray scale image	–	–
[211]	Extractor	Blind	Binary	16×16	–
[252]	Extractor	Non-blind	Random Gaussian sequence	–	–
[114], [184]	Extractor	Non-blind	Binary, gray scale image	–	–
[44]	Detector	Non-blind	Binary sequence	–	Artifacts in watermarked image
[10]	Detector	Semi-blind	Binary image	Very small	–
[62]	Detector	Semi-blind	Random binary sequence	< 1024	–
[130]	Extractor	Semi-blind	Random binary sequence	–	User defined watermark may not be used
[204]	Extractor	Blind	Random binary logo	32×32	Similar to [113]

to be continued in the next page

Table 2.2 – continued from previous page

Scheme	Extractor/ detector	Information required during watermark extraction	Watermark	Length of watermark	Other remarks
[127]	Extractor	Blind	Binary image	32×32	Small size of watermark
[117]	Extractor	Semi-blind	Gray scale	32×32	SVD+DWT
[54]	Extractor	Semi-blind	Binary	–	Audio watermarking, similar to [113]
[97]	Extractor	Blind	Binary image	8×8	Very small size of watermark

6. The blind watermarking scheme proposed by Kundur et al. [113] is the most popular among DWT based watermarking schemes. The scheme of Kundur et al. [113] has been used by Zebbiche et al. [249], Hassanien et al. [69], Soheili et al. [204], Fallahpour et al. [54].

7. Vatsa et al. [221] have proposed a semi-blind biometric watermarking scheme using RDWT. Its modification as a blind watermarking scheme is found to be an easier one.

2.2 Watermarking Schemes and Weighted Binary Coding

This section is divided into five different sub-sections. Theory of watermark embedding and extraction algorithms of the watermarking scheme S_1 are discussed in section 2.2.1. Watermark embedding and extraction algorithms of watermarking scheme S_2 are discussed in section 2.2.2. Motivation to propose weighted binary coding, its theory, its encoding and decoding algorithms are discussed in section 2.2.3. Theory of watermark embedding and extraction algorithms of the watermarking schemes S_3 and S_4 are discussed in sections 2.2.4 and 2.2.5 respectively.

2.2.1 Extended Watermarking Scheme of [221] in RDWT Domain: S_1

Vatsa et al. [221] have proposed a biometric watermarking scheme. A color face image has been used as an original image and Mel-Frequency-Cepstral-Coefficients (MFCC) [86] voice feature have been used as a watermark. Watermarking has been done in RDWT domain. Phase congruency based edge and corner feature detection algorithm [109] has been applied on the original image to find embedding locations.

A key has been used to select embedding locations from the available embedding locations. These embedding locations are changed with respect to original image. The same selected embedding locations are required during watermark extraction and this is a semi-blind watermarking scheme.

A main update in S_1 is that embedding locations are selected from the detailed sub-bands of the original image. Further, RDWT is applied on the original image to find detailed sub-bands. A key is used to select embedding locations from the available embedding locations. These embedding locations are not changed with respect to original image. This update makes S_1 a blind watermarking scheme. We have ensured that the quality of watermarked images and extracted watermarks obtained using watermarking schemes S_1 and of Vatsa et al. [221] are very close to each other.

In the following, embedding and extraction algorithms of S_1 are discussed.

Embedding Algorithm of S_1

Input:

- Gray scale original image $\mathbf{I}_o = \{I_o(m_1, n_1) : m_1 = 1, 2, \cdots M_1; n_1 = 1, 2, \cdots N_1\}$ of size $M_1 \times N_1$.
- Watermark (a face image) $\mathbf{W}_o = \{W_o(m_2, n_2) : m_2 = 1, 2, \cdots M_2; n_2 = 1, 2, \cdots N_2\}$ of size $M_2 \times N_2$.
- Embedding locations selection key $\mathbf{ckey}_1 = \{ckey_1(m_2, n_2) \rightarrow (i, j, k) : i \in \{1, 2, \cdots M_1\}; j \in \{1, 2, \cdots N_1\}; k \in \{H, V, D\}; m_2 = 1, 2, \cdots M_2; n_2 = 1, 2, \cdots N_2\}$. H, V and D represent detailed bands of the image $\mathbf{I}_o$. Note that $ckey_1(m_2, n_2)$ should be different for different (m_2, n_2)s and '$\rightarrow$' denotes 'maps into'.
- Watermark embedding strength α_1.

Processing:

1. Apply 1-level RDWT on the image $\mathbf{I}_o$ to obtain $\hat{\mathbf{I}} = \{\hat{I}(u_1, v_1, l_1) : u_1 = 1, 2, \cdots M_1; v_1 = 1, 2, \cdots N_1; l_1 = A, H, V, D\}$. The subset $\hat{\mathbf{I}}_A = \{\hat{I}(u_1, v_1, A) : u_1 = 1, 2, \cdots M_1; v_1 = 1, 2, \cdots N_1\}$ is corresponding to A that gives approximation part of the image and it is called approximation band. Similarly, subsets $\hat{\mathbf{I}}_H$, $\hat{\mathbf{I}}_V$, $\hat{\mathbf{I}}_D$ are corresponding to H, V and D respectively that give detailed part of the image and are called detailed bands.

2. Define $\hat{\mathbf{I}}_w = \hat{\mathbf{I}}$.

3. Update $\hat{\mathbf{I}}_w$ by embedding watermark coefficients as follows

$$\hat{I}_w(ckey_1(m_2, n_2)) = \alpha_1 W_o(m_2, n_2);\ m_2 = 1, 2, \cdots M_2;\ n_2 = 1, 2, \cdots N_2. \tag{2.1}$$

4. Apply 1-level inverse RDWT, followed by the floating point truncation on the updated $\hat{\mathbf{I}}_w$ to obtain the watermarked image $\mathbf{I}_w$.

Output:

Watermarked image $\mathbf{I}_w$ of size $M_1 \times N_1$ that has same format as of I_o.

Extraction Algorithm of S_1

Input:

- An image $\mathbf{I}' = \{I'(m_1, n_1) : m_1 = 1, 2, \cdots M_1; n_1 = 1, 2, \cdots N_1\}$ of size $M_1 \times N_1$ (that may be watermarked, unmarked or attacked).
- Embedding locations selection key $\mathbf{ckey}_1$ as defined in embedding algorithm of S_1.
- Watermark embedding strength α_1 as defined in embedding algorithm of S_1.

Processing:

1. Apply 1-level RDWT on the image $\mathbf{I}'$ to obtain $\hat{\mathbf{I}}' = \{\hat{I}'(u_1, v_1, l_1) : u_1 = 1, 2, \cdots M_1; v_1 = 1, 2, \cdots N_1; l_1 = A, H, V, D\}$.

2. Use the following formula followed by the floating point truncation to extract watermark coefficients as

$$W_e(m_2, n_2) = \frac{\hat{I}'(ckey_1(m_2, n_2))}{\alpha_1};\ m_2 = 1, 2, \cdots M_2; n_2 = 1, 2, \cdots N_2;\ \alpha_1 \neq 0. \tag{2.2}$$

Output:

Extracted watermark $\mathbf{W}_e = \{W_e(m_2, n_2) : m_2 = 1, 2, \cdots M_2; n_2 = 1, 2, \cdots N_2\}$ of size $M_2 \times N_2$ that has the same format as of $\mathbf{W}_o$.

2.2.2 Extended Watermarking Scheme of [221] in DWT Domain: S_2

Watermarking scheme S_2 is similar to the watermarking scheme S_1 except the following differences: (i) DWT is applied on the original sub-image to find embedding locations; (ii) Watermarking is done in the DWT domain. Embedding and extraction algorithms are discussed in the following.

Embedding Algorithm of S_2

Input:

- Gray scale original image $\mathbf{I}_o$ of size $M_1 \times N_1$, as defined in the previous section.
- Watermark (a face image) $\mathbf{W}_o$ of size $M_2 \times N_2$, as defined in the previous section.

- Embedding locations selection key $\mathbf{ckey}_2 = \{ckey_2(m_2, n_2) \rightarrow (i, j, k), i \in \{1, 2, \cdots \frac{M_1}{2}\}; j \in \{1, 2, \cdots \frac{N_1}{2}\}; k \in \{H, V, D\}; m_2 = 1, 2, \cdots M_2; n_2 = 1, 2, \cdots N_2\}$. Note that $ckey_2(m_2, n_2)$ should be different for different (m_2, n_2)s and '$\rightarrow$' denotes 'maps into'.

- Watermark embedding strength α_2.

Processing:

1. Apply 1-level DWT on the image $\mathbf{I}_o$ to obtain $\hat{\mathbf{I}} = \{\hat{I}(u_1, v_1, l_1); u_1 = 1, 2, \cdots \frac{M_1}{2}; v_1 = 1, 2, \cdots \frac{N_1}{2}; l_1 = A, H, V, D\}$.

2. Define $\hat{\mathbf{I}}_w = \hat{\mathbf{I}}$.

3. Update $\hat{\mathbf{I}}_w$ by embedding watermark coefficients as follows

$$\hat{I}_w(ckey_2(m_2, n_2)) = \alpha_2 W_o(m_2, n_2); m_2 = 1, 2, \cdots M_2; n_2 = 1, 2, \cdots N_2. \tag{2.3}$$

4. Apply 1-level inverse DWT, followed by floating point truncation on the updated $\hat{\mathbf{I}}_w$ to obtain the watermarked image $\mathbf{I}_w$.

Output:

Watermarked image $\mathbf{I}_w$ of size $M_1 \times N_1$ that has same format as of $\mathbf{I}_o$.

Extraction Algorithm of S_2

Input:

- An image $\mathbf{I}'$ of size $M_1 \times N_1$, as defined in the previous section.

- Embedding locations selection key $\mathbf{ckey}_2$, as defined in the previous section.

- Watermark embedding strength α_2, as defined in the previous section.

Processing:

1. Apply 1-level DWT on the image $\mathbf{I}'$ to obtain $\hat{\mathbf{I}}' = \{\hat{I}'(u_1, v_1, l_1) : u_1 = 1, 2, \cdots \frac{M_1}{2}; v_1 = 1, 2, \cdots \frac{N_1}{2}; l_1 = A, H, V, D\}$.

2. Use the following formula followed by the floating point truncation to extract watermark coefficients as follows

$$W_e(m_2, n_2) = \frac{\hat{I}'(ckey_2(m_2, n_2))}{\alpha_2}; m_2 = 1, 2, \cdots M_2; n_2 = 1, 2, \cdots N_2, \alpha_2 \neq 0. \tag{2.4}$$

Output:

Extracted watermark $\mathbf{W}_e$ of size $M_2 \times N_2$ that has the same format as of $\mathbf{W}_o$.

2.2.3 Weighted Binary Coding for a Face Image

Kundur et al. [113] have proposed a blind watermarking scheme in DWT domain. A gray scale image has been used as an original image and a binary sequence has been used as a watermark.

In this chapter, an eight-bit gray scale face image is considered as a watermark. If we use the watermarking scheme of Kundur et al. [113] and consider an eight-bit gray scale face image as a watermark, then the face image must be converted into a binary sequence during the embedding process. Further, during the extraction process, face image is estimated using an extracted binary sequence.

In this section, we have proposed a weighted binary coding. In the proposed weighted binary coding, more importance is given to more significant bits of a face image. The weighted binary coding consists of two algorithms namely, weighted binary encoding and decoding. Weighted binary encoding converts a face image into a binary sequence and the decoding reconstructs the face image from the binary sequence.

Weighted Binary Encoding

This section discusses the theory of weighted binary encoding. Based on this theory, an algorithm for weighted binary encoding is proposed. Let $\mathbf{W}_o = \{W_o(m_2, n_2) : m_2 = 1, 2, \cdots M_2; n_2 = 1, 2, \cdots N_2\}$ be an eight bit gray scale image of size $M_2 \times N_2$, and N_w be the number of locations available for embedding.

Assumptions: We have made the following assumptions in the theory of weighted binary encoding.

$\mathcal{A}1$. All the pixels $W_o(m_2, n_2)$s of $\mathbf{W}_o$ have equal importance.

$\mathcal{A}2$. Each bit of the $W_o(m_2, n_2)$s should be embedded at least once during watermarking, if possible. This assumption helps in avoiding the information loss of watermark during watermarking.

$\mathcal{A}3$. Odd redundancy of watermark bits is better than even redundancy.

Statements: Based on the above assumptions, we have made following statements.

$\mathcal{S}1$. According to assumption $\mathcal{A}1$, the number of available embedding locations for each $W_o(m_2, n_2)$ is $d = \left\lfloor \frac{N_w}{M_2 \times N_2} \right\rfloor$.

$\mathcal{S}2$. The number of available embedding locations for m_3th LSB of each $W_o(m_2, n_2)$ is mm_3, where

$$\sum_{m_3=1}^{8} mm_3 = d. \tag{2.5}$$

$\mathcal{S}3$. Number of available embedding locations for each bit of each $W_o(m_2, n_2)$ is a natural number. $\mathcal{S}2$ may produce mm_3 as a fraction. Therefore, number of available embedding locations for m_3th LSB of each $W_o(m_2, n_2)$ is updated with $R(mm_3)$, where, $R(mm_3)$ is a natural number in a neighborhood of mm_3.

$\mathcal{S}4$. In view of assumptions $\mathcal{A}2$ and $\mathcal{A}3$, $R(mm_3)$ must satisfy the following.

Table 2.3: $R(mm_3)$s for two different values of N_w. $M_2 \times N_2 = 64 \times 64$.

	$N_w = 3 \times 256 \times 256$ $d = 48$ $m = 1.33$		$N_w = 3 \times 512 \times 512$ $d = 192$ $m = 5.33$	
m_3	mm_3	$R(mm_3)$	mm_3	$R(mm_3)$
1	1.33	1	5.33	5
2	2.66	3	10.66	11
3	3.99	5	15.99	17
4	5.32	5	21.32	21
5	6.65	7	26.65	27
6	7.98	7	31.98	31
7	9.31	9	37.31	37
8	10.64	11	42.64	43

- $|R(mm_3) - mm_3|$ is minimum.
- $R(mm_3)$ is an odd integer.
- $\sum R(mm_3) = d$.
- $R(mm_3) \geq 1$ for all $m_3 = 1, 2, \cdots 8$, if possible.

Table 2.3 gives possible $R(mm_3)$s for two different values of N_w.

The values of N_w and $R(mm_3)$ used in experiments are reported in Table 2.3.

Algorithm A_1 for weighted binary encoding: The algorithm A_1 converts $\mathbf{W}_o$ (an eight bit gray scale image of size $M_2 \times N_2$) in binary form $\mathbf{W}$. It satisfies the statements $\mathcal{S}1$-$\mathcal{S}4$. It takes two input: $\mathbf{W}_o$ and N_w and returns an output: $\mathbf{W}$. This algorithm can be represented as

$$\mathbf{W} = A_1(\mathbf{W}_o, N_w).$$

The steps involved in algorithm A_1 are as follows.

Step1. Compute $d = \left\lfloor \frac{N_w}{M_2 \times N_2} \right\rfloor$.

Step2. Compute $m = \left\lfloor \frac{d}{\sum m_3} \right\rfloor, m_3 = 1, 2, \cdots, 8$.

Step3. Find $R(mm_3)$ as stated in $\mathcal{S}4$, $m_3 = 1, 2, \cdots, 8$.

Step4. Convert $W_o(m_2, n_2)$ in weighted binary form as follows

$$W_o(m_2, n_2) \rightarrow b_8 b_7 \cdots b_1 \rightarrow \left\{ \begin{array}{c} \overbrace{b_8 b_8 \cdots b_8}^{R(8m)} \\ \\ \overbrace{b_7 b_7 \cdots b_7}^{R(7m)} \\ . \\ . \\ . \\ \overbrace{b_{m_3} b_{m_3} \cdots b_{m_3}}^{R(m_3 m)} \\ . \\ . \\ . \\ \overbrace{b_1 b_1 \cdots b_1}^{R(m)} \end{array} \right\} = W(m_2, n_2, m_3, n_3); \quad (2.6)$$

where, $b_8 b_7 \cdots b_1$ is binary representation of $W_o(m_2, n_2)$; $\mathbf{W} = \{W(m_2, n_2, m_3, n_3) \in \{0, 1\} : m_2 = 1, 2, \cdots M_2; n_2 = 1, 2, \cdots N_2; m_3 = 1, 2, \cdots 8; n_3 = 1, 2, \cdots R(mm_3)\}$. Note that the terms above over-braces are redundancy of bits, m_3s determine the significance of corresponding bits and n_3s handle redundant bits.

Algorithm A_2 for Weighted Binary Decoding

The algorithm A_2 estimates watermark $\mathbf{W}_e$ from an extracted sequence of bits $\mathbf{W}_{ex} = \{W_{ex}(m_2, n_2, m_3, n_3) \in \{0,1\} : m_2 = 1, 2, \cdots M_2; n_2 = 1, 2, \cdots N_2; m_3 = 1, 2, \cdots 8; n_3 = 1, 2, \cdots R(mm_3)\}$. It takes an input $\mathbf{W}_{ex}$ and returns an output $\mathbf{W}_e$. In algorithm A_2, we assume that algorithm A_1 is used for encoding. The steps involve in A_2 are as follows.

Step1. Define sets $\mathbf{W}_{d1}(m_2, n_2, m_3)$s, $m_2 = 1, 2, \cdots M_2, n_2 = 1, 2, \cdots N_2, m_3 = 1, 2, \cdots 8$; $\mathbf{W}_{d1}(m_2, n_2, m_3) = \{W_{ex}(m_2, n_2, m_3, n_3) \in \{0,1\} : n_3 = 1, 2, \cdots R(mm_3)\}$.

Step2. Estimate the bits $W_{d2}(m_2, n_2, m_3)$s from the corresponding sets $\mathbf{W}_{d1}(m_2, n_2, m_3)$s using

$$W_{d2}(m_2, n_2, m_3) = \begin{cases} 0 & \text{if} \quad \phi_0(\mathbf{W}_{d1}(m_2, n_2, m_3)) > \phi_1(\mathbf{W}_{d1}(m_2, n_2, m_3)) \\ 1 & \text{else} \end{cases}; \tag{2.7}$$

where, ϕ_0 returns number of 0s, and ϕ_1 returns number of 1s.

Step3. Reconstruct watermark coefficients $W_e(m_2, n_2)$s

$$W_e(m_2, n_2) = \sum_{m_3=1}^{8} 2^{m_3-1} W_{d2}(m_2, n_2, m_3). \tag{2.8}$$

Step4. Estimate extracted watermark $\mathbf{W}_e$ of size $M_2 \times N_2$ as

$$\mathbf{W}_e = \{W_e(m_2, n_2) : m_2 = 1, 2, \cdots M_2; n_2 = 1, 2, \cdots N_2\}.$$

2.2.4 Extended Watermarking Scheme of [113] in DWT Domain: S_3

Watermarking scheme S_3 is an extended version of Kundur et al. [113]. Watermarking scheme S_3 operates in the DWT domain. The main differences between S_3 and watermarking scheme of [113] are as follows: (i) In embedding algorithm of S_3, weighted binary encoding is used to convert a face image watermark into a binary sequence; (ii) in extraction algorithm of S_3, weighted binary decoding is used to reconstruct a face image from an extracted binary sequence.

Embedding and extraction algorithms will be discussed in the following:

Embedding Algorithm of S_3

Input:

- Gray scale original image $\mathbf{I}_o$ of size $M_1 \times N_1$ as defined in section 2.2.1.
- Watermark (a face image) $\mathbf{W}_o$ of size $M_2 \times N_2$ as defined in section 2.2.1.
- Embedding locations selection key $\mathbf{ckey}_3 = \{ckey_3(m_2, n_2, m_3, n_3) \rightarrow (i, j, k); i \in \left\{1, 2, \cdots \frac{M_1}{2}\right\}; j \in \left\{1, 2, \cdots \frac{N_1}{2}\right\}; k \in \{H, V, D\}; m_2 = 1, 2, \cdots M_2; n_2 = 1, 2, \cdots N_2; m_3 = 1, 2, \cdots 8; n_3 = 1, 2, \cdots R(mm_3)$ (section 2.2.3)$\}$, where, N_w is $3 \times \frac{M_1}{2} \times \frac{N_1}{2}$ and '$\rightarrow$' denotes 'maps into'.
- Watermark embedding strength $\alpha_3 \neq 0$.

Processing:

1. Apply 1-level DWT on the image $\mathbf{I}_o$ to obtain $\hat{\mathbf{I}}$ as discussed in section 2.2.2.

2. We have embedded one bit in each position of each detailed band of the image. Therefore, number of available embedding locations for watermarking is $N_w = 3 \times \frac{M_1}{2} \times \frac{N_1}{2}$.

3. Convert $\mathbf{W}_o$ in binary form $\mathbf{W}$ by using weighted binary encoding algorithm A_1 as follows:

$$\mathbf{W} = A_1(\mathbf{W}_o, N_w).$$

4. Define $\hat{\mathbf{I}}_w = \hat{\mathbf{I}}$.

5. Update $\hat{\mathbf{I}}_w$ by embedding $\mathbf{W}$ as follows:

   (a) Compute $r(m_2, n_2, m_3, n_3)$ as follows:

$$r(m_2, n_2, m_3, n_3) = \hat{I}(ckey_3(m_2, n_2, m_3, n_3)) \mod \alpha_3;$$

   (b) Compute $b(m_2, n_2, m_3, n_3)$ as follows:

$$b(m_2, n_2, m_3, n_3) = (\hat{I}(ckey_3(m_2, n_2, m_3, n_3)) - r(m_2, n_2, m_3, n_3))/\alpha_3;$$

(c) **if**$(b(m_2, n_2, m_3, n_3) \mod 2 == 0$ AND $W(m_2, n_2, m_3, n_3) == 0)$ **then**
$\hat{I}_w(ckey_3(m_2, n_2, m_3, n_3)) \leftarrow \hat{I}(ckey_3(m_2, n_2, m_3, n_3)) - r(m_2, n_2, m_3, n_3)$

else if$(b(m_2, n_2, m_3, n_3) \mod 2 == 1$ AND $W(m_2, n_2, m_3, n_3) == 0)$ **then**
$\hat{I}_w(ckey_3(m_2, n_2, m_3, n_3)) \leftarrow \hat{I}(ckey_3(m_2, n_2, m_3, n_3)) - r(m_2, n_2, m_3, n_3) + \alpha_3$

else if$(b(m_2, n_2, m_3, n_3) \mod 2 == 0$ AND $W(m_2, n_2, m_3, n_3) == 1)$ **then**
$\hat{I}_w(ckey_3(m_2, n_2, m_3, n_3)) \leftarrow \hat{I}(ckey_3(m_2, n_2, m_3, n_3)) - r(m_2, n_2, m_3, n_3) + \alpha_3$

else if$(b(m_2, n_2, m_3, n_3) \mod 2 == 1$ AND $W(m_2, n_2, m_3, n_3) == 1)$ **then**
$\hat{I}_w(ckey_3(m_2, n_2, m_3, n_3)) \leftarrow \hat{I}(ckey_3(m_2, n_2, m_3, n_3)) - r(m_2, n_2, m_3, n_3)$
end if
where, (m_2, n_2, m_3, n_3)s are as defined in the section 2.2.4, mod is the general modulo operation such that quotient is an integer and the symbol '$\leftarrow$' represents assignment operator.

6. Apply 1-level inverse DWT followed by the floating point truncation on the updated $\hat{\mathbf{I}}_w$ to obtain the watermarked image $\mathbf{I}_w$.

Output:

Watermarked image $\mathbf{I}_w$ of size $M_1 \times N_1$ that has same format as of $\mathbf{I}_o$.

Extraction Algorithm of S_3

Input:

- An image $\mathbf{I}'$ of size $M_1 \times N_1$, as defined in section 2.2.1.
- Embedding locations selection key $\mathbf{ckey}_3$, as defined in section 2.2.4.
- Watermark embedding strength α_3, as defined in section 2.2.4.

Processing:

1. Apply 1-level DWT on the image $\mathbf{I}'$ to obtain $\hat{\mathbf{I}}'$, as discussed in section 2.2.2.
2. Use the following formula to extract watermark bits $W_{ex}(m_2, n_2, m_3, n_3)$s as follows

$$W_{ex}(m_2, n_2, m_3, n_3) = \text{roundoff}_{2\alpha_3}(\hat{I}'(ckey_3(m_2, n_2, m_3, n_3)) \mod 2\alpha_3), \quad (2.9)$$

   where,

$$\text{roundoff}_{2\alpha_3}(x) = \begin{cases} 0 & \text{if } x < \alpha_3 \\ 1 & \text{if } x \geq \alpha_3 \end{cases}, \quad (2.10)$$

   and (m_2, n_2, m_3, n_3)s are defined as in section 2.2.4.
3. Reconstruct watermark $\mathbf{W}_e$ from extracted bits $W_{ex}(m_2, n_2, m_3, n_3)$s by using weighted binary decoding.

Output:

Extracted watermark $\mathbf{W}_e$ of size $M_2 \times N_2$ that has same the format as of $\mathbf{W}_o$.

2.2.5 Extended Watermarking Scheme of [113] in RDWT Domain: S_4

Watermarking scheme S_4 is similar to the watermarking scheme S_3 except that it operates in the RDWT domain. In the following, embedding and extraction algorithms are discussed.

Embedding Algorithm of S_4

Input:

- Gray scale original image $\mathbf{I}_o$ of size $M_1 \times N_1$ as defined in section 2.2.1.
- Watermark (a face image) $\mathbf{W}_o$ of size $M_2 \times N_2$ as defined in section 2.2.1.
- Embedding locations selection key $\mathbf{ckey}_4 = \{ckey_4(m_2, n_2, m_3, n_3) \rightarrow (i, j, k); i \in \{1, 2, \cdots M_1\}; j \in \{1, 2, \cdots N_1\}; k \in \{H, V, D\}; m_2 = 1, 2, \cdots M_2; n_2 = 1, 2, \cdots N_2; m_3 = 1, 2, \cdots 8; n_3 = 1, 2, \cdots R(mm_3)$ (section 2.2.3)$\}$, where, N_w is $3 \times M_1 \times N_1$ and '$\rightarrow$' denotes 'maps into'.
- Watermark embedding strength $\alpha_4 \neq 0$.

Processing:

1. Apply 1-level RDWT on the image $\mathbf{I}_o$ to obtain $\hat{\mathbf{I}}$ as discussed in section 2.2.1.
2. We have embedded one bit in each position of each detailed band of the image. Therefore, number of available embedding locations for watermarking is $N_w = 3 \times M_1 \times N_1$.
3. Convert $\mathbf{W}_o$ in binary form $\mathbf{W}$ by using weighted binary encoding algorithm A_1 as follows:
$$\mathbf{W} = A_1(\mathbf{W}_o, N_w).$$
4. Define $\hat{\mathbf{I}}_w = \hat{\mathbf{I}}$.
5. Update $\hat{\mathbf{I}}_w$ by embedding $\mathbf{W}$ according to step 5 of embedding algorithm of S_3, where (m_2, n_2, m_3, n_3)s and embedding strength are defined as in section 2.2.5.
6. Apply 1-level inverse RDWT followed by the floating point truncation on the updated $\hat{\mathbf{I}}_w$ to obtain the watermarked image $\mathbf{I}_w$.

Output:

Watermarked image $\mathbf{I}_w$ of size $M_1 \times N_1$ that has the same format as of $\mathbf{I}_o$.

Extraction Algorithm of S_4

Input:

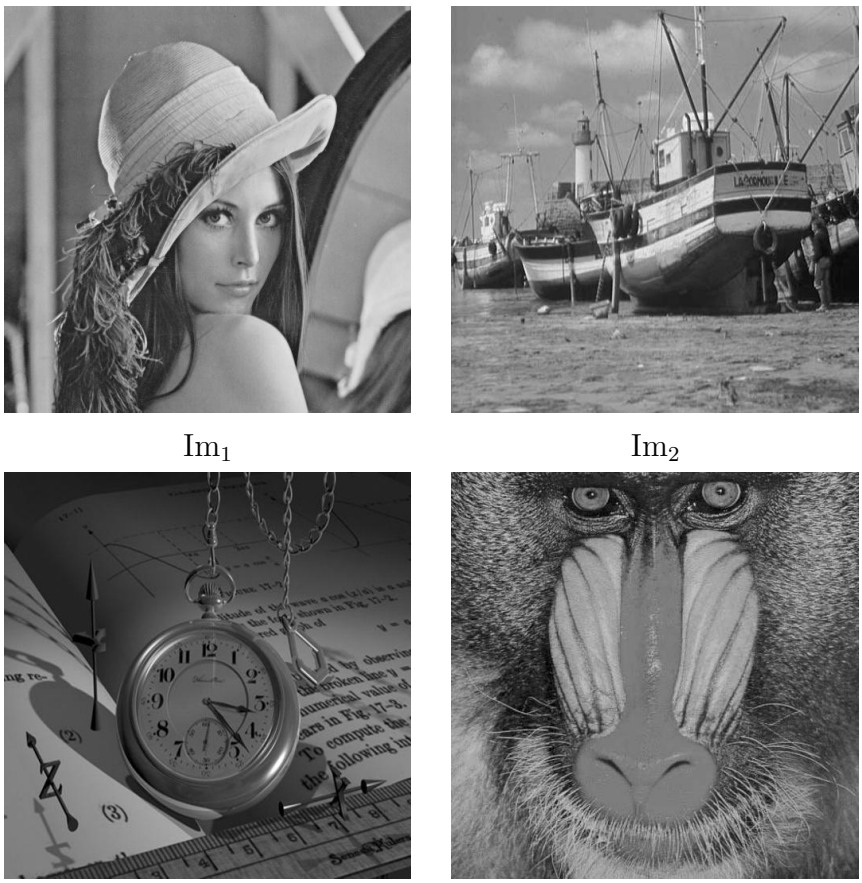
- An image $\mathbf{I}'$ of size $M_1 \times N_1$, as defined in section 2.2.1.
- Embedding locations selection key $\mathbf{ckey}_4$, as defined in section 2.2.5.
- Watermark embedding strength, α_4, as defined in section 2.2.5.

Processing:

1. Apply 1-level RDWT on the image $\mathbf{I}'$ to obtain $\hat{\mathbf{I}}'$, as discussed in section 2.2.1.
2. Use the formula (2.9) to extract watermark bits $W_{ex}(m_2, n_2, m_3, n_3)$s, where (m_2, n_2, m_3, n_3)s and embedding strength are defined as in section 2.2.5.
3. Reconstruct watermark $\mathbf{W}_e$ from extracted bits $W_{ex}(m_2, n_2, m_3, n_3)$s by using weighted binary decoding.

Output:

Extracted watermark $\mathbf{W}_e$ of size $M_2 \times N_2$ that has same format as of $\mathbf{W}_o$.



Im_1 Im_2

Im_3 Im_4

Figure 2.1: Original/host images.

2.3 Experiments, Results and Analysis

Eight experiments have been performed for a detailed analysis of the watermarking schemes S_1, S_2, S_3 and S_4. Peak-signal-to-noise-ratio (PSNR) is used to measure the quality of watermarked images. Further, PSNR and normalized correlation coefficient (NC/NCC) are used to measure the quality of extracted watermarks. Experiment 1 aims to study the effect of watermark embedding strength on the performance of watermarking schemes and to find the optimal watermark embedding strength for each watermarking scheme (S_1, S_2, S_3 and S_4). Optimal watermark embedding

W_1 W_2 W_3

Figure 2.2: Original watermarks.

strength is defined such that degradation in watermarked image is unnoticeable and distortion in corresponding extracted watermark is minimum (PSNR and NC of extracted watermark are maximum). Higher priority has been given to the quality of watermarked image. In Experiment 1, the performance of the proposed watermarking schemes has been compared with existing DWT based watermarking schemes. Experiments 2-8 analyse the performance of the proposed watermarking schemes against various common attacks/operations such as cropping, Gaussian filtering, Gaussian noise, salt and pepper noise, rotation, JPEG compression and resize respectively.

All the experiments have been performed on MATLAB platform. In the experiments, a data-set of four host/original images and three watermarks has been used. Fig. 2.1 shows all host images (Im_1, Im_2, Im_3 and Im_4) and Fig. 2.2 shows all watermarks (W_1, W_2, W_3) of the data-set. Each host image is an eight bit gray scale image of size 512×512 pixels and each watermark is an eight bit gray scale face image of size 64×64 pixels. All the combinations (a total of 12 combinations) of the host images and the watermarks have been used to obtain different watermarked images. The 'randperm' function of MATLAB is used to generate the keys $\mathbf{ckey}_1$, $\mathbf{ckey}_2$, $\mathbf{ckey}_3$ and $\mathbf{ckey}_4$. Daubechies wavelet filter of length two (db1) is used for implementing the DWT and RDWT.

2.3.1 Experiment 1: Performance of Watermarking Schemes with Watermark Embedding Strength

Performance of watermarking schemes S_1 and S_2 have been evaluated at watermark embedding strengths α_1, $\alpha_2 = 0.01, 0.02 \cdots, 0.70$ and watermarking schemes S_3 and S_4 have been evaluated at watermark embedding strengths α_3, $\alpha_4 = 0.1, 0.2, \cdots, 4.0$. Table 2.4 gives the quantitative performance of watermarking schemes for the combinations Im_1 and W_1 and, Im_2 and W_2 of host images and watermarks at various watermark embedding strength. Fig. 2.3 gives graphical comparison of the performance of watermarking schemes for the combination of Im_1 and W_1. The salient observations for each watermarking scheme are as follows.

Watermarking scheme S_1: PSNR and NC of extracted watermarks increase initially with watermark embedding strength and then become almost constant after watermark embedding strength of 0.3. PSNR of watermarked images decreases with watermark embedding strength. At watermark embedding strength of 0.3, degradation in watermarked image is unnoticeable and distortion in extracted watermark is almost the minimum. Therefore, optimal value of watermark embedding strength α_1 (α_1^*) is 0.3.

Watermarking scheme S_2: PSNR and NC of extracted watermarks increase initially, attain maximum values and then decrease with watermark embedding strength. PSNR and NC of extracted watermark attains the maximum value near watermark embedding strength of 0.28. Near $\alpha_2 = 0.28$, degradation in watermarked image is slightly noticeable. PSNR of watermarked images decreases with watermark embedding strength. It has been observed that near $\alpha_2 = 0.05$ the degradation in watermarked image is unnoticeable. Therefore, optimal value of watermark embedding strength α_2 (α_2^*) is 0.05.

Table 2.4: Quantitative performance of the watermarking schemes with respect to watermark embedding strength.

Embedding Strength	PSNR of Watermarked Image (dB)	PSNR of Extracted Watermark (dB)	NC of Extracted Watermark	PSNR of Watermarked Image (dB)	PSNR of Extracted Watermark (dB)	NC of Extracted Watermark
	Combination of Im_1 and W_1					
	Watermarking scheme S_1			Watermarking scheme S_2		
0.01	56.17	-8.44	0.0780	48.52	15.35	0.9625
0.05	53.80	2.98	0.2928	45.43	29.24	0.9985
0.1	50.06	5.16	0.4690	41.30	35.06	0.9996
0.2	44.89	5.90	0.6131	35.93	41.14	0.9999
0.3	41.53	6.05	0.6589	32.53	43.38	0.9999
0.4	39.10	6.10	0.6773	30.10	39.20	0.9998
0.5	37.17	6.12	0.6865	28.23	33.09	0.9994
0.6	35.63	6.13	0.6914	26.77	28.73	0.9985
0.7	34.30	6.14	0.6944	25.54	25.93	0.9972
	Watermarking scheme S_3			Watermarking scheme S_4		
0.3	∞	8.00	0.7746	∞	7.87	0.7629
0.4	69.06	8.34	0.7936	86.08	7.64	0.7486
0.5	57.14	12.30	0.9236	63.12	9.38	0.8450
0.6	58.00	15.89	0.9662	65.72	8.83	0.8194
1	52.37	∞	1	55.21	12.34	0.9230
1.5	49.74	40.19	0.9999	52.24	17.79	0.9785
2	47.59	∞	1	50.28	16.49	0.9707
2.5	45.82	∞	1	48.60	19.94	0.9868
3	44.33	∞	1	47.18	18.74	0.9826
3.5	43.05	64.25	1.0000	45.94	19.20	0.9844
4	41.90	∞	1	44.82	17.26	0.9757
	Combination Im_2 and W_2					
	Watermarking scheme S_1			Watermarking scheme S_2		
0.01	55.61	-9.21	0.0102	46.65	15.20	0.9194
0.05	54.48	3.60	0.1505	45.55	29.01	0.9961
0.1	52.23	7.27	0.3000	43.27	35.19	0.9991
0.2	48.06	9.08	0.4864	39.10	40.03	0.9997
0.3	44.98	9.53	0.5773	36.00	38.77	0.9996
0.4	42.65	9.70	0.6229	33.73	36.52	0.9993
0.5	40.77	9.80	0.6484	31.87	34.30	0.9989
0.6	39.27	9.84	0.6630	30.40	32.38	0.9983
0.7	37.96	9.87	0.6729	29.13	30.89	0.9976
	Watermarking scheme S_3			Watermarking scheme S_4		
0.3	∞	8.50	0.6347	∞	8.67	0.6084
0.4	68.51	9.00	0.7373	85.69	8.99	0.6870
0.5	57.22	12.33	0.8417	63.75	9.71	0.7174
0.6	57.71	15.53	0.9157	65.35	9.73	0.7348
1	52.29	∞	1	55.12	12.42	0.8361
1.5	49.66	41.31	0.9998	52.21	16.42	0.9286
2	47.52	∞	1	50.18	15.44	0.9075
2.5	45.76	∞	1	48.51	16.92	0.9351
3	44.23	∞	1	47.08	16.54	0.9289
3.5	42.93	44.42	0.9999	45.81	16.31	0.9253
4	41.80	∞	1	44.73	15.01	0.8990

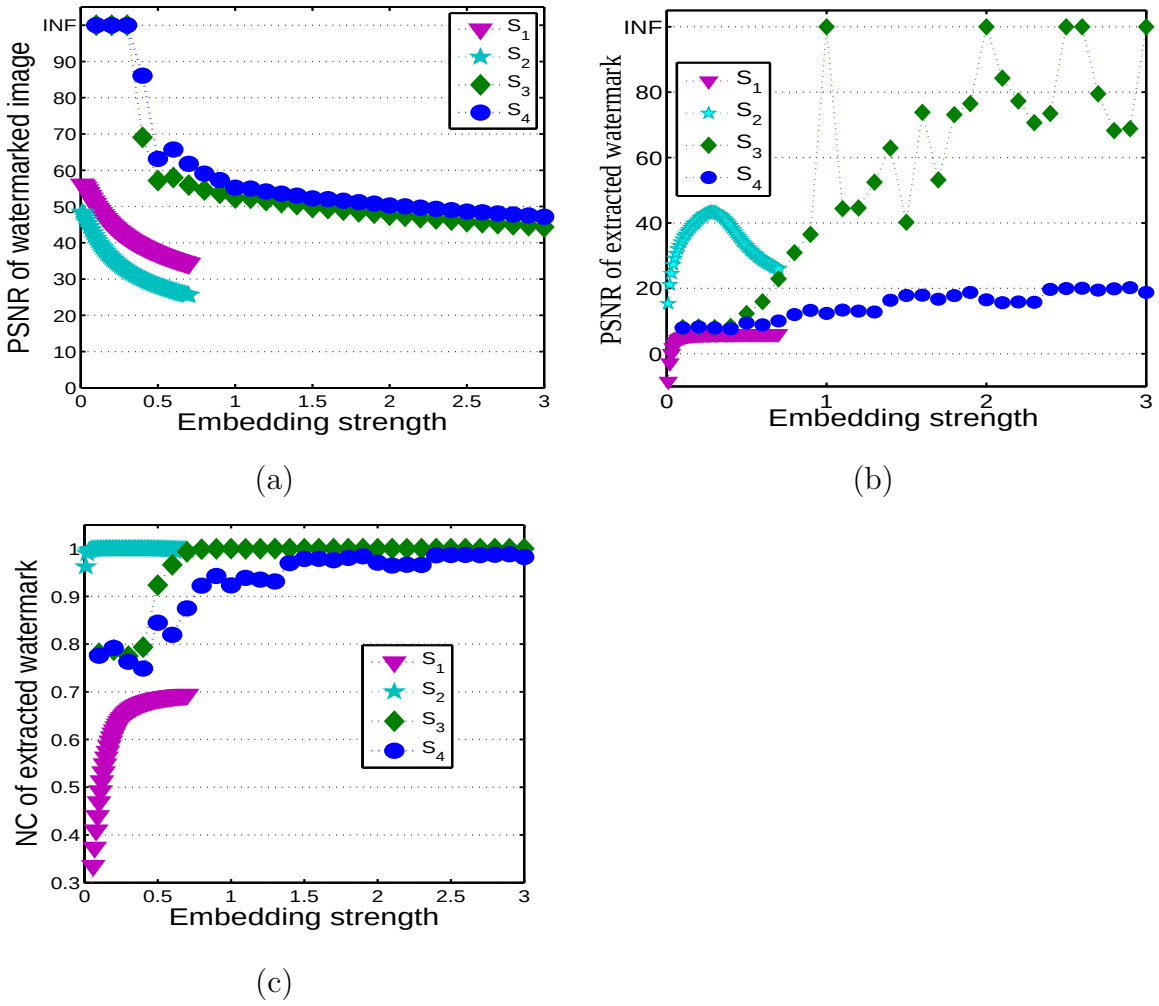


Figure 2.3: Performance of watermarking schemes (S_1, S_2, S_3 and S_4) at different values of watermark embedding strengths for the combination of Im_1 and W_1. (a): PSNRs of watermarked images. (b): PSNRs of extracted watermarks. (c): NCs of extracted watermarks.

Watermarking scheme S_3: PSNR and NC of extracted watermarks are oscillatory and attain several local and global maxima. Global maxima are attained near $\alpha_3 = 1, 2, 2.5, 2.6, 3, 3.2, 3.7, 4$. PSNR of watermarked images decreases with watermark embedding strength except watermark embedding strength range $[0.4, 0.6]$. In the watermark embedding strength (α_3) range $[0.4, 0.6]$, the PSNR of watermarked images is slightly oscillatory. Near watermark embedding strength $\alpha_3 = 1$, the degradation in watermarked image is unnoticeable and distortion in extracted watermark is global minimum. Therefore, the optimal value of watermark embedding strength α_3 (α_3^*) is 1.

Watermarking scheme S_4: PSNR and NC of extracted watermarks consist of small oscillations and attain several local maxima. The values of local maxima increase with watermark embedding strength. The PSNR of watermarked images decreases with watermark embedding strength except watermark embedding strength range $[0.4, 0.6]$. In the watermark embedding strength (α_4) range $[0.4, 0.6]$, the PSNR of watermarked images is slightly oscillatory. Near $\alpha_4 = 2.9$, degradation in watermarked image is unnoticeable and distortion in extracted watermark is local minimum and almost global minimum. Therefore, optimal value of watermark embedding strength α_4 (α_4^*) is 2.9.

Table 2.5: Quantitative results of the proposed watermarking schemes. ($\alpha_1 = 0.3$, $\alpha_2 = 0.05$, $\alpha_3 = 1$, $\alpha_4 = 2.9$)

Combination	PSNR of watermarked image (dB)				PSNR of extracted watermark (dB)				NC of extracted watermark			
	S_1	S_2	S_3	S_4	S_1	S_2	S_3	S_4	S_1	S_2	S_3	S_4
Im_1 and W_1	41.53	45.43	52.37	47.52	6.05	29.24	∞	20.20	0.6589	0.9984	1	0.9884
Im_1 and W_2	45.08	47.02	52.38	47.56	9.71	29.05	∞	19.45	0.6131	0.9962	1	0.9699
Im_1 and W_3	44.19	46.67	52.39	47.57	8.73	29.36	∞	19.86	0.6213	0.9972	1	0.9776
Im_2 and W_1	41.51	44.37	52.22	47.34	5.94	29.34	∞	16.67	0.6366	0.9985	1	0.9718
Im_2 and W_2	44.98	45.55	52.29	47.44	9.53	29.01	∞	18.05	0.5773	0.9961	1	0.9522
Im_2 and W_3	44.097	45.28	52.29	47.44	8.60	29.27	∞	17.90	0.5944	0.9971	1	0.9603
Im_3 and W_1	41.57	44.86	51.92	47.15	5.98	28.71	78.23	12.15	0.6442	0.9983	0.9999	0.9186
Im_3 and W_2	45.11	46.24	52.10	47.41	9.60	28.96	77.26	14.90	0.5923	0.9961	0.9999	0.8959
Im_3 and W_3	44.24	45.94	52.10	47.38	8.64	29.08	63.15	14.11	0.6055	0.9970	0.9999	0.9002
Im_4 and W_1	41.22	42.01	52.35	47.51	5.69	29.11	∞	19.13	0.5664	0.9984	1	0.9842
Im_4 and W_2	44.45	42.67	52.37	47.53	8.97	28.95	84.25	19.97	0.4683	0.9961	0.9999	0.9702
Im_4 and W_3	43.67	42.50	52.37	47.55	8.12	29.24	84.25	19.50	0.4911	0.9971	0.9999	0.9734

Table 2.5 provides a quantitative comparison of the proposed watermarking schemes for all 12 combinations of host image and watermark. Figs. 2.4 and 2.5 show watermarked images that correspond to the combinations of Im_1 and W_1, and, Im_2 and W_2 respectively. Fig. 2.6 shows the extracted watermarks that correspond to Figs. 2.4 and 2.5. It has been observed that watermarked images are not visually degraded (Figs. 2.4 and 2.5), the watermarks extracted using S_1 are very noisy and difficult to recognize (Fig. 2.6 (a)), the watermarks extracted using S_2 are blurred but can easily be recognized (Fig. 2.6 (b)), the watermarks extracted using S_3 are very close to original embedded watermarks (Fig. 2.6 (c)), and the watermarks extracted using S_4 are noisy but can be recognized (Fig. 2.6 (d)). The performance of watermarking schemes can be ranked as

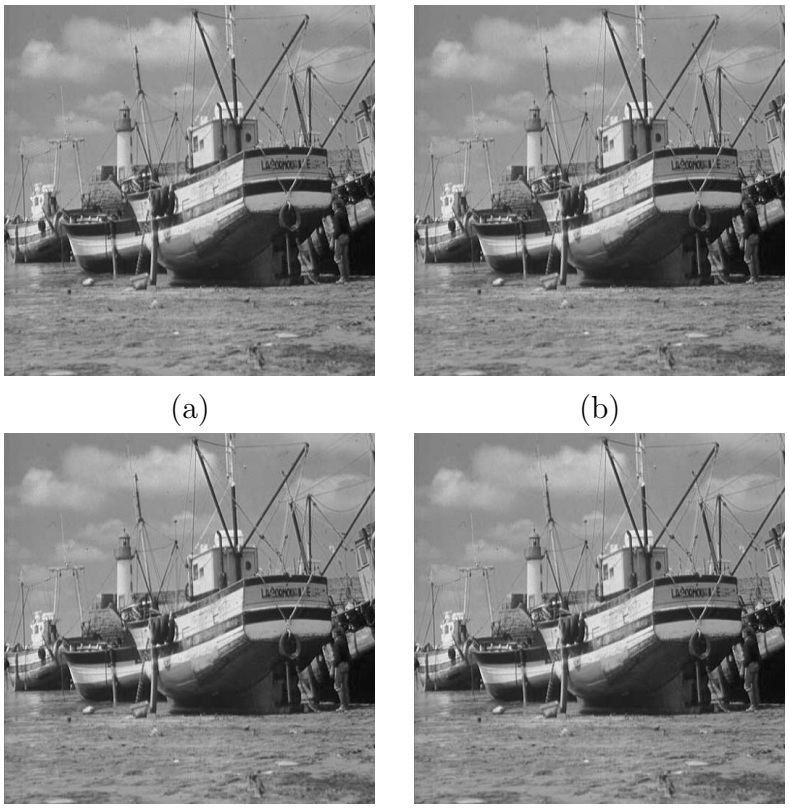
$$S_3 > S_2 > S_4 > S_1.$$

These results ensure that both DWT based watermarking schemes have secured first and second rank respectively, which proves that DWT based watermarking schemes are outperformed over RDWT based watermarking schemes. This is a breakthrough as recently Cao et al. [27], Parker et al. [161], Vatsa et al. [221], Yang et al. [240] have claimed the superiority of RDWT based watermarking schemes over DWT based watermarking schemes. For Experiment 1, the performance of watermarking scheme S_3 is the best. The use of the weighted binary coding has drastically improved the performance of watermarking schemes (compare S_3 with S_2 and S_4 with S_1).

(a) (b)

(c) (d)

Figure 2.4: Watermarked images for the combination of Im_1 and W_1. (a): Watermarking scheme S_1, $\alpha_1 = 0.3$. (b): Watermarking scheme S_2, $\alpha_2 = 0.05$. (c): Watermarking scheme S_3, $\alpha_3 = 1$. (d): Watermarking scheme S_4, $\alpha_4 = 2.9$.



(a) (b)

(c) (d)

Figure 2.5: Watermarked images for the combination of Im_2 and W_2. (a): Watermarking scheme S_1, $\alpha_1 = 0.3$. (b): Watermarking scheme S_2, $\alpha_2 = 0.05$. (c): Watermarking scheme S_3, $\alpha_3 = 1$. (d): Watermarking scheme S_4, $\alpha_4 = 2.9$.

Combination of Im_1 and W_1

Combination of Im2 and W2

(a) (b) (c) (d)

Figure 2.6: Extracted watermarks. (a): Watermarking scheme S_1, $\alpha_1 = 0.3$. (b): Watermarking scheme S_2, $\alpha_2 = 0.05$. (c): Watermarking scheme S_3, $\alpha_3 = 1$. (d): Watermarking scheme S_4, $\alpha_4 = 2.9$.

Table 2.6: Comparison of the proposed watermarking schemes with Lin et al. [124] and Ma et al. [135].

	S_1	S_2	S_3	S_4	[124]	[135]
Embedding domain	RDWT	DWT	DWT	RDWT	DWT	DWT
Category of watermarking method	Blind	Blind	Blind	Blind	Blind	Blind
Type of watermark	Face image	Face image	Face image	Face image	Face image	Binary logo
Size of host image (pixels)	512×512	512×512	512×512	512×512	560×296	512×512
Size of watermark (pixels)	64×64	64×64	64×64	64×64	8×8	32×16
Size of watermark (bits)	$64 \times 64 \times 8$ = 32,768	$64 \times 64 \times 8$ = 32,768	$64 \times 64 \times 8$ = 32,768	$64 \times 64 \times 8$ = 32,768	$8 \times 8 \times 8$ = 512	32×16 = 512
PSNR of watermarked image	41.53* dB	45.42* dB	52.37* dB	47.52* dB	44.25 dB	48.07 dB
NC of extracted watermark	0.6589*	0.9985*	1*	0.9884*	1	1

*combination of Im_1 and W_1.

Table 2.6 compares the proposed watermarking schemes with the existing DWT based watermarking schemes (Lin et al. [124] and Ma et al. [135]). The proposed watermarking scheme S_3 embeds 64 times larger watermark, maintains distortion in extracted watermark at the same level and provides a better imperceptibility in the watermarked images. The other proposed watermarking schemes (S_1, S_2 and S_4) have the advantage of large watermark size and disadvantage of distortion in extracted watermarks.

In rest of the chapter, results for the combination of Im_1 and W_1 have been reported. It has also been verified that results for the other eleven combinations of host images and watermarks are very close to the results for the combination of Im_1 and W_1.

Table 2.7: Cropping results for the combination of Im_1 and W_1 at various watermark embedding strengths.

Cropping Percentage	PSNR of watermarked image (dB)				PSNR of extracted watermark (dB)				NC of extracted watermark			
	Watermarking scheme S_1											
	α_1= 0.1	α_1= 0.25	α_1= 0.4	α_1= 0.6	α_1= 0.1	α_1= 0.25	α_1= 0.4	α_1= 0.6	α_1= 0.1	α_1= 0.25	α_1= 0.4	α_1= 0.6
10.01	15.34	15.33	15.32	15.3	4.99	5.767	5.857	5.888	0.437	0.607	0.642	0.6565
60.12	8.029	8.029	8.028	8.026	3.9	4.657	4.761	4.801	0.186	0.348	0.4	0.4252
	Watermarking scheme S_2											
	α_2= 0.1	α_2= 0.25	α_2= 0.4	α_2= 0.6	α_2= 0.1	α_2= 0.25	α_2= 0.4	α_2= 0.6	α_2= 0.1	α_2= 0.25	α_2= 0.4	α_2= 0.6
10.01	15.33	15.29	15.21	15.07	9.808	13.02	13.59	13.7	0.8705	0.9339	0.9419	0.9435
60.12	8.029	8.025	8.019	8.006	5.244	6.162	6.273	6.301	0.5346	0.6142	0.6254	0.6284
	Watermarking scheme S_3											
	α_3= 1	α_3= 2	α_3= 3	α_3= 4	α_3= 1	α_3= 2	α_3= 3	α_3= 4	α_3= 1	α_3= 2	α_3= 3	α_3= 4
10.01	15.34	15.34	15.34	15.33	15.77	15.79	15.73	15.75	0.9653	0.9654	0.9649	0.9651
60.12	8.029	8.029	8.029	8.029	6.855	6.853	6.852	6.852	0.6843	0.6841	0.684	0.684
	Watermarking scheme S_4											
	α_4= 1	α_4= 2	α_4= 3	α_4= 4	α_4= 1	α_4= 2	α_4= 3	α_4= 4	α_4= 1	α_4= 2	α_4= 3	α_4= 4
10.01	15.34	15.34	15.34	15.34	11.08	13.15	14.15	13.51	0.8937	0.9361	0.9491	0.9417
60.12	8.029	8.029	8.029	8.029	6.24	6.436	6.641	6.466	0.6245	0.648	0.6678	0.6524

2.3.2 Experiment 2: Cropping from Center

In this experiment, the center of the watermarked images has been cropped. To do so, a certain percentage of pixels from center of the watermarked images has been blackened. The used cropping percentage is approximately $10, 20, \cdots, 60$.

Table 2.7 describes the quantitative performance of the watermarking schemes S_1, S_2, S_3, and S_4 under cropping attack on the watermarked images of different watermark embedding strengths. Better PSNR/NC of extracted watermark ensures better robustness. It has been observed that the robustness of S_1 and S_2 against cropping improves with watermark embedding strength. Robustness of S_3 is constant at watermark embedding strengths of 1, 2, 3, and 4. Robustness of S_4 is maximum near watermark embedding strength of 3.

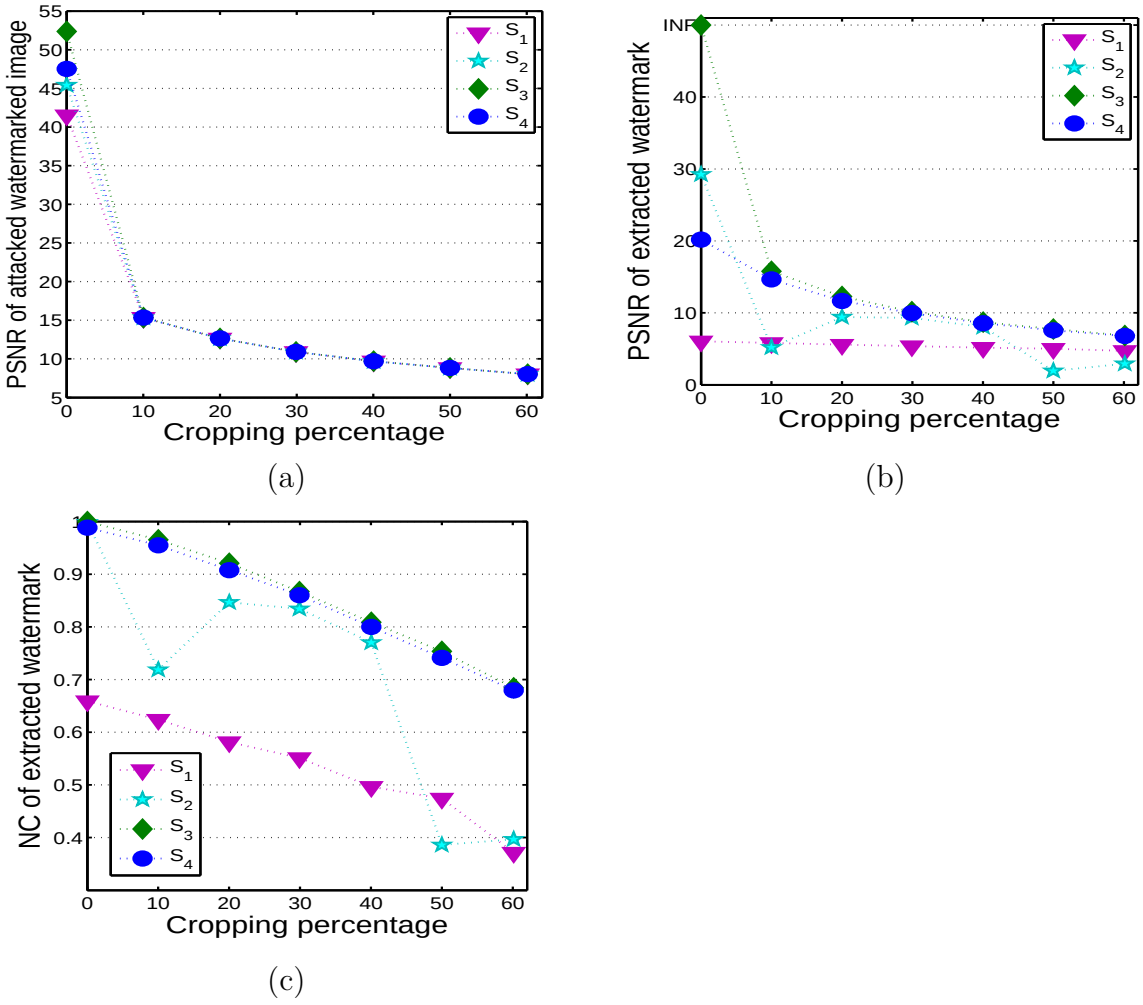


Figure 2.7: Performance of watermarking schemes (S_1, S_2, S_3 and S_4) for the combination of Im_1 and W_1 near respective optimal watermark embedding strength ($\alpha_1 = 0.3$, $\alpha_2 = 0.05$, $\alpha_3 = 1$, $\alpha_4 = 2.9$) under cropping attack on the watermarked images. (a): PSNRs of cropped watermarked images for different values of cropping percentage. (b): PSNRs of watermarks extracted from cropped watermarked images for different values of cropping percentage. (c): NCs of watermarks extracted from cropped watermarked images for different values of cropping percentage.

Fig. 2.7 gives graphical comparison of performance of the proposed watermarking schemes with respect to cropping attack on watermarked images. The salient observations from Fig. 2.7 are as follows.

Watermarking scheme S_1: PSNR and NC of extracted watermarks decrease with increase in cropping percentage. S_1 has the moderate performance except at cropping of 50%. At cropping of 50%, S_1 is better than S_2.

Watermarking scheme S_2: PSNR and NC of extracted watermarks have zigzags. S_2 under-performs S_3 and S_4 but outperforms S_1 except at cropping of 50%.

Watermarking scheme S_3: It has the best performance. PSNR and NC of extracted watermarks decrease with increase in cropping percentage.

Watermarking scheme S_4: It has the second best performance. Its performance is lower than the performance of S_3. PSNR and NC of extracted watermarks decrease with increase in cropping percentage.

Based on Fig. 2.7, the performance of watermarking schemes are ranked as

$$S_3 > S_4 > S_2 > S_1.$$

Table 2.8: Gaussian filter results for the combination of Im_1 and W_1 at various watermark embedding strengths.

Filter variance	PSNR of watermarked image (dB)				PSNR of extracted watermark (dB)				NC of extracted watermark			
	Watermarking scheme S_1											
	α_1= 0.1	α_1= 0.25	α_1= 0.4	α_1= 0.6	α_1= 0.1	α_1= 0.25	α_1= 0.4	α_1= 0.6	α_1= 0.1	α_1= 0.25	α_1= 0.4	α_1= 0.6
0.4	46.85	43.23	40.14	37.02	4.96	5.7	5.781	5.81	0.426	0.622	0.668	0.6869
1	33.38	33.36	33.33	33.27	3.79	4.245	4.298	4.316	0.077	0.17	0.252	0.3429
	Watermarking scheme S_2											
	α_2= 0.1	α_2= 0.25	α_2= 0.4	α_2= 0.6	α_2= 0.1	α_2= 0.25	α_2= 0.4	α_2= 0.6	α_2= 0.1	α_2= 0.25	α_2= 0.4	α_2= 0.6
0.3	41.3	34.14	30.28	26.93	34.88	37.82	34.56	27.54	0.9996	0.9998	0.9998	0.9985
0.5	39.55	36.65	33.88	31.05	10.73	11.09	11.07	10.86	0.9613	0.9869	0.9898	0.9897
1	33.33	33.19	32.95	32.5	4.494	4.904	4.945	4.942	0.2906	0.5808	0.7184	0.7969
	Watermarking scheme S_3											
	α_3= 1	α_3= 2	α_3= 3	α_3= 4	α_3= 1	α_3= 2	α_3= 3	α_3= 4	α_3= 1	α_3= 2	α_3= 3	α_3= 4
0.3	52.35	47.59	44.33	41.91	35.48	35.44	∞	∞	0.9996	0.9996	1	1
0.5	40.82	40.63	40.31	39.95	8.062	8.358	10.91	10.4	0.7824	0.7902	0.8892	0.8745
1	33.41	33.4	33.4	33.39	7.085	5.801	5.42	5.192	0.7075	0.5681	0.5112	0.4681
	Watermarking scheme S_4											
	α_4= 1	α_4= 2	α_4= 3	α_4= 4	α_4= 1	α_4= 2	α_4= 3	α_4= 4	α_4= 1	α_4= 2	α_4= 3	α_4= 4
0.3	55.14	50.26	47.17	44.82	12.35	16.48	18.74	17.22	0.9231	0.9706	0.9826	0.9755
0.4	48.3	47.15	45.83	44.58	9.033	11.04	13.39	10.72	0.8292	0.8926	0.939	0.8855
1	33.41	33.41	33.4	33.4	6.519	5.48	5.153	4.876	0.6552	0.519	0.4609	0.3998

2.3.3 Experiment 3: Gaussian Filtering

This experiment applies Gaussian filters of window size 3×3 and of different variance on the watermarked images. We have used different variance values as $0.1, 0.2, \cdots, 1.0$.

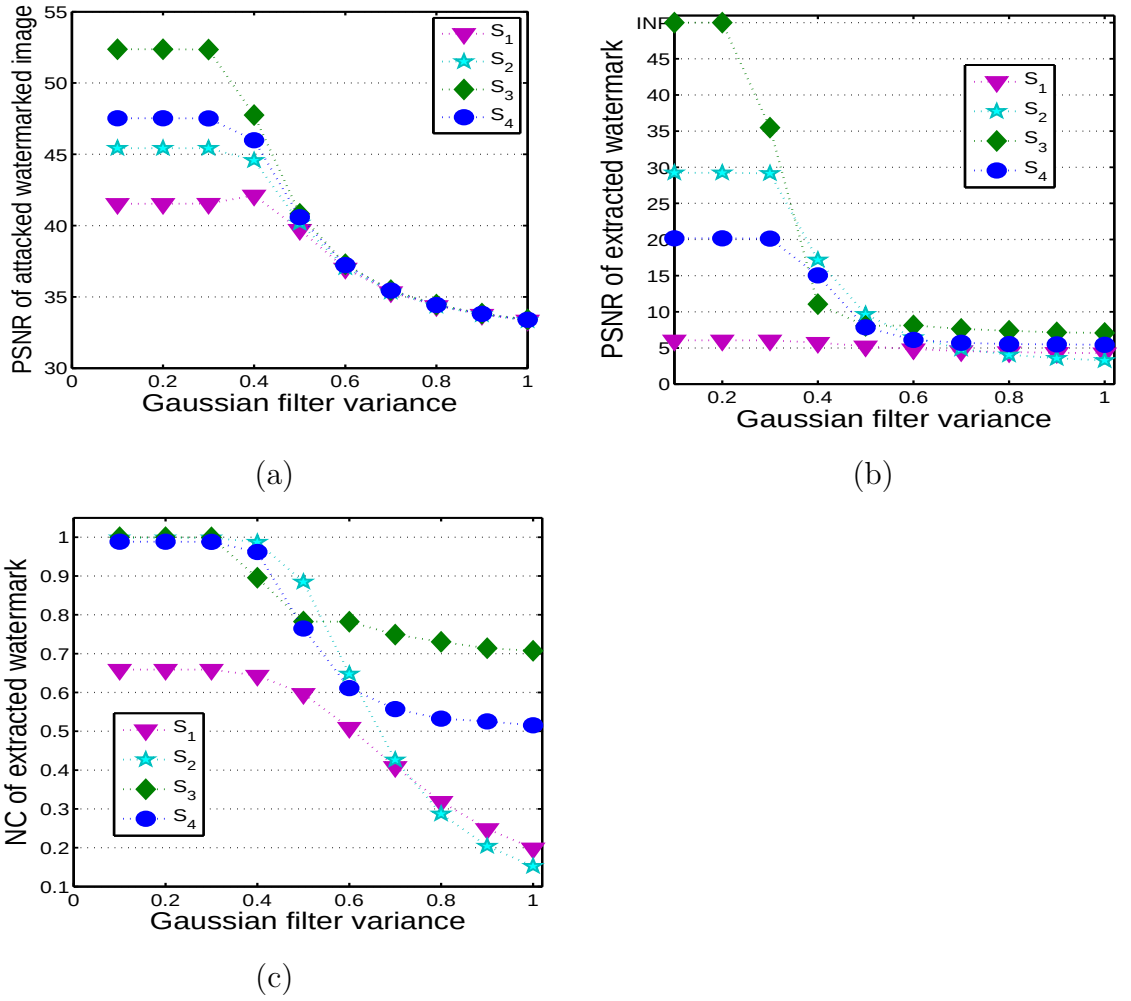


Figure 2.8: Performance of watermarking schemes (S_1, S_2, S_3 and S_4) for the combination of Im_1 and W_1 near respective optimal watermark embedding strength ($\alpha_1 = 0.3$, $\alpha_2 = 0.05$, $\alpha_3 = 1$, $\alpha_4 = 2.9$) after Gaussian filtering on watermarked images. (a): PSNRs of Gaussian filtered watermarked images for different values of Gaussian filter variance. (b): PSNRs of watermarks extracted from Gaussian filtered watermarked images for different values of Gaussian filter variance. (c): NCs of watermarks extracted from Gaussian filtered watermarked images for different values of Gaussian filter variance.

Table 2.8 describes the performance of watermarking schemes S_1, S_2, S_3, and S_4 under Gaussian filtering attack on the watermarked images of different watermark embedding strengths. It has been observed that the robustness of S_1 against Gaussian filtering improves with watermark embedding strength. Robustness of S_2 is maximum near watermark embedding strength of 0.25 till the filter variance of 0.5. Robustness of S_3 improves with watermark embedding strength till the filter variance of 0.5. Robustness of S_4 is maximum near watermark embedding strength of 3 till the filter variance of 0.4.

Fig. 2.8 gives graphical comparison of performance of the proposed watermarking schemes with respect to Gaussian filtering attack on watermarked images. The salient observations from Fig. 2.8 are as follows.

Watermarking scheme S_1: Till the Gaussian filter variance of 0.7, S_1 shows the moderate performance but after that S_1 shows the better performance than S_2. PSNR and NC of extracted watermarks decrease with increase in Gaussian filter variance.

Watermarking scheme S_2: Till the Gaussian filter variance of 0.3, S_2 has the second best performance. In Gaussian filter variance interval [0.4,0.5], S_2 has the best performance. After the variance of 0.5, performance of S_2 drops abruptly and after the variance of 0.8, the performance of S_2 is moderate. PSNR and NC of extracted watermarks decrease with increase in Gaussian filter variance.

Watermarking scheme S_3: Till the Gaussian filter variance of 0.3, the performance of S_3 is the best. At variance of 0.4, S_2 and S_4 have better performance than S_3 and at variance of 0.5, the performance of S_3 is the second best and lower than the performance of S_2. Beyond the variance of 0.5, the performance of S_3 becomes the best again. The PSNR and NC of extracted watermarks decrease with increase in Gaussian filter variance.

Watermarking scheme S_4: Till the Gaussian filter variance of 0.3, the performance of S_4 is lower than the performance of S_2 and S_3, and is better than the performance of S_1. At the variance of 0.4, the performance of S_4 is the second best and lower than the performance of S_2. In the variance interval $[0.4, 0.6]$, S_2 and S_3 have better performance. Beyond variance of 0.6, the performance of S_4 is the second best and lower than the performance of S_3. PSNR and NC of extracted watermarks decrease with increase in Gaussian filter variance.

Based on Fig. 2.8, the performance of watermarking schemes are ranked as

$$S_3 > S_2 > S_4 > S_1 \text{ when Gaussian filter variance is less than 0.4,}$$

$$S_2 > S_3 > S_4 > S_1 \text{ when Gaussian filter variance is from 0.4 to 0.5,}$$

$$S_3 > S_4 > S_1 > S_2 \text{ when Gaussian filter variance is greater than 0.6.}$$

Table 2.9: Gaussian noise results for the combination of Im_1 and W_1 at various watermark embedding strengths.

Noise variance $\times 10^{-4}$	PSNR of watermarked image (dB)				PSNR of extracted watermark (dB)				NC of extracted watermark			
	Watermarking scheme S_1											
	α_1= 0.1	α_1= 0.25	α_1= 0.4	α_1= 0.6	α_1= 0.1	α_1= 0.25	α_1= 0.4	α_1= 0.6	α_1= 0.1	α_1= 0.25	α_1= 0.4	α_1= 0.6
0.1	46.75	42.15	38.73	35.45	5.13	5.997	6.097	6.129	0.465	0.641	0.677	0.6911
1.0	39.56	38.2	36.48	34.26	5.01	5.973	6.083	6.129	0.449	0.633	0.672	0.6905
	Watermarking scheme S_2											
	α_2= 0.1	α_2= 0.25	α_2= 0.4	α_2= 0.6	α_2= 0.1	α_2= 0.25	α_2= 0.4	α_2= 0.6	α_2= 0.1	α_2= 0.25	α_2= 0.4	α_2= 0.6
0.1	40.69	33.93	30.05	26.75	28.33	36.49	37.12	28.51	0.9981	0.9997	0.9998	0.9984
1	37.57	33.05	29.68	26.58	19.72	27.74	31.31	27.59	0.9865	0.9979	0.999	0.998
	Watermarking scheme S_3											
	α_3= 1	α_3= 2	α_3= 3	α_3= 4	α_3= 1	α_3= 2	α_3= 3	α_3= 4	α_3= 1	α_3= 2	α_3= 3	α_3= 4
0.1	47.66	45.41	43.18	41.19	8.548	18.21	41.06	63.92	0.8091	0.9803	0.9999	1
1	39.69	39.25	38.6	37.82	8.136	7.838	8.644	10.41	0.7875	0.7661	0.8164	0.8788
	Watermarking scheme S_4											
	α_4= 1	α_4= 2	α_4= 3	α_4= 4	α_4= 1	α_4= 2	α_4= 3	α_4= 4	α_4= 1	α_4= 2	α_4= 3	α_4= 4
0.1	48.45	46.84	45.19	43.54	8.185	10.35	14.21	15.01	0.7891	0.873	0.9505	0.9587
1	39.82	39.57	39.2	38.74	8.001	7.937	8.38	8.834	0.7793	0.7689	0.8074	0.8173

2.3.4 Experiment 4: Gaussian Noise

This experiment adds Gaussian noise of zero mean and of different variance in the watermarked images. The used Gaussian noise variance is $10^{-5}, 2 \times 10^{-5}, \cdots, 10^{-4}$.

Table 2.9 describes the performance of watermarking schemes S_1, S_2, S_3, and S_4 under Gaussian noise addition in the watermarked images of different watermark embedding strengths. It has been observed that robustness of S_1 against Gaussian noise improves with watermark embedding strength. Robustness of S_2 is maximum near watermark embedding strength of 0.4. Robustness of S_3 and S_4 improves with watermark embedding strength.

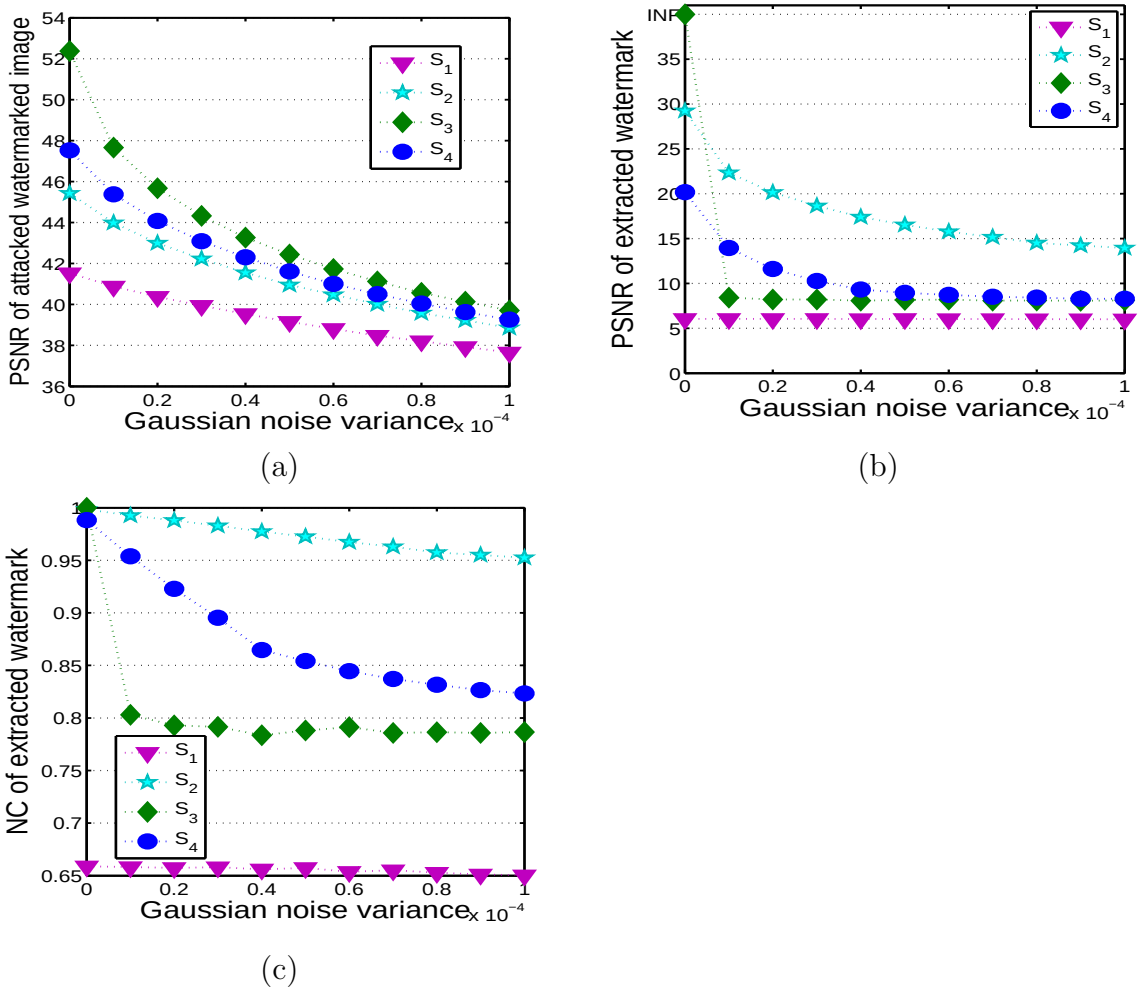


Figure 2.9: Performance of watermarking schemes (S_1, S_2, S_3 and S_4) for the combination of Im_1 and W_1 near respective optimal watermark embedding strength ($\alpha_1 = 0.3$, $\alpha_2 = 0.05$, $\alpha_3 = 1$, $\alpha_4 = 2.9$) after Gaussian noise addition in watermarked images. (a): PSNRs of Gaussian noisy watermarked images for different values of Gaussian noise variance. (b): PSNRs of watermarks extracted from Gaussian noisy watermarked images for different values of Gaussian noise variance. (c): NCs of watermarks extracted from Gaussian noisy watermarked images for different values of Gaussian noise variance.

Fig. 2.9 gives graphical comparison of performance of the proposed watermarking schemes with respect to Gaussian noise addition in the watermarked images. From Fig. 2.9, we have observed that the PSNR and NC of extracted watermarks decrease with increase in Gaussian noise. Based on Fig. 2.9, performance of the watermarking schemes are ranked as

$$S_2 > S_4 > S_3 > S_1.$$

Table 2.10: Salt & pepper noise results for the combination of Im_1 and W_1 at various watermark embedding strengths.

Noise density	PSNR of watermarked image (dB)				PSNR of extracted watermark (dB)				NC of extracted watermark			
	Watermarking scheme S_1											
	α_1= 0.1	α_1= 0.25	α_1= 0.4	α_1= 0.6	α_1= 0.1	α_1= 0.25	α_1= 0.4	α_1= 0.6	α_1= 0.1	α_1= 0.25	α_1= 0.4	α_1= 0.6
0.05	18.35	18.54	18.45	18.35	-2.404	3.183	4.649	5.442	0.116	0.293	0.395	0.514
0.95	5.662	5.671	5.665	5.668	-13.81	-6.25	-2.73	-0.19	0.002	-0.01	0.013	0.011
	Watermarking scheme S_2											
	α_2= 0.1	α_2= 0.25	α_2= 0.4	α_2= 0.6	α_2= 0.1	α_2= 0.25	α_2= 0.4	α_2= 0.6	α_2= 0.1	α_2= 0.25	α_2= 0.4	α_2= 0.6
0.05	18.42	18.32	18.24	17.91	-1.39	6.328	10.12	13.34	0.4653	0.7669	0.8838	0.9396
0.95	5.675	5.671	5.674	5.664	-13.8	-6.09	-2.55	-0.11	0.0207	0.0373	0.023	0.0274
	Watermarking scheme S_3											
	α_3= 1	α_3= 2	α_3= 3	α_3= 4	α_3= 1	α_3= 2	α_3= 3	α_3= 4	α_3= 1	α_3= 2	α_3= 3	α_3= 4
0.05	18.49	18.5	18.44	18.47	42.23	35.98	38.01	37.78	0.9999	0.9997	0.9998	0.9998
0.1	15.47	15.41	15.43	15.44	26.75	24.77	24.78	26.28	0.9973	0.9957	0.9957	0.997
0.95	5.664	5.674	5.676	5.671	4.314	4.137	7.791	4.139	0.2626	0.128	0.8536	0.1096
	Watermarking scheme S_4											
	α_4= 1	α_4= 2	α_4= 3	α_4= 4	α_4= 1	α_4= 2	α_4= 3	α_4= 4	α_4= 1	α_4= 2	α_4= 3	α_4= 4
0.05	18.44	18.4	18.47	18.38	11.5	14.39	16.08	15.29	0.9063	0.952	0.9677	0.9613
0.95	5.662	5.664	5.673	5.665	4.13	4.121	6.965	4.122	0.158	0.1288	0.8872	0.1326

2.3.5 Experiment 5: Salt and Pepper Noise

This experiment mixes salt and pepper noise of different density in the watermarked images. The used salt and pepper noise density is $0.05, 0.10, \cdots, 1.0$.

Table 2.10 describes the performance of watermarking schemes S_1, S_2, S_3, and S_4 under salt and pepper noise addition in the watermarked images of different watermark embedding strengths. We have observed that the robustness of S_1 and S_2 against salt and pepper noise improves with watermark embedding strength. Robustness of S_3 is almost constant at watermark embedding strength of 1, 2, 3 and 4. Robustness of S_4 is maximum near watermark embedding strength of 3.

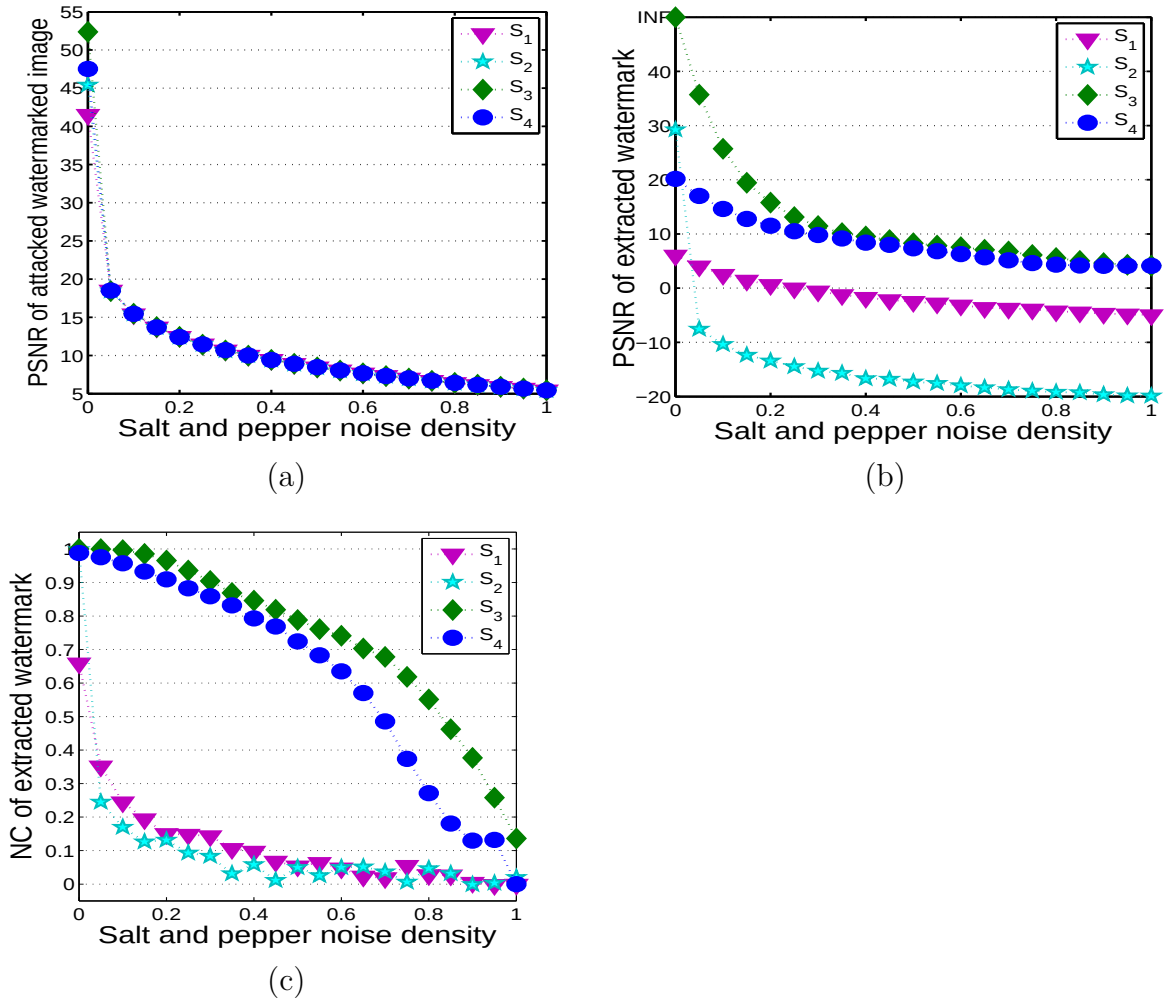


Figure 2.10: Performance of watermarking schemes (S_1, S_2, S_3 and S_4) for the combination of Im_1 and W_1 near respective optimal watermark embedding strength ($\alpha_1 = 0.3$, $\alpha_2 = 0.05$, $\alpha_3 = 1$, $\alpha_4 = 2.9$) after mixing salt and pepper noise in watermarked images. (a): PSNRs of noisy watermarked images for different values of salt and pepper noise density. (b): PSNRs of watermarks extracted from noisy watermarked images for different values of salt and pepper noise density. (c): NCs of watermarks extracted from noisy watermarked images for different values of salt and pepper noise density.

Fig. 2.10 gives graphical comparison of performance of the proposed watermarking schemes with respect to salt and pepper noise addition in the watermarked images. From Fig. 2.10, it has been observed that the PSNR and NC of extracted watermarks decrease with increase in salt and pepper noise density. PSNR and NC curves of extracted watermarks for S_1 and S_2 have small zigzags. Based on Fig. 2.10, performance of the watermarking schemes are ranked as

$$S_3 > S_4 > S_1 > S_2.$$

Table 2.11: Rotation results for the combination of Im_1 and W_1 at various watermark embedding strengths. (-: clockwise direction, no sign: counterclockwise direction.)

Rotation degree	PSNR of watermarked image (dB)				PSNR of extracted watermark (dB)				NC of extracted watermark			
	Watermarking scheme S_1											
	α_1= 0.1	α_1= 0.25	α_1= 0.4	α_1= 0.6	α_1= 0.1	α_1= 0.25	α_1= 0.4	α_1= 0.6	α_1= 0.1	α_1= 0.25	α_1= 0.4	α_1= 0.6
-10	12.27	12.27	12.26	12.25	2.368	3.745	3.95	4.03	-0.027	-0.027	-0.026	-0.024
-2	17.71	17.7	17.68	17.64	3.02	3.927	4.042	4.082	0.0109	0.0121	0.0128	0.013
2	17.95	17.93	17.91	17.88	2.829	3.901	4.04	4.088	0.0155	0.0181	0.0208	0.0234
10	12.39	12.39	12.38	12.37	2.17	3.749	3.972	4.053	0.0068	0.0073	0.0078	0.0084
	Watermarking scheme S_2											
	α_2= 0.1	α_2= 0.25	α_2= 0.4	α_2= 0.6	α_2= 0.1	α_2= 0.25	α_2= 0.4	α_2= 0.6	α_2= 0.1	α_2= 0.25	α_2= 0.4	α_2= 0.6
-10	12.26	12.24	12.2	12.14	2.834	3.815	3.944	3.993	-0.002	-0.009	-0.0142	-0.018
-2	17.7	17.62	17.48	17.22	2.958	3.817	3.932	3.978	-0.007	-0.007	-0.0063	-0.005
2	17.93	17.85	17.7	17.43	2.675	3.757	3.909	3.97	-0.014	-0.012	-0.0097	-0.007
10	12.39	12.36	12.32	12.25	2.873	3.844	3.963	4.006	0.0169	0.0082	0.0007	-0.006
	Watermarking scheme S_3											
	α_3= 1	α_3= 2	α_3= 3	α_3= 4	α_3= 1	α_3= 2	α_3= 3	α_3= 4	α_3= 1	α_3= 2	α_3= 3	α_3= 4
-10	12.27	12.27	12.26	12.26	7.75	7.502	7.76	7.436	0.7631	0.7434	0.7662	0.7369
-2	17.7	17.7	17.7	17.69	8.181	8.043	8.103	7.893	0.7906	0.7777	0.789	0.7689
2	17.94	17.94	17.93	17.92	8.09	7.935	8.126	7.912	0.7877	0.7737	0.7912	0.7697
10	12.39	12.39	12.39	12.38	7.777	7.573	7.743	7.532	0.7632	0.7454	0.7645	0.7438
	Watermarking scheme S_4											
	α_4= 1	α_4= 2	α_4= 3	α_4= 4	α_4= 1	α_4= 2	α_4= 3	α_4= 4	α_4= 1	α_4= 2	α_4= 3	α_4= 4
-10	12.27	12.27	12.27	12.26	7.777	7.575	7.825	7.138	0.7611	0.7423	0.7638	0.7079
-2	17.71	17.7	17.7	17.7	8.358	8.173	8.408	7.975	0.7987	0.784	0.8043	0.77
2	17.94	17.94	17.94	17.93	8.378	8.159	8.426	7.865	0.7989	0.782	0.8042	0.7628
10	12.39	12.39	12.39	12.39	7.833	7.526	7.81	7.067	0.7648	0.739	0.7626	0.7022

2.3.6 Experiment 6: Rotation

This experiment rotates the watermarked images in a counterclockwise direction around their center point and then crop to the size of original image. The used rotation degree is $-10, -8, \cdots, 10$.

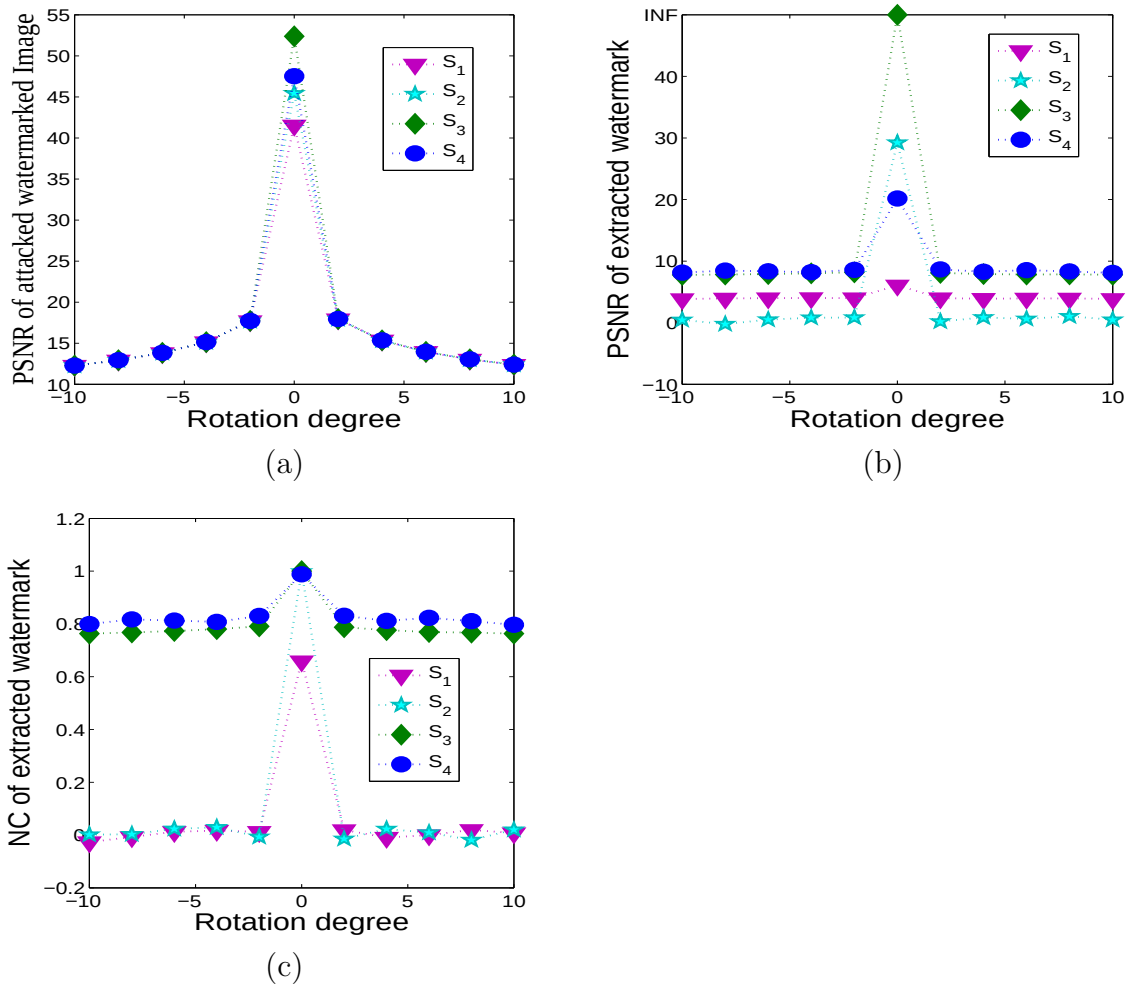


Figure 2.11: Performance of watermarking schemes (S_1, S_2, S_3 and S_4) for the combination of Im_1 and W_1 near respective optimal watermark embedding strength ($\alpha_1 = 0.3$, $\alpha_2 = 0.05$, $\alpha_3 = 1$, $\alpha_4 = 2.9$) after rotating the watermarked images. (a): PSNRs of rotated watermarked images for different values of rotation degree. (b): PSNRs of watermarks extracted from rotated watermarked images for different values of rotation degree. (c): NCs of watermarks extracted from rotated watermarked images for different values of rotation degree. (-: clockwise direction, no sign: counterclockwise direction.)

Table 2.11 describes the performance of watermarking schemes S_1, S_2, S_3, and S_4 against rotation attack on the watermarked images of different watermark embedding strengths. It has been observed that the robustness of S_1 and S_2 against rotation improves with watermark embedding strength and robustness of S_3 and S_4 is constant at watermark embedding strength of 1, 2, 3 and 4.

Fig. 2.11 gives graphical comparison of performance of the proposed watermarking schemes with respect to rotation attack on the watermarked images. From Fig. 2.11, it has been observed that the PSNR and NC of extracted watermarks decrease with increase in magnitude of rotation degree. Further, PSNR and NC of extracted watermarks are symmetrical about rotation degree of 0 (zero). Based on Fig. 2.11, performance of the watermarking schemes are ranked as

$$S_4 > S_3 > S_1 > S_2.$$

Table 2.12: JPEG compression results for the combination of Im_1 and W_1 at various watermark embedding strengths.

Quality	PSNR of watermarked image (dB)				PSNR of extracted watermark (dB)				NC of extracted watermark			
	Watermarking scheme S_1											
	α_1= 0.1	α_1= 0.25	α_1= 0.4	α_1= 0.6	α_1= 0.1	α_1= 0.25	α_1= 0.4	α_1= 0.6	α_1= 0.1	α_1= 0.25	α_1= 0.4	α_1= 0.6
1	24.25	24.24	24.24	24.24	2.915	3.915	4.049	4.098	-0.003	0.006	0.013	0.021
10	30.4	30.4	30.39	30.37	3.251	4.005	4.11	4.145	0.014	0.029	0.052	0.076
95	42.94	40.29	37.75	34.95	4.88	5.963	6.087	6.128	0.417	0.637	0.676	0.691
	Watermarking scheme S_2											
	α_2= 0.1	α_2= 0.25	α_2= 0.4	α_2= 0.6	α_2= 0.1	α_2= 0.25	α_2= 0.4	α_2= 0.6	α_2= 0.1	α_2= 0.25	α_2= 0.4	α_2= 0.6
1	24.25	24.25	24.24	24.24	3.827	4.089	4.12	4.13	0.0092	0.0222	0.0346	0.0472
80	37.6	32.97	29.13	26.12	6.586	11.52	17.57	21.16	0.6906	0.915	0.9789	0.991
95	39.26	33.54	29.87	26.67	20.45	28.65	32.19	27.85	0.9883	0.9982	0.9992	0.9981
	Watermarking scheme S_3											
	α_3= 1	α_3= 2	α_3= 3	α_3= 4	α_3= 1	α_3= 2	α_3= 3	α_3= 4	α_3= 1	α_3= 2	α_3= 3	α_3= 4
1	24.25	24.25	24.25	24.25	4.247	4.237	4.294	4.16	0.173	0.1667	0.2006	0.1039
90	40.62	40.34	39.86	39.08	7.95	6.948	7.139	7.624	0.774	0.6973	0.7119	0.7449
95	43.31	42.46	41.22	39.73	8.073	7.978	10.54	13.69	0.7843	0.7724	0.8806	0.9432
	Watermarking scheme S_4											
	α_4= 1	α_4= 2	α_4= 3	α_4= 4	α_4= 1	α_4= 2	α_4= 3	α_4= 4	α_4= 1	α_4= 2	α_4= 3	α_4= 4
1	24.25	24.25	24.25	24.25	4.18	4.21	4.264	4.224	0.1202	0.1491	0.1814	0.157
90	40.72	40.56	40.32	39.94	7.601	6.565	6.377	6.196	0.7482	0.6569	0.6398	0.6165
95	43.55	43.06	42.37	41.41	8.13	7.359	8.523	8.939	0.7841	0.7264	0.8014	0.8191

2.3.7 Experiment 7: JPEG Compression

This experiment compresses the watermarked images using JPEG compression of different image quality factor. The used image quality factor is $1, 10, 20, 30, 40, 50, 60, 70, 80, 90, 95$.

Table 2.12 describes the performance of watermarking schemes S_1, S_2, S_3, and S_4 under the JPEG compression attack on the watermarked images of different watermark embedding strengths. It has been observed that the robustness of S_1 against JPEG compression slightly improves with watermark embedding strength. Robustness of S_2 improves with watermark embedding strength till the image quality factor of 80. After this image quality factor, robustness of S_2 is maximum near

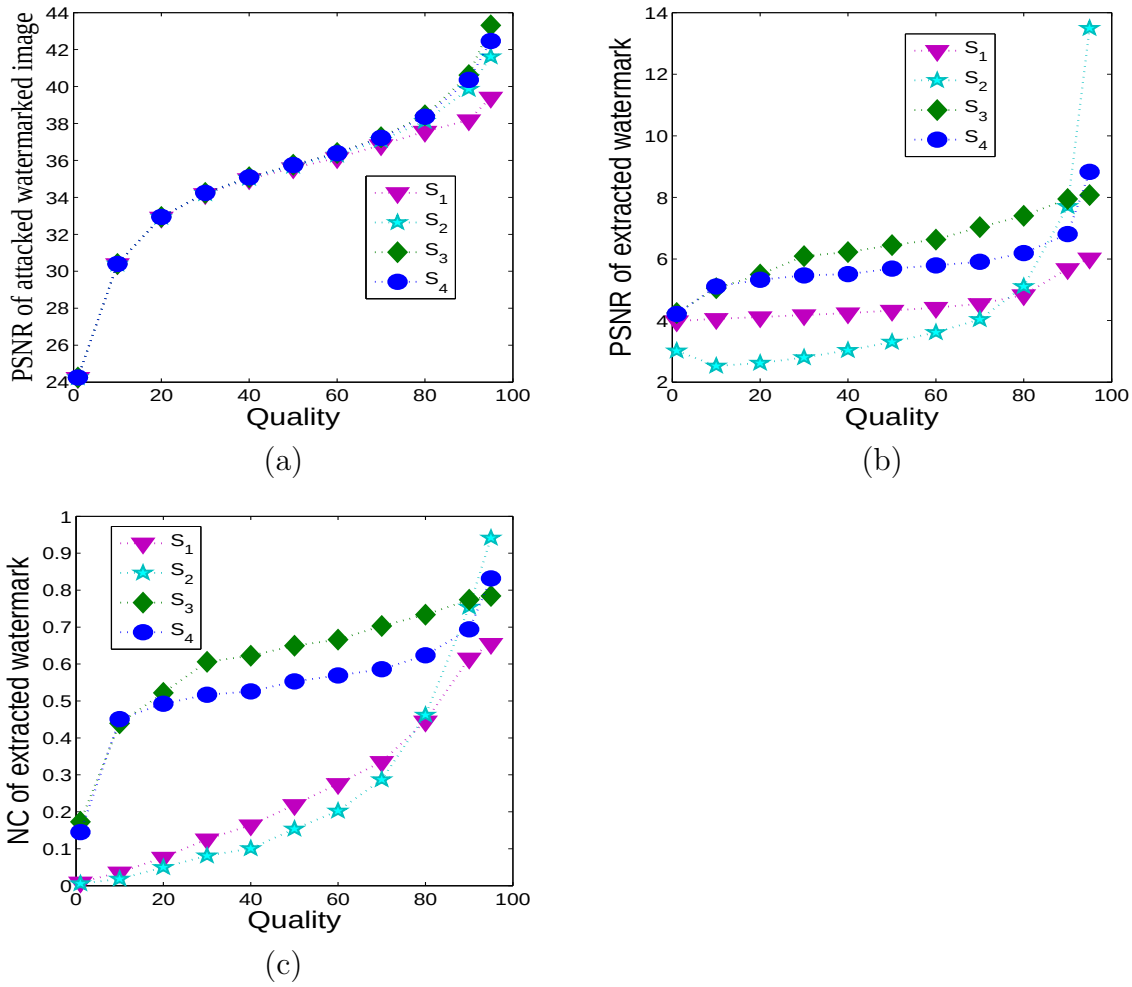


Figure 2.12: Performance of watermarking schemes (S_1, S_2, S_3 and S_4) for the combination of Im_1 and W_1 near respective optimal watermark embedding strength ($\alpha_1 = 0.3$, $\alpha_2 = 0.05$, $\alpha_3 = 1$, $\alpha_4 = 2.9$) after JPEG compression of watermarked images. (a): PSNRs of JPEG compressed watermarked images for different values of compression Quality. (b): PSNRs of watermarks extracted from JPEG compressed watermarked images for different values of compression Quality.(c): NCs of watermarks extracted from JPEG compressed watermarked images for different values of compression Quality.

the watermark embedding strength of 0.4. Robustness of S_3 is almost constant with respect to watermark embedding strength till the image quality factor of 90. After this image quality factor, robustness of S_3 improves with watermark embedding strength. Robustness of S_4 is almost constant with watermark embedding strength.

Fig. 2.12 gives graphical comparison of performance of the proposed watermarking schemes with respect to JPEG compression attack on the watermarked images. From Fig. 2.12, it has been observed that the PSNR and NC of extracted watermarks increase with increase in the JPEG compression quality. Based on Fig. 2.12, performance of watermarking schemes are ranked as

$S_3 > S_4 > S_1 > S_2$ when the JPEG compression quality is less than 80,

$S_2 > S_4 > S_3 > S_1$ when the JPEG compression quality is more than 90.

Table 2.13: Resize results for the combination of Im_1 and W_1 at various watermark embedding strengths.

Noise density	PSNR of watermarked image (dB)				PSNR of extracted watermark (dB)				NC of extracted watermark			
	Watermarking scheme S_1											
	α_1= 0.1	α_1= 0.25	α_1= 0.4	α_1= 0.6	α_1= 0.1	α_1= 0.25	α_1= 0.4	α_1= 0.6	α_1= 0.1	α_1= 0.25	α_1= 0.4	α_1= 0.6
0.1	20.32	20.31	20.31	20.31	3.95	4.092	4.109	4.115	-0.002	-0	-0	-0
0.9	39.18	38.78	38.14	37.05	4.223	4.873	4.948	4.973	0.25	0.457	0.544	0.591
	Watermarking scheme S_2											
	α_2= 0.1	α_2= 0.25	α_2= 0.4	α_2= 0.6	α_2= 0.1	α_2= 0.25	α_2= 0.4	α_2= 0.6	α_2= 0.1	α_2= 0.25	α_2= 0.4	α_2= 0.6
0.1	20.31	20.31	20.31	20.32	4.07	4.119	4.123	4.123	0.026	0.0263	0.0264	0.0268
0.9	38.51	36.35	34	31.42	7.771	8.187	8.206	8.116	0.8127	0.8867	0.8965	0.8987
	Watermarking scheme S_3											
	α_3= 1	α_3= 2	α_3= 3	α_3= 4	α_3= 1	α_3= 2	α_3= 3	α_3= 4	α_3= 1	α_3= 2	α_3= 3	α_3= 4
0.1	20.31	20.31	20.31	20.31	5.61	5.229	4.974	4.844	0.549	0.477	0.4247	0.3927
0.9	39.25	39.12	38.92	38.66	8.14	7.732	8.028	7.811	0.7837	0.7529	0.7708	0.7569
	Watermarking scheme S_4											
	α_4= 1	α_4= 2	α_4= 3	α_4= 4	α_4= 1	α_4= 2	α_4= 3	α_4= 4	α_4= 1	α_4= 2	α_4= 3	α_4= 4
0.1	20.31	20.32	20.31	20.31	5.488	5.107	4.888	4.751	0.5234	0.4511	0.4026	0.3678
0.9	39.29	39.23	39.12	38.99	7.972	6.559	6.265	5.794	0.7741	0.6559	0.6248	0.5659

2.3.8 Experiment 8: Resize

This experiment first scales down the watermarked images and then scales up to the original size. The used scale is $0.1, 0.2, \cdots, 1.0$.

Table 2.13 describes the performance of watermarking schemes S_1, S_2, S_3, and S_4 under resize attack on the watermarked images of different watermark embedding strengths. It has been observed that the robustness of S_1 against resize operation slightly improves with watermark embedding strength. Robustness of S_2 is almost maximum near the watermark embedding strength of 0.4. Robustness of S_3 and S_4 is maximum near the watermark embedding strength of 1.

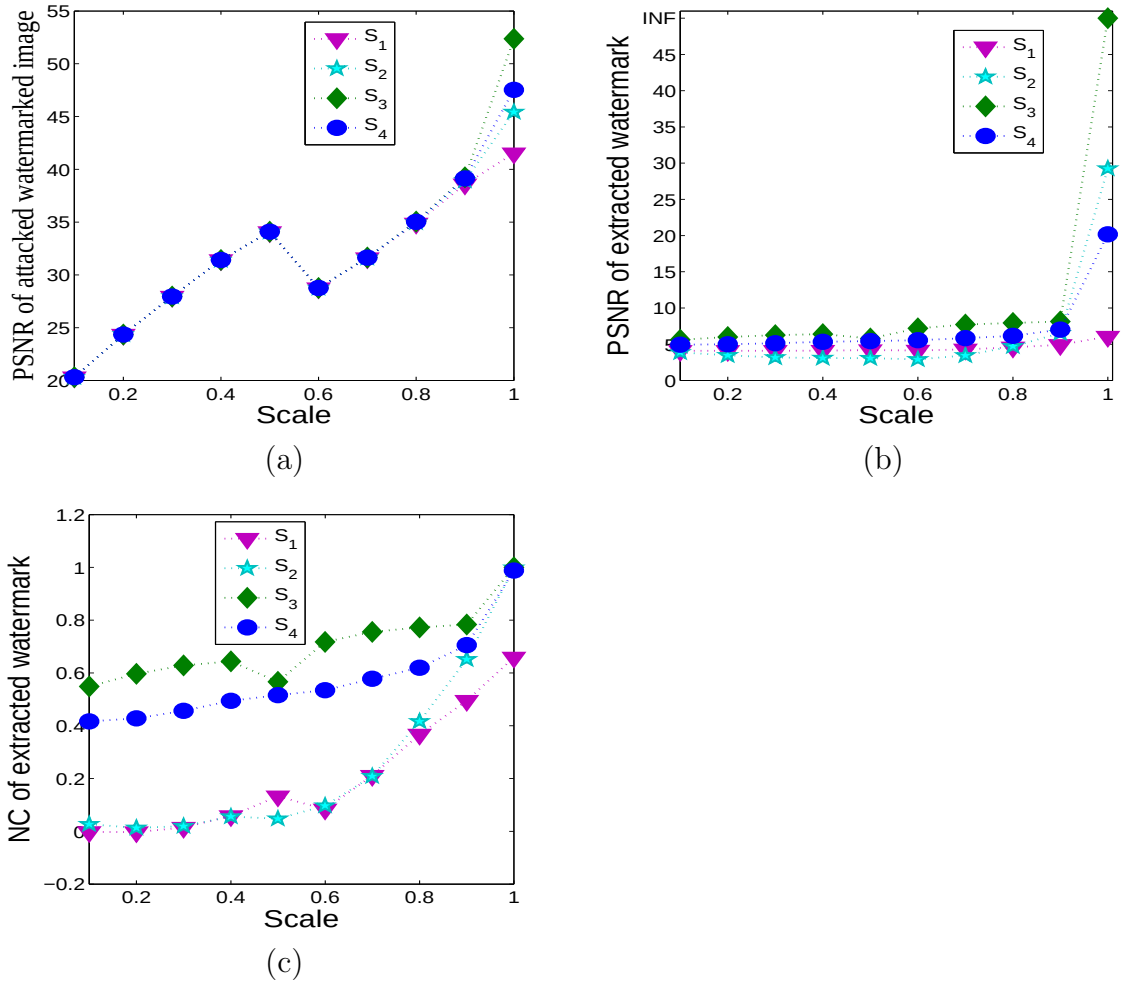


Figure 2.13: Performance of watermarking schemes (S_1, S_2, S_3 and S_4) for the combination of Im_1 and W_1 near respective optimal watermark embedding strength ($\alpha_1 = 0.3$, $\alpha_2 = 0.05$, $\alpha_3 = 1$, $\alpha_4 = 2.9$) after resizing the watermarked images. (a): PSNRs of resized watermarked images for different values of resize scale. (b): PSNRs of watermarks extracted from resized watermarked images for different values of resize scale.(c): NCs of watermarks extracted from resized watermarked images for different values of resize scale.

Fig. 2.13 gives graphical comparison of performance of the proposed watermarking schemes with respect to resize attack on the watermarked images. From Fig. 2.13, it has been observed that the PSNR and NC of extracted watermarks increase with increase in resize scale (except resize scale near 0.5). Based on Fig. 2.13, performance of watermarking schemes are ranked as

$$S_3 > S_4 > S_2 > S_1.$$

2.3.9 Comparison of PSNR and NC of Extracted Watermarks

From Fig. 2.3 and Figs. 2.7 – 2.13, the following relation has been observed between PSNR and NC of extracted watermarks.

1. PSNR of extracted watermarks increases with increase in NC and vice-versa.
2. For the high value of NC of extracted watermarks (near 0.99) the PSNR curves of extracted watermarks have better discriminative capability for performance comparison.
3. For the low value of NC, NC curves of extracted watermarks have better discriminative capability for performance comparison.

Table 2.14: Performance ranking of watermarking schemes.

Attack	S_1	S_2	S_3	S_4	First Rank
No attack	4	2	1	3	S_3 (DWT)
Cropping	4	3	1	2	S_3 (DWT)
Gaussian filter (variance < 0.4)	4	2	1	3	S_3 (DWT)
Gaussian filter (variance 0.4 to 0.5)	4	1	2	3	S_2 (DWT)
Gaussian filter (variance > 0.6)	3	4	1	2	S_3 (DWT)
Gaussian noise	4	1	3	2	S_2 (DWT)
Salt & Pepper Noise	3	4	1	2	S_3 (DWT)
Rotation	3	4	2	1	S_4 (RDWT)
JPEG Compression (Quality < 80)	3	4	1	2	S_3 (DWT)
JPEG Compression (Quality > 90)	4	1	3	2	S_2 (DWT)
Resize	4	3	1	2	S_3 (DWT)

2.4 Conclusions

In this chapter, four blind watermarking schemes have been proposed and compared. Eight bit gray scale face image has been used as a watermark. The size of watermark is 64×64 pixels ($64 \times 64 \times 8$ bits), which is 64 times larger than the size of watermark that has been used in Lin et al. [124] and Ma et al. [135].

The optimal watermark embedding strength has been found for each proposed watermarking scheme. The optimal watermark embedding strengths for S_1, S_2, S_3 and S_4 are found to be 0.3, 0.05, 1 and 2.9 respectively. We have found that without attack, watermarking scheme S_3 has the outstanding performance; PSNR value of watermarked image is more than 50 dB and PSNR and NC value of extracted watermark is ∞ dB and 1 respectively.

The performance ranking of each watermarking scheme under different scenarios (without attack, cropping, Gaussian filtering, Gaussian noise, salt and pepper noise, rotation, JPEG compression and resize) is given in table 2.14. One breakthrough is that DWT based watermarking schemes have dominated over RDWT based schemes except for rotation attack.

The weighted binary coding has drastically improved the performance of watermarking schemes compared with watermarking schemes of same transform domain. This signifies the importance of weighted binary coding.

PSNR and NC of extracted watermarks increase and decrease together. For a higher value of NC, PSNR curves provide better distinctiveness for performance comparison of watermarking schemes and vice-versa. For Gaussian noise and JPEG compression of high quality (Quality>90), the scheme S_2 has obtained the highest robustness. Further, for other attacks (except rotation) such as cropping, Gaussian filter, salt and pepper noise, resize, and JPEG compression of low quality (Quality<80), scheme S_3 has obtained the highest robustness. Scheme S_4 has the best robustness against rotation attack.

Chapter 3

Image Watermarking in Real Oriented Wavelet Transform Domain

A relation has been found, in this chapter, when the real oriented wavelet transform (ROWT) follows its left inverse. Based on this relation, two watermarking schemes have been developed in the ROWT domain for images, namely non-blind and blind watermarking schemes. Further, we have obtained special mathematical properties based on the quotient-remainder-theorem. These mathematical properties have been used in the proposed blind watermarking scheme. The proposed watermarking schemes have been compared with the existing complex wavelet transform (CWT) family based watermarking schemes and a drastic increase in the length/size of watermarks has been shown in both the proposed schemes. In the experiments, meaningful binary logos have been used as watermarks. The performance of the proposed schemes have been studied under various common image processing operations such as cropping, Gaussian filtering, Gaussian noise and salt & pepper noise. Experimental results demonstrate that the proposed schemes are more robust than the existing CWT family based watermarking schemes.

Table 3.1: Features of watermarking schemes with respect to transformed domain.

Literature	Transform	Feature
[122]	Fourier transform	robust against rotation, scale and translation
[207]	discrete cosine transform	better robustness against JPEG compression [225]
[207]	wavelet transform	better robustness against JPEG 2000 compression [203]
[101]	discrete Fourier transform and log polar map	robust against rotation, scale, translation and cropping
[218]	DCT+DWT	zero visible distortion in watermarked images

The rest of the chapter is organized as follows. In section 3.1 motivation and related work are discussed. In Section 3.2, the ROWT, its implementation on an image and its observed property are discussed. The proposed watermarking schemes are described in section 3.3. Experimental results are analyzed in section 3.4. Conclusions are provided in section 3.5.

3.1 Motivation and Related Work

According to domain in which watermark is embedded, watermarking schemes are divided into two broad categories: spatial and transformed-domain schemes. Several transformed domains are popular in watermarking. Table 3.1 provides features of various transformed domain watermarking schemes. Table 3.1 ensures that features of watermarking schemes change with respect to transformation. This fact ensures that a proper transformed domain should be selected according to a given application scenario, and, hence motivates to develop improved watermarking schemes in various transform domain.

Recently, transforms of complex wavelet family are emerged as very important multimedia processing tools. Complex wavelet integrates the phase concept of Fourier transform and multi-resolution analysis concept of wavelets. DTCWT (dual-tree-complex-wavelet-transform) is an important member of complex wavelet transforms family. An extended version of DTCWT for images is called ROWT (real-oriented-wavelet-transform) [191]. The details of complex wavelets and ROWT are discussed in section 3.2. Applications of complex wavelet transforms family have been found in estimating image geometrical structures, local displacement and motion estimation [136, 186, 191], denoising [242], image segmentation [192], seismic imaging [142], disparity estimation [111] and content based image retrieval [63, 105, 106]. In the field of watermarking, researchers have developed various watermarking schemes in a domain of complex wavelet transform (CWT) family [37, 133, 213, 239]. However, small watermark length/size is a major limitation in all the existing CWT family based watermarking schemes. A main reason for this limitation may be that the left inverse and the right inverse of family members of CWT are not equal.

Table 3.2: List of symbols used in section 3.2.

ROWT	real oriented wavelet transform.
ϕ_h	real scaling function.
ϕ_g	imaginary scaling function.
ψ_h	real wavelet function.
ψ_g	imaginary wavelet function.
h_0	analysis filter corresponds to scaling function ϕ_h.
h_1	analysis filter corresponds to wavelet function ψ_h.
g_0	analysis filter corresponds to scaling function ϕ_g.
g_1	analysis filter corresponds to wavelet function ψ_h.
$\tilde{h}_0$	synthesis filter corresponds to scaling function ϕ_h.
$\tilde{h}_1$	synthesis filter corresponds to wavelet function ψ_h.
$\tilde{g}_0$	synthesis filter corresponds to scaling function ϕ_g.
$\tilde{g}_1$	synthesis filter corresponds to wavelet function ψ_h.

3.2 ROWT and its Observed Property

In this section, ROWT and its implementation on gray scale image are discussed followed by the observed property of the ROWT. A list of symbols used in this section is defined in table 3.2.

3.2.1 ROWT

Selesnick et al. [191] defined the complex wavelet function and the complex scaling function as follows:

$$\psi_c(t) = \psi_h(t) + \mathrm{j}\psi_g(t) \tag{3.1}$$

$$\phi_c(t) = \phi_h(t) + \mathrm{j}\phi_g(t) \tag{3.2}$$

where, $\psi_c(t)$ is an analytic function, i.e. $\psi_g(t) = \mathcal{H}[\psi_h(t)]$, $\mathcal{H}[.]$ is the Hilbert transform operator, ϕ_h is the scaling function that corresponds to the wavelet ψ_h, ϕ_g is the scaling function that corresponds to the wavelet ψ_g and j is the square root of -1.

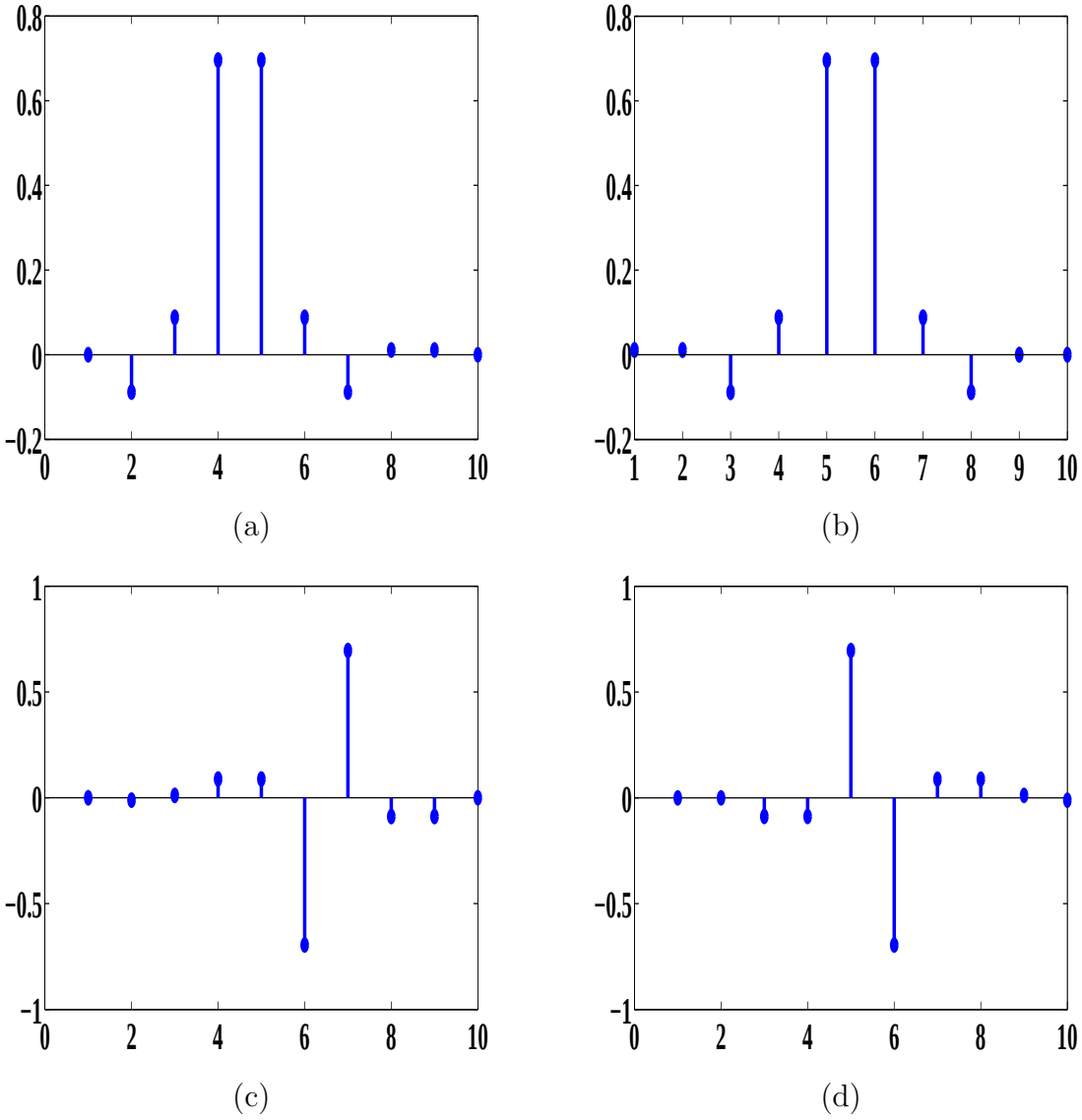


Figure 3.1: Analysis filter bank for decomposition of image/signal [190, 191]. (a) Real scaling analysis filter h_0 that corresponds to ϕ_h. (b) Imaginary scaling analysis filter g_0 that corresponds to ϕ_g. (c) Real wavelet analysis filter h_1 that corresponds to ψ_h. (d) Imaginary wavelet analysis filter g_1 that corresponds to ψ_g.

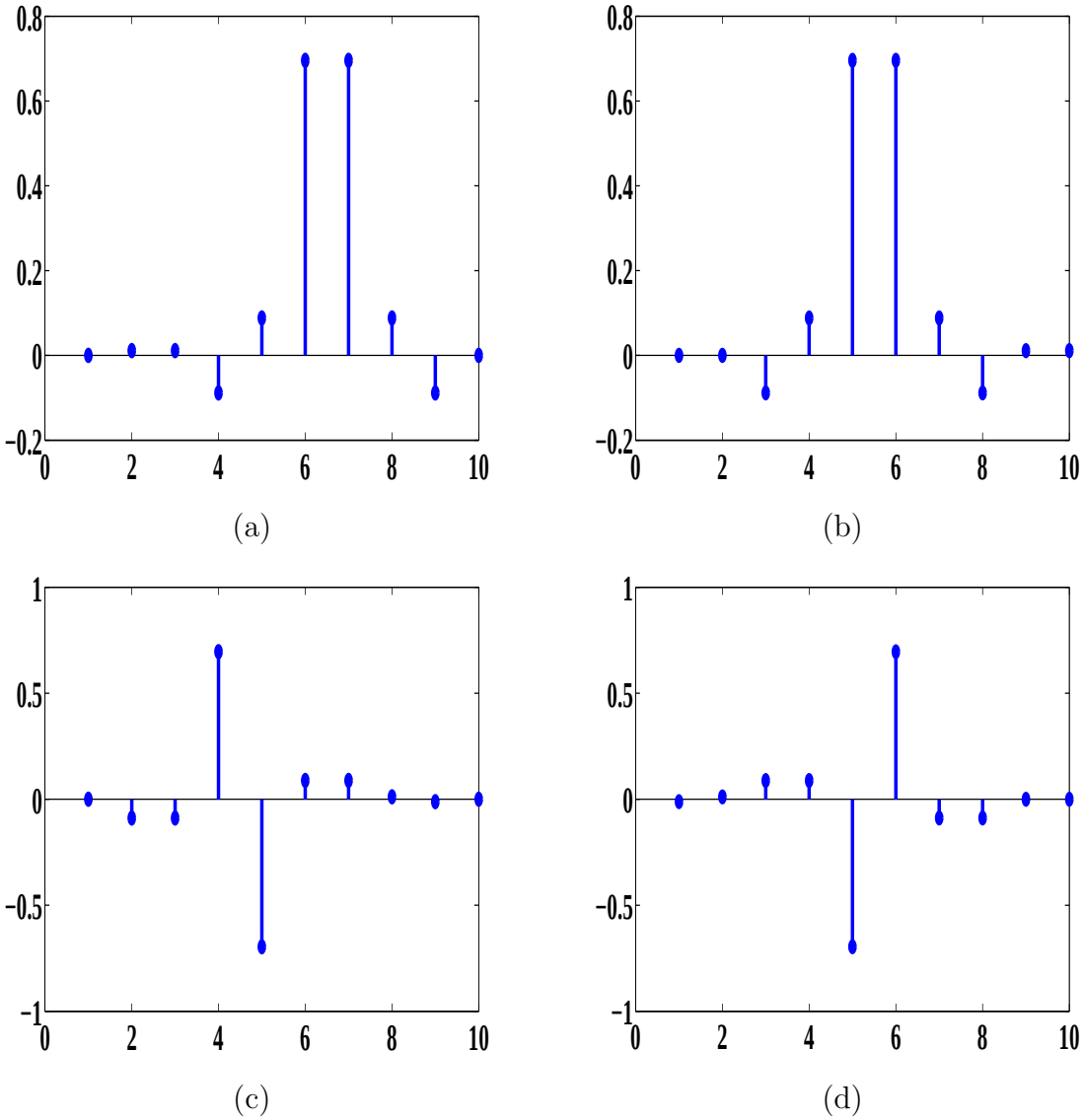


Figure 3.2: Synthesis filter bank for reconstruction of image/signal [190, 191]. (a) Real scaling synthesis filter $\tilde{h}_0$ that corresponds to ϕ_h. (b) Imaginary scaling synthesis filter $\tilde{g}_0$ that corresponds to ϕ_g. (c) Real wavelet synthesis filter $\tilde{h}_1$ that corresponds to ψ_h. (d) Imaginary wavelet synthesis filter $\tilde{g}_1$ that corresponds to ψ_g.

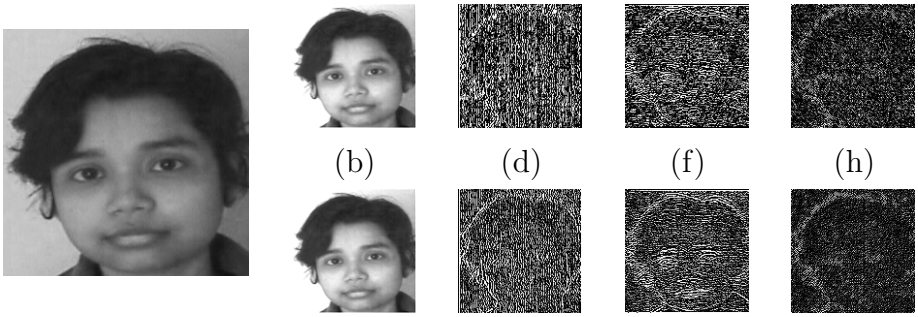


Figure 3.3: The ROWT of an image (a). (a): a sample image, (b): sub-band A_1 that corresponds to ϕ_1, (c): sub-band A_2 that corresponds to ϕ_2, (d): sub-band P_V that corresponds to ψ_1, (e): sub-band N_V that corresponds to ψ_4, (f): sub-band P_H that corresponds to ψ_2, (g): sub-band N_H that corresponds to ψ_5, (h): sub-band P_D that corresponds to ψ_3 (i): sub-band N_D that corresponds to ψ_6.

The ROWT consists of six real-oriented 2D wavelets that are defined as follows,

$$\psi_l(x,y) = \frac{1}{\sqrt{2}}(\psi_{1,l}(x,y) + \psi_{2,l}(x,y)), \tag{3.3}$$

$$\psi_{l+3}(x,y) = \frac{1}{\sqrt{2}}(\psi_{1,l}(x,y) - \psi_{2,l}(x,y)), \tag{3.4}$$

where $l = 1, 2, 3$,

$$\psi_{1,1}(x,y) = \phi_h(x)\psi_h(y), \quad \psi_{2,1}(x,y) = \phi_g(x)\psi_g(y),$$

$$\psi_{1,2}(x,y) = \psi_h(x)\phi_h(y), \quad \psi_{2,2}(x,y) = \psi_g(x)\phi_g(y),$$

$$\psi_{1,3}(x,y) = \psi_h(x)\psi_h(y), \quad \psi_{2,3}(x,y) = \psi_g(x)\psi_g(y),$$

and two scaling functions that are defined as follows,

$$\phi_1(x,y) = \phi_h(x)\phi_h(y), \quad \phi_2(x,y) = \phi_g(x)\phi_g(y).$$

The factor $1/\sqrt{2}$ in (3.3)-(3.4) is the normalization factor that is used to make the sum/difference operations as orthonormal operations. The ROWT has been implemented on an image using two fast-wavelet-transforms (FWT) [64, 138, 191] in parallel. The analysis filter bank (Fig. 3.1) of the ROWT is used to decompose

Algorithm 1 Algorithm for 1-level forward ROWT

Input: An image I of size $M \times N$ pixels, analysis filters h_0, h_1, g_0, g_1. ▷ See table 3.2 for detailed explanation of symbols.

Output: decomposed sub-bands, A_1, A_2, P_H, P_V, P_D, N_H, N_V and N_D each of size $\frac{M}{2} \times \frac{N}{2}$ pixels.

1: Convolute I in parallel with h_0, h_1, g_0 and g_1 along columns followed by down-sampling of factor 2 along columns. Store the results as I_1, I_2, I_3 and I_4 respectively.

2: Convolute I_1 in parallel with h_0 and h_1 along rows followed by down-sampling of factor 2 along rows. Store the results as I_{Ah} and I_{Hh} respectively.

3: Convolute I_2 in parallel with h_0 and h_1 along rows followed by down-sampling of factor 2 along rows. Store the results as I_{Vh} and I_{Dh} respectively.

4: Convolute I_3 in parallel with g_0 and g_1 along rows followed by down-sampling of factor 2 along rows. Store the results as I_{Ag} and I_{Hg} respectively.

5: Convolute I_4 in parallel with g_0 and g_1 along rows followed by down-sampling of factor 2 along rows. Store the results as I_{Vg} and I_{Dg} respectively.

6: Assign:

$$A_1 \leftarrow I_{Ah};$$

$$A_2 \leftarrow I_{Ag}.$$

7: Compute:

$$P_H = \frac{1}{\sqrt{2}}(I_{Hh} + I_{Hg});$$

$$N_H = \frac{1}{\sqrt{2}}(I_{Hh} - I_{Hg});$$

$$P_V = \frac{1}{\sqrt{2}}(I_{Vh} + I_{Vg});$$

$$N_V = \frac{1}{\sqrt{2}}(I_{Vh} - I_{Vg});$$

$$P_D = \frac{1}{\sqrt{2}}(I_{Dh} + I_{Dg});$$

$$N_D = \frac{1}{\sqrt{2}}(I_{Dh} - I_{Dg}).$$

8: **Return** Eight decomposed sub-bands A_1, A_2, P_H, P_V, P_D, N_H, N_V and N_D each of size $\frac{M}{2} \times \frac{N}{2}$ pixels.

Algorithm 2 Algorithm for 1-level inverse ROWT

Input: Eight decomposed sub-bands A_1, A_2, P_H, P_V, P_D, N_H, N_V and N_D each of size $\frac{M}{2} \times \frac{N}{2}$ pixels, synthesis filters $\tilde{h}_0$, $\tilde{h}_1$, $\tilde{g}_0$, $\tilde{g}_1$. ▷ See table 3.2 for detailed explanation of symbols.

Output: Reconstructed image I of size $M \times N$ pixels.

1: Compute:

$$I_{Hh} = \frac{1}{\sqrt{2}}(P_H + N_H);$$

$$I_{Hg} = \frac{1}{\sqrt{2}}(P_H - N_H);$$

$$I_{Vh} = \frac{1}{\sqrt{2}}(P_V + N_V);$$

$$I_{Vg} = \frac{1}{\sqrt{2}}(P_H - N_H);$$

$$I_{Dh} = \frac{1}{\sqrt{2}}(P_D + N_D);$$

$$I_{Dg} = \frac{1}{\sqrt{2}}(P_D - N_D).$$

2: Assign:

$$I_{Ah} \leftarrow A_1$$

$$I_{Ag} \leftarrow A_2.$$

3: Convolute I_{Hh} and I_{Dh} with $\tilde{h}_1$ along rows succeeded by up-sampling of factor 2 along rows. Store the results as I_1 and I_2 respectively.

4: Convolute I_{Hg} and I_{Dg} with $\tilde{g}_1$ along rows succeeded by up-sampling of factor 2 along rows. Store the results as I_3 and I_4 respectively.

5: Convolute I_{Vh} and I_2 with $\tilde{h}_1$ along columns succeeded by up-sampling of factor 2 along columns. Store the results as I_5 and I_6 respectively.

6: Convolute I_{Vg} and I_4 with $\tilde{g}_1$ along columns succeeded by up-sampling of factor 2 along columns. Store the results as I_7 and I_8 respectively.

7: Convolute I_{Ah} and I_1 with $\tilde{h}_0$ along columns succeeded by up-sampling of factor 2 along columns. Store the results as I_9 and I_{10} respectively.

8: Convolute I_{Ag} and I_3 with $\tilde{g}_0$ along columns succeeded by up-sampling of factor 2 along columns. Store the results as I_{11} and I_{12} respectively.

9: Convolute I_5 and I_9 with $\tilde{h}_0$ along rows succeeded by up-sampling of factor 2 along rows. Store the results as I_{13} and I_{14} respectively.

10: Convolute I_7 and I_{11} with $\tilde{g}_0$ along rows succeeded by up-sampling of factor 2 along rows. Store the results as I_{15} and I_{16} respectively.

11: Compute $y_1 = I_6 + I_{10} + I_{13} + I_{14}$.

12: Compute $y_2 = I_8 + I_{12} + I_{15} + I_{16}$.

13: Compute $I = (y_1 + y_2)/\sqrt{2}$.

14: **Return** Reconstructed image I of size $M \times N$ pixels.

an image into eight sub-bands and synthesis filter bank (Fig. 3.2) of the ROWT is used to reconstruct back the image from its decomposed sub-bands. The details of one-level forward ROWT and one-level inverse ROWT are discussed in the algorithms 1 and 2 respectively.

One-level implementation of the ROWT [190, 191] on a sample gray scale image is shown in Fig. 3.3. The size of the sample image is 256×256 pixels and size of each decomposed sub-band is 128×128 pixels. Note that the sub-bands A_1 and A_2 are called approximation sub-bands, the sub-bands P_V, P_H and P_D are called positive sub-bands, and the sub-bands N_V, N_H and N_D are called negative sub-bands.

3.2.2 Observed Property of ROWT

Let A_1 and A_2 be the approximation sub-bands and $P_\theta s$ and $N_\theta s$ be the positive and negative sub-bands respectively obtained from an image I on applying the ROWT [190, 191] on it , where $\theta = H, V$ and D. Modify $P_\theta s$ and $N_\theta s$ as follows:

$$P'_\theta = P_\theta + Q_1 \tag{3.5}$$

$$N'_\theta = N_\theta + Q_2 \tag{3.6}$$

where, Q_1 and Q_2 are two real matrices that have a size, equal to the size of P_θs and N_θs. Let I' be the reconstructed image by applying the inverse ROWT on A_1, A_2, P'_θs and N'_θs sub-bands. Let P''_θs and N''_θs be the positive and negative sub-bands respectively obtained from I' by applying the ROWT on it. Then the following two relations have been observed:

$$P''_\theta + N''_\theta = P_\theta + N_\theta + Q_1 \quad \text{if } Q_2 = Q_1, \tag{3.7}$$

$$P''_\theta - N''_\theta = P_\theta - N_\theta + Q_1 \quad \text{if } Q_2 = -Q_1. \tag{3.8}$$

A numerical example has been provided in Fig. 3.4 to elaborate and verify the observed property of the ROWT. Fig. 3.4 reports a small mismatch in the

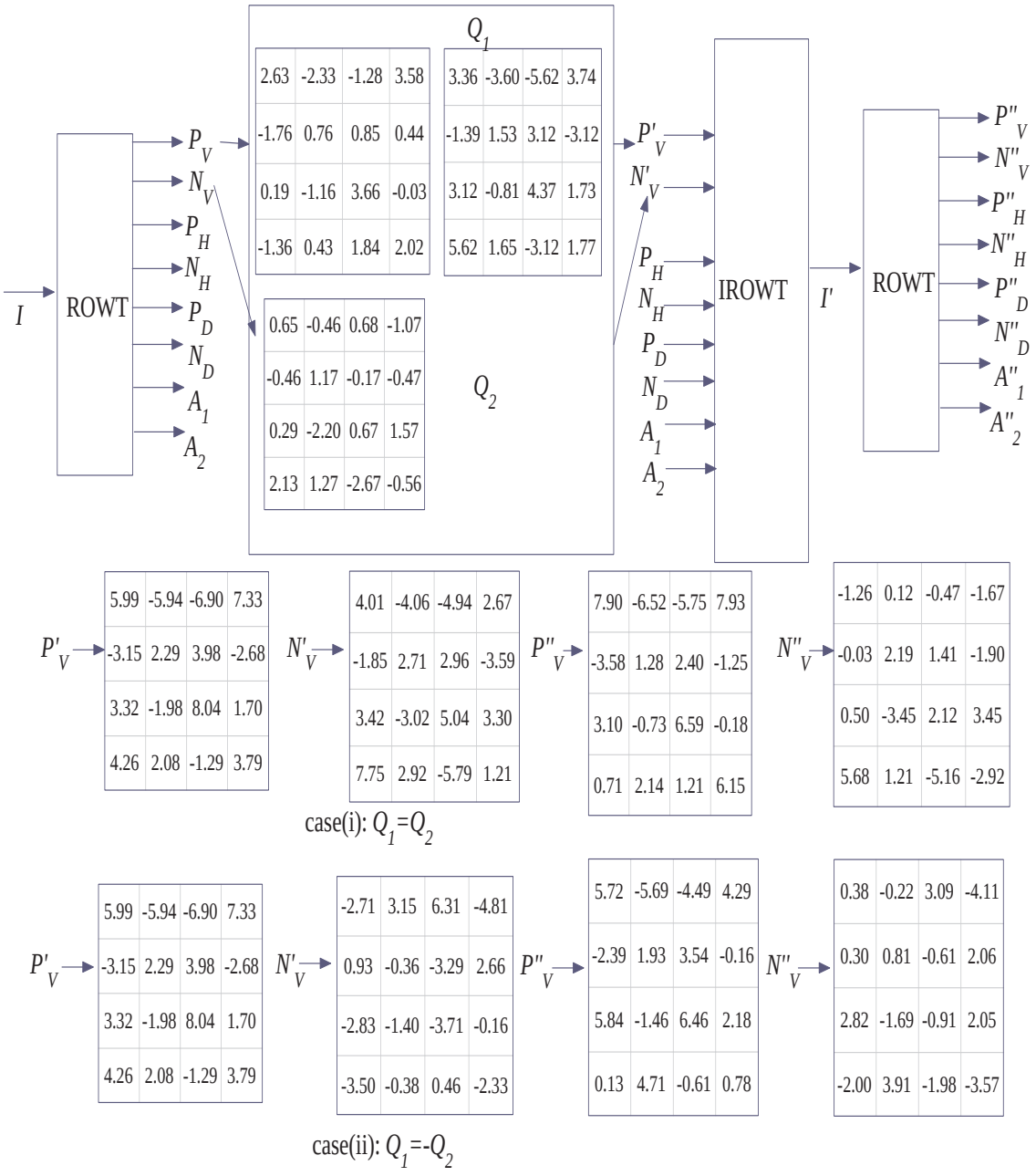


Figure 3.4: Illustration of the observed property of the ROWT using numerical example.

observed property. This small mismatch may be due to the truncation error in data representation and transform implementation. Note that inverse ROWT (algorithm 2) followed by ROWT (algorithm 1) does not make an identity transform. This situation is very different than the DCT, DWT and other transforms, wherein, inverse of a transform followed by itself makes an identity transform. This main difference between the ROWT and other transforms emphasizes the need for significant changes to the conventional watermarking models. In this chapter, the observed property of the ROWT is used as a building block in the proposed watermarking schemes.

3.3 Watermarking Schemes

This section is divided into two sections: non-blind watermarking schemes (section 3.3.1) and blind watermarking schemes (section 3.3.2). In section 3.3.1, a traditional non-blind watermarking scheme, proposed non-blind watermarking scheme in the ROWT domain and the watermark estimation rules from extracted watermark bits are discussed. In section 3.3.2, a traditional blind watermarking scheme and proposed blind watermarking scheme in the ROWT domain are discussed. A list of symbols used in section 3.3 is explained in table 3.3.

3.3.1 Non-blind Watermarking Schemes

A watermark embedding algorithm and the corresponding watermark extraction algorithm of a traditional non-blind watermarking scheme are explained in algorithms 3 and 4 respectively. A numerical example is provided in Fig. 3.5 to illustrate the traditional non-blind watermarking scheme.

Table 3.3: List of symbols used in section 3.3.

I_o	Original image
W_o	Original watermark
α	Watermarking strength
δ	error controller, a parameter in the proposed blind watermark embedding algorithm, which controls error rate in extracted watermarks.
k	$\in \{1, 2\}$, used as a sub-key in the proposed watermarking algorithm.
G	a map such that $G : \{P, N\} \to \{-1, 1\}$, used as a sub-key in the proposed watermarking algorithm.
P,N (regular text/ superscript/ subscript)	represent a positive, a negative sub-band respectively of a ROWT transformed image.
Subscripts H, V, D	represent a horizontal, a vertical, a detailed sub-band respectively of a ROWT transformed image.
A (regular text or superscript)	represents an approximate sub-band of a ROWT transformed image.
I_W	Watermarked image
I_w	an image, from which watermark is to be extracted (may be watermarked, attacked, unmarked).
W	a temporary variable used to store extracted bits.
W_e/W_e^is	Extracted watermark(s)
$M_1 \times N_1$	size of original/watermarked image (pixels)
$M_2 \times N_2$	size of original/extracted watermark (pixels)
L_1	A set of watermarking pixels from a domain (spatial/transformed) of the I_o, where, watermark is embedded/ from I_W/I_w, from where, watermark is to be extracted.
L_2	Set of all pixels in the $W_o/W_e/W_e^is$.
l_1	a pixel from the L_1.
l_2	a pixel from the L_2 corresponds to the l_1.
π	a map that associates each l_1 with a l_2.
$I_o(l_1)$	the pixel/coefficient value of the I_o at the l_1.
$W_o(l_2)$	the pixel value of the W_o at the l_2.
$I_W(l_1)$	pixel/coefficient value of the I_W at the l_1.
$W_e(l_2)$	pixel value of the W_e at the l_2.

Algorithm 3 A traditional non-blind watermark embedding algorithm in transform domain [39, 114].

Input: I_o, W_o, α, L_1, π, and a transform T and its inverse T^{-1}. ▷ See table 3.3 for detailed explanation of each symbol.

Output: Watermarked image I_W.

1: Apply transform T on the I_o to obtain the transformed image TI_o.
2: Define $TI_W = TI_o$, where, TI_W represents an intermediate watermarked image I_W in the transform domain T.
3: Select a $l_1 \in L_1$.
4: Compute $l_2 = \pi(l_1)$.
5: Compute and assign $TI_W(l_1) \leftarrow TI_o(l_1) + \alpha W_o(l_2)$. ▷ one watermark bit is embedded at one position
6: Repeat steps 4 to 5 for all values of l_1.
7: Apply inverse T transform (T^{-1}) on the updated TI_W to obtain the watermarked image I_W.
8: **Return** I_W. ▷ Watermarked image

Algorithm 4 A traditional non-blind watermark extraction algorithm in transform domain [39, 114].

Input: I_o, I_w, α, L_1, π, transform T same as used in the algorithm 3. ▷ See table 3.3 for detailed explanation of each symbol.

Output: Extracted watermark(s) $W_e/W_e^i s$.

1: Apply transform T on the I_w and the I_o to obtain the transformed images TI_w and TI_o respectively.
2: Select a $l_1 \in L_1$.
3: Compute $d = |TI_w(l_1) - TI_o(l_1)|$.
4: Extract a bit and store in W as follows:

$$W(l_1) = \begin{cases} 0 & \text{if} \quad d < \alpha/2 \\ 1 & \text{if} \quad d \geq \alpha/2 \end{cases} . \tag{3.9}$$

▷ one watermark bit is extracted using one position
5: Repeat steps 3 to 4 for all values of l_1.
6: Use the watermark estimation rule to estimate extracted watermark(s) $W_e/W_e^i s$ from the W.
7: **Return** $W_e/W_e^i s$. ▷ Extracted watermark(s).

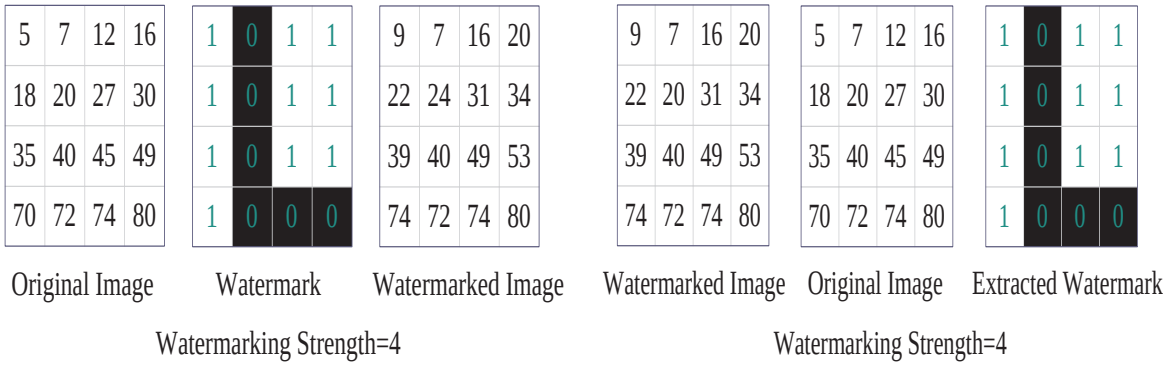
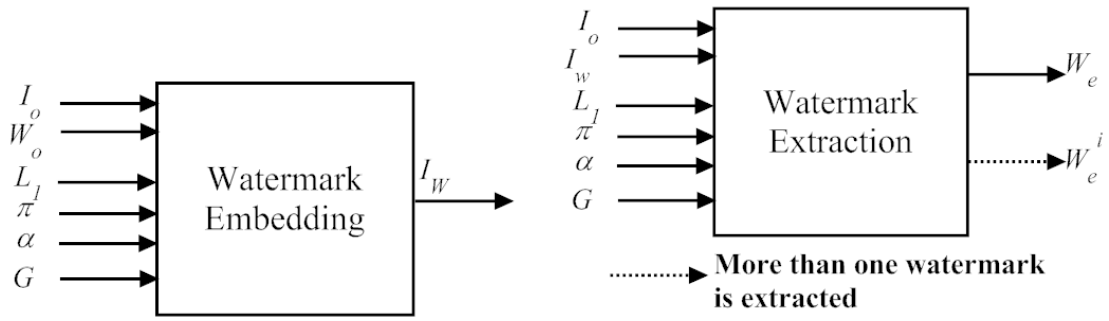


Figure 3.5: A numerical example to illustrate a traditional non-blind watermarking algorithms. (a) Embedding algorithm. (b): Extraction algorithm.



(a) Watermark embedding (b) Watermark extraction

Figure 3.6: Overview of proposed non-blind watermarking scheme.

Algorithm 5 The proposed non-blind watermark embedding algorithm in the ROWT domain.

Input: I_o, W_o, α, L_1, π, $G(P)$ and $G(N)$. ▷ See table 3.3 for detailed explanation of each symbol.

Output: Watermarked image I_W.

1: Apply 1-level ROWT on I_o. Store the decomposed sub-bands as I_oA_1, I_oA_2, I_oP_H, I_oP_V, I_oP_D, I_oN_H, I_oN_V, I_oN_D.

2: Define $I_oP_HW = I_oP_H$, $I_oP_VW = I_oP_V$, $I_oP_DW = I_oP_D$, $I_oN_HW = I_oN_H$, $I_oN_VW = I_oN_V$, $I_oN_DW = I_oN_D$.

3: Compute $s = G(P) \times G(N)$.

4: Select a $l_1 \in L_1$.

5: Extract $\theta \in \{H, V, D\}$ from l_1.

6: Compute $l_2 = \pi(l_1)$.

7: Assign:

$$I_oP_\theta W(l_1) \leftarrow I_oP_\theta(l_1) + \alpha \times G(P) \times W_o(l_2);$$

$$I_oN_\theta W(l_1) \leftarrow I_oN_\theta(l_1) + \alpha \times G(N) \times W_o(l_2).$$

▷ one watermark bit is embedded at two positions

8: Repeat steps 5 to 7 for all values of l_1.

9: Apply inverse ROWT on the sub-bands I_oA_1, I_oA_2, and updated I_oP_HW, I_oP_VW, I_oP_DW, I_oN_HW, I_oN_VW, I_oN_DW to obtain the watermarked image I_W.

10: **Return** I_W. ▷ Watermarked image

Algorithm 6 The proposed non-blind watermark extraction algorithm in the ROWT domain.

Input: I_w, a watermark estimation rule, and I_o, α, L_1, π, $G(P)$, $G(N)$ same as used in algorithm 5. ▷ See table 3.3 for detailed explanation of each symbol.

Output: Extracted watermark(s) $W_e/W_e^i s$.

1: Apply the 1-level ROWT on the I_o and I_w. Store the decomposed sub-bands of I_o as I_oA_1, I_oA_2, I_oP_H, I_oP_V, I_oP_D, I_oN_H, I_oN_V and I_oN_D, and sub-bands of I_w as I_wA_1, I_wA_2, I_wP_H, I_wP_V, I_wP_D, I_wN_H, I_wN_V and I_wN_D.

2: Compute $s = G(P) \times G(N)$.

3: Select a $l_1 \in L_1$.

4: Extract $\theta \in \{H, V, D\}$ from l_1.

5: Compute

$$d = \left| \begin{array}{c} [I_wP_\theta(l_1) + s \times I_wN_\theta(l_1)] - \\ [I_oP_\theta(l_1) + s \times I_oN_\theta(l_1)] \end{array} \right|. \tag{3.10}$$

6: Extract a bit and store it in W as follows:

$$W(l_1) = \begin{cases} 0 & \text{if} \quad d < \alpha/2 \\ 1 & \text{if} \quad d \geq \alpha/2 \end{cases}. \tag{3.11}$$

▷ one watermark bit is extracted using two positions

7: Repeat steps 4 to 6 for all values of l_1.

8: Use the watermark estimation rule to estimate extracted watermark(s) $W_e/W_e^i s$ from the W.

9: **Return** $W_e/W_e^i s$. ▷ Extracted watermark(s).

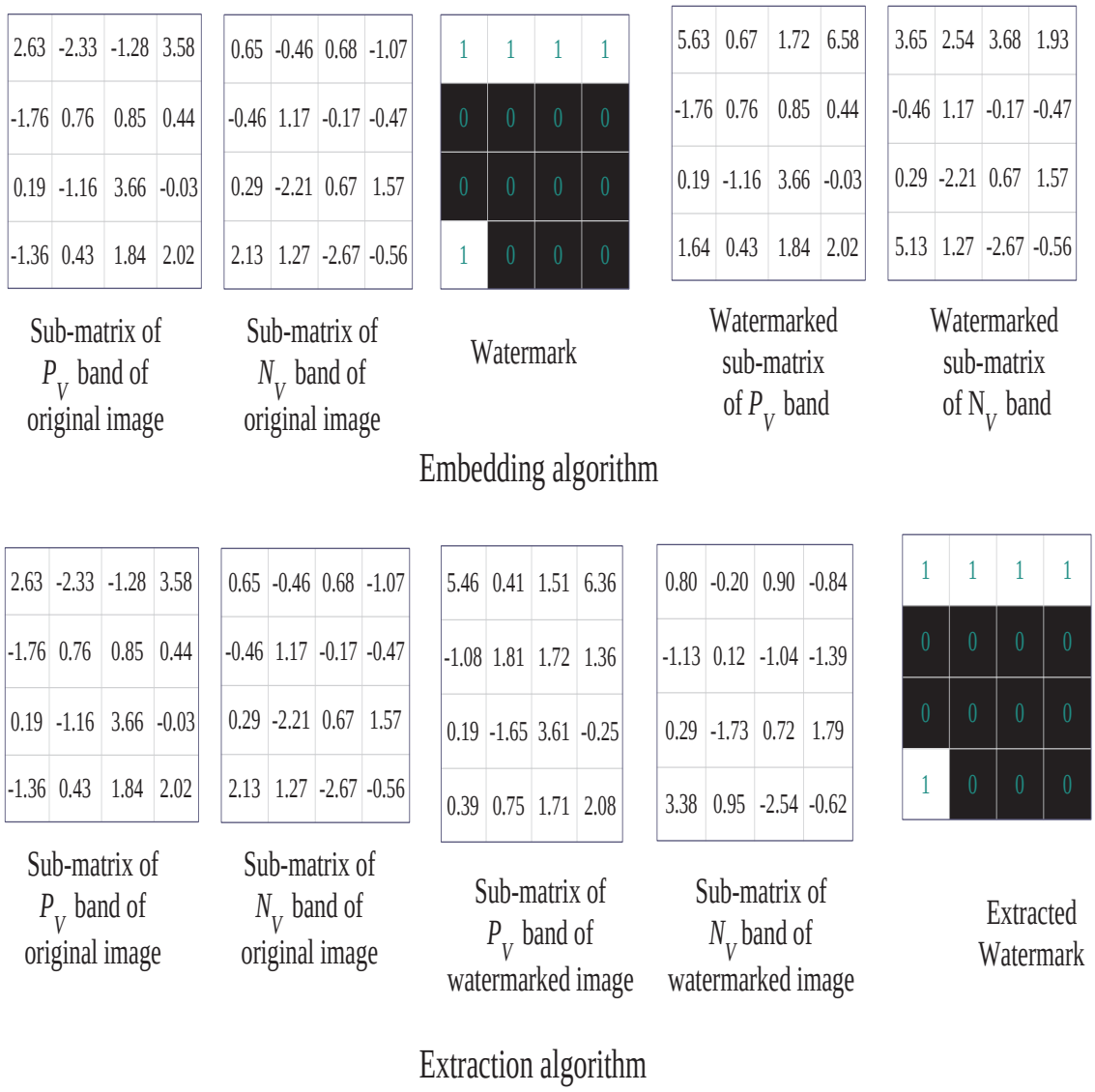


Figure 3.7: A numerical example to illustrate the proposed non-blind watermarking scheme in the ROWT domain. In this example, $\alpha = 3$, and $G(P) = G(N) = 1$.

Figs. 3.6 (a) and (b) summarize the components of the proposed non-blind watermark embedding and extraction algorithms. The details of watermark embedding and extraction algorithms are discussed in algorithms 5 and 6. In algorithm 5, watermark bits are embedded by utilizing (3.5) and (3.6), and in the algorithm 6, watermark bits are extracted by utilizing (3.7) or (3.8). A numerical example is provided in Fig. 3.7 to illustrate the proposed non-blind watermarking scheme.

According to the traditional non-blind watermarking scheme (algorithms 3 and 4), one watermark bit is embedded at one position and one watermark bit is extracted using one position. According to the proposed non-blind watermarking scheme (algorithms 5 and 6), one watermark bit is embedded at two positions and one watermark bit is extracted using two positions. This is the main difference between the traditional and proposed non-blind watermarking schemes.

A watermark is estimated from the extracted watermark bits. In watermark estimation, the following three scenarios can arise:

1. A watermark is embedded once and each watermark bit is embedded once. In this case, π is an one-to-one function and one watermark W_e is estimated as follows:

$$W_e(l_2) \;=\; W(l_1). \tag{3.12}$$

2. A watermark is embedded n (> 1) times and each watermark bit is embedded n times. In this scenario, π is a many-to-one function, the redundancy of the watermark is n, and n watermarks W_e^i are estimated as follows:

$$W_e^i(l_2) \;=\; W(\pi^{-1}(\pi(l_1))_i), \tag{3.13}$$

where, $i = 1, 2, \cdots n$, π^{-1} is the inverse map of π and

$$\pi^{-1}(\pi(l_1)) = \{\pi^{-1}(\pi(l_1))_i\}.$$

3. A watermark is embedded once and each watermark bit is embedded n (an odd number) times. In this situation, π is a many-to-one function, the redundancy of the watermark bits is n and one watermark is estimated by the voting method as follows:

$$W_e(l_2) = b(\pi^{-1}(\pi(l_1))), \tag{3.14}$$

where,

$$b(.) = \begin{cases} 0 & \text{if } c_0(.) > c_1(.) \\ 1 & \text{if } c_0(.) < c_1(.) \end{cases}, \tag{3.15}$$

and $c_0(\pi^{-1}(\pi(l_1)))$ and $c_1(\pi^{-1}(\pi(l_1)))$ are a number of 0 and 1 watermark bits, respectively, at the $\pi^{-1}(\pi(l_1))$.

3.3.2 Blind Watermarking Schemes

A Traditional Blind Watermarking Scheme

A watermark embedding algorithm and the corresponding watermark extraction algorithm of a traditional blind watermarking scheme are explained in algorithms 7 and 8 respectively. The core idea in the watermark embedding algorithm is that *if watermark bit is one, then make the watermarking coefficient as odd multiple of watermarking strength else if watermark bit is zero, then make the coefficient as even multiple of watermarking strength.* The core idea in the watermark extraction algorithm is that *if watermarked coefficient is odd multiple of watermarking strength, then extracted watermark bit is one else if watermarked coefficient is even multiple of watermarking strength, then extracted watermark bit is zero.* A numerical example is provided in Fig. 3.8 to illustrate the traditional blind watermarking scheme.

Algorithm 7 A traditional blind watermark embedding algorithm in transform domain [113, 235].

Input: I_o, W_o, α, L_1, π, an arbitrary transform T and its inverse transform T^{-1}. ▷ See table 3.3 for detailed explanation of each symbol.

Output: Watermarked image I_W.

1: Apply transform T on the I_o to obtain the transformed image TI_o.
2: Define $TI_W = TI_o$, where, TI_W represents an intermediate watermarked image I_W in the transform domain T.
3: Compute $r = TI_o(l_1) \mod \alpha$.
4: Compute $b = (TI_o(l_1) - r)/\alpha$.
5: Compute $l_2 = \pi(l_1)$.
6: **if** ($b \mod 2 == 0$ AND $W_o(l_2) == 0$) **then** $TI_W(l_1) \leftarrow TI_o(l_1) - r$
7: **else if** ($b \mod 2 == 1$ AND $W_o(l_2) == 0$) **then** $TI_W(l_1) \leftarrow TI_o(l_1) - r + \alpha$
8: **else if** ($b \mod 2 == 0$ AND $W_o(l_2) == 1$) **then** $TI_W(l_1) \leftarrow TI_o(l_1) - r + \alpha$
9: **else if** ($b \mod 2 == 1$ AND $W_o(l_2) == 1$) **then** $TI_W(l_1) \leftarrow TI_o(l_1) - r$
10: **end if** ▷ one watermark bit is embedded at one position
11: Repeat steps 3 to 10 for all values of l_1.
12: Apply inverse T transform (T^{-1}) on the updated TI_W to obtain the watermarked image I_W.
13: **Return** I_W. ▷ Watermarked image

Algorithm 8 A traditional blind watermark extraction algorithm in transform domain [113, 235].

Input: I_w, watermark estimation rule, and α, L_1, π and transform T same as used in the algorithm 7. ▷ See table 3.3 for detailed explanation of each symbol.

Output: Extracted watermark(s) $W_e/W_e^i s$.

1: Apply transform T on the I_w to obtain the transformed image TI_w.
2: Select a $l_1 \in L_1$
3: Compute $r = TI_w(l_1) \mod \alpha$.
4: **if** $(r > \frac{\alpha}{2})$ **then** $TI_w(l_1) \leftarrow TI_w(l_1) + \alpha - r$
5: **else**$TI_w(l_1) \leftarrow TI_w(l_1) - r$
6: **end if**
7: Compute $q = TI_w(l_1)/\alpha$.
8: Compute and store extracted bit in W as:
9: **if** q is even **then** $W(l_1) = 0$
10: **else**$W(l_1) = 1$.
11: **end if** ▷ one watermark bit is extracted using one position
12: Repeat steps 3 to 11 for all values of l_1.
13: Use the watermark estimation rule to estimate extracted watermark(s) $W_e/W_e^i s$ from the W.
14: **return** $W_e/W_e^i s$. ▷ Extracted watermark(s).

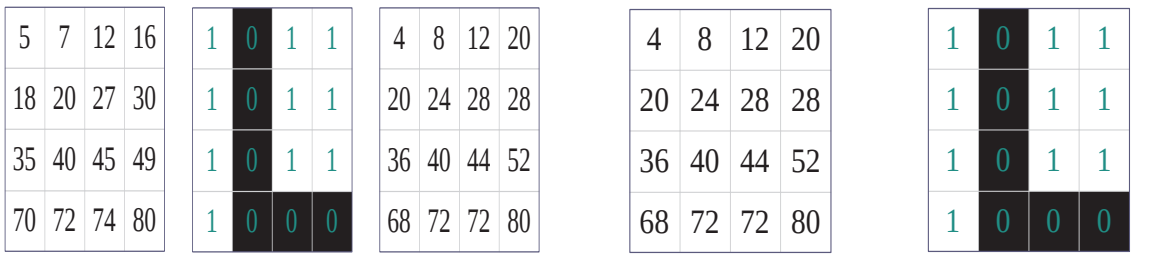


Figure 3.8: A numerical example to illustrate a traditional blind watermarking algorithms. (a) Embedding algorithm. (b): Extraction algorithm.

Special Mathematical Properties

The core theory in the traditional blind watermarking scheme is to make the watermarked coefficients an even/odd multiple of watermarking strength. Success of this theory depends on the fact that watermarked coefficients are well preserved after applying a transform succeeded by its inverse transform. This fact is not true for the ROWT, that is ROWT (algorithm 1) succeeded by its left inverse (algorithm 1) does not make an identity transform. The core theory in the proposed blind watermarking scheme in the ROWT domain is to add/subtract a value in coefficients of positive and negative sub-bands of the original image according to the observed property of the ROWT such that remainder of sum of the added value and sum/difference of the coefficients of the positive and negative sub-bands belongs to a well defined desired interval. Success of this theory is guaranteed by the relations (3.7) and (3.8). The added values are found using specially derived mathematical properties based on the Quotient-Remainder theorem. The added/subtracted values depend on watermarking strength and a desired interval.

Let μ be a non-negative real number and α be a positive real number. Then the remainder r can be found such that $\mu = \alpha m + r$, where m is the non-negative integer and $0 \leq r < \alpha$. This is the Quotient-Remainder theorem. Here, m is termed as the quotient. Based on the Quotient-Remainder theorem, the following properties hold:

1. remainder(r_1) of $\mu + \frac{\alpha - r}{2}$ is $\alpha\left(\frac{1+\delta}{2}\right) < r_1 < \alpha\left(\frac{2-\delta}{2}\right)$, if $\delta\alpha < r < \alpha(1-\delta)$,

2. remainder(r_2) of $\mu + \alpha\left(\frac{1+\delta}{2}\right)$ is $\alpha\left(\frac{1+\delta}{2}\right) \leq r_2 \leq \alpha\left(\frac{1+3\delta}{2}\right)$, if $r \leq \delta\alpha$,

3. remainder(r_3) of $\mu + \alpha\left(\frac{2-\delta}{2}\right)$ is $\alpha\left(\frac{1-3\delta}{2}\right) \leq r_3 < \alpha\left(\frac{2-\delta}{2}\right)$, if $r \geq \alpha(1-\delta)$,

4. remainder(r_4) of $\mu + \frac{2\alpha - r}{2}$ is $\frac{\delta\alpha}{2} < r_4 < \alpha\left(\frac{1-\delta}{2}\right)$, if $\delta\alpha < r < \alpha(1-\delta)$,

5. remainder(r_5) of $\mu + \alpha\left(\frac{2+\delta}{2}\right)$ is $\frac{\delta\alpha}{2} \leq r_5 \leq \frac{3\delta\alpha}{2}$, if $r \leq \delta\alpha$,

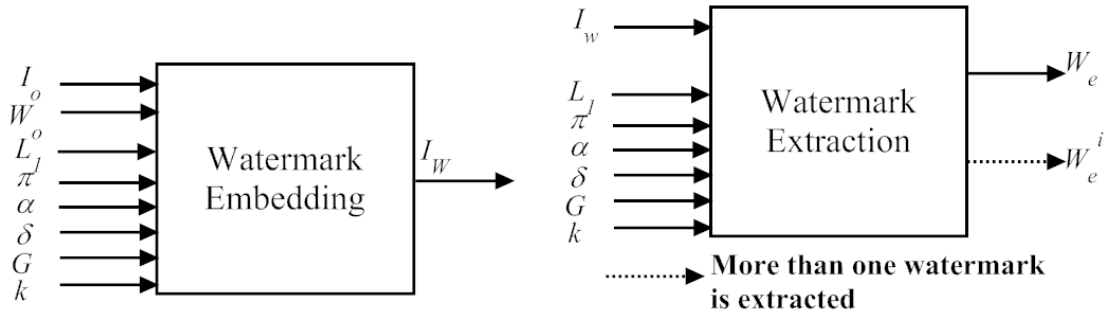
6. remainder(r_6) of $\mu + \alpha\left(\frac{3-\delta}{2}\right)$ is $\alpha\left(\frac{1-3\delta}{2}\right) \leq r_6 < \alpha\left(\frac{1-\delta}{2}\right)$, if $r \geq \alpha(1-\delta)$,

as long as $\delta \in \left(0, \frac{1}{3}\right)$. Moreover,

7. $\alpha\left(\frac{1+\delta}{2}\right) \leq r_1, r_2, r_3 < \alpha\left(\frac{2-\delta}{2}\right)$,

8. $\frac{\delta\alpha}{2} \leq r_4, r_5, r_6 < \alpha\left(\frac{1-\delta}{2}\right)$.

In properties 1-6, the term μ is equivalent to the sum (or difference) of the coefficients of positive and negative sub-bands of an original image in the ROWT domain. Properties 1-6 are used in the proposed blind watermark embedding algorithm 9 and properties 7-8 are used in the proposed blind watermark extraction algorithm 10.



(a) Watermark embedding algorithm (b) Watermark extraction algorithm

Figure 3.9: Overview of proposed blind watermarking scheme.

The Proposed Blind Watermarking Scheme in the ROWT Domain

Fig. 3.9 (a) summarizes the components in the watermark embedding algorithm and Fig. 3.9 (b) summarizes the components in the watermark extraction algorithm. The details of the watermark embedding and extraction algorithms are discussed in algorithms 9 and 10 respectively. A numerical example is provided in Fig. 3.10 to illustrate the proposed blind watermarking scheme.

Like the proposed non-blind watermarking scheme, in this scheme also (algorithms 9 and 10), one watermark bit is embedded at two positions and one watermark bit is extracted using two positions.

Algorithm 9 The proposed blind watermark embedding algorithm in the ROWT domain.

Input: I_o, W_o, α, L_1, π, $G(P)$, $G(N)$, k and δ. ▷ See table 3.3 for detailed explanation of each symbol.

Output: Watermarked image I_W.

1: Apply the 1-level ROWT on the I_o. Store the decomposed sub-bands as I_oA_1, I_oA_2, I_oP_H, I_oP_V, I_oP_D, I_oN_H, I_oN_V, I_oN_D.

2: Define $I_oP_HW = I_oP_H$, $I_oP_VW = I_oP_V$, $I_oP_DW = I_oP_D$, $I_oN_HW = I_oN_H$, $I_oN_VW = I_oN_V$, $I_oN_DW = I_oN_D$.

3: Compute $s = G(P) \times G(N)$.

4: Select a $l_1 \in L_1$.

5: Compute $l_2 = \pi(l_1)$.

6: Extract $\theta \in \{H, V, D\}$ from the l_1.

7: Compute $r = |I_oP_\theta(l_1) + s \times I_oN_\theta(l_1)| \mod \alpha$.

8: Compute α_1 as follows: ▷ this computation is according to properties 1-6 discussed in section 3.3.2.

$$\alpha_1 = \begin{cases} \alpha + \delta\alpha & \text{if} \quad 0 \le r \le \delta\alpha \\ \alpha - r & \text{if} \quad \delta\alpha < r < \alpha - \delta\alpha \\ 2\alpha - \delta\alpha & \text{if} \quad \alpha - \delta\alpha \le r < \alpha \end{cases}. \tag{3.16}$$

9: Compute α_2 as follows: ▷ this computation is according to properties 1-6 discussed in section 3.3.2.

$$\alpha_2 = \begin{cases} 2\alpha + \delta\alpha & \text{if} \quad 0 \le r \le \delta\alpha \\ 2\alpha - r & \text{if} \quad \delta\alpha < r < \alpha - \delta\alpha \\ 3\alpha - \delta\alpha & \text{if} \quad \alpha - \delta\alpha \le r < \alpha \end{cases}. \tag{3.17}$$

10: **if** ($k == 1$ AND $W_o(l_2) == 0$) **then**

$$I_oP_\theta W(l_1) = I_oP_\theta(l_1) + G(P) \times \frac{\alpha_1}{2};$$

$$I_oN_\theta W(l_1) = I_oN_\theta(l_1) + G(N) \times \frac{\alpha_1}{2};$$

11: **else if** ($k == 1$ AND $W_o(l_2) == 1$) **then**

$$I_oP_\theta W(l_1) = I_oP_\theta(l_1) + G(P) \times \frac{\alpha_2}{2};$$

$$I_oN_\theta W(l_1) = I_oN_\theta(l_1) + G(N) \times \frac{\alpha_2}{2};$$

12: **else if** ($k == 2$ AND $W_o(l_2) == 0$) **then**

$$I_oP_\theta W(l_1) = I_oP_\theta(l_1) + G(P) \times \frac{\alpha_2}{2};$$

$$I_oN_\theta W(l_1) = I_oN_\theta(l_1) + G(N) \times \frac{\alpha_2}{2};$$

13: **else if** ($k == 2$ AND $W_o(l_2) == 1$) **then**

$$I_oP_\theta W(l_1) = I_oP_\theta(l_1) + G(P) \times \frac{\alpha_1}{2};$$

$$I_oN_\theta W(l_1) = I_oN_\theta(l_1) + G(N) \times \frac{\alpha_1}{2};$$

14: **end if** ▷ one watermark bit is embedded at two positions

15: Repeat steps 5 to 14 for all values of l_1.

16: Apply inverse ROWT on the sub-bands I_oA_1, I_oA_2, and updated I_oP_HW, I_oP_VW, I_oP_DW, I_oN_HW, I_oN_VW and I_oN_DW to obtain the watermarked image I_W.

17: **return** I_W. ▷ Watermarked image.

Algorithm 10 The proposed blind watermark extraction algorithm in the ROWT domain.

Input: I_w, watermark estimation rule, and α, L_1, π, $G(P)$, $G(N)$ and k same as used in the algorithm 9. ▷ See table 3.3 for detailed explanation of each symbol.

Output: Extracted watermark(s) $W_e/W_e^i s$.

1: Apply ROWT on the I_w. Store the decomposed sub-bands as I_wA_1, I_wA_2, I_wP_H, I_wP_V, I_wP_D, I_wN_H, I_wN_V, I_wN_D.
2: Compute $s = G(P) \times G(N)$.
3: Select a $l_1 \in L_1$.
4: Extract $\theta \in \{H, V, D\}$ from l_1.
5: Compute $r = |I_oP_\theta(l_1) + s \times I_oN_\theta(l_1)| \mod \alpha$.
6: Extract a bit and store in W as follows:
7: **if** $(k == 1)$ **then**

$$W(l_1) = \begin{cases} 1 & \text{if} \quad 0 \leq r < \frac{\alpha}{2} \\ 0 & \text{if} \quad \frac{\alpha}{2} \leq r < \alpha \end{cases} ; \tag{3.18}$$

8: **else if** $(k == 2)$ **then**

$$W(l_1) = \begin{cases} 0 & \text{if} \quad 0 \leq r < \frac{\alpha}{2} \\ 1 & \text{if} \quad \frac{\alpha}{2} \leq r < \alpha \end{cases} . \tag{3.19}$$

9: **end if** ▷ one watermark bit is extracted using two positions
10: Repeat Steps 4 to 9 for all values of l_1.
11: Use the watermark estimation rule to estimate extracted watermark(s) $W_e/W_e^i s$ from the W.
12: **Return** $W_e/W_e^i s$. ▷ Extracted watermark(s).

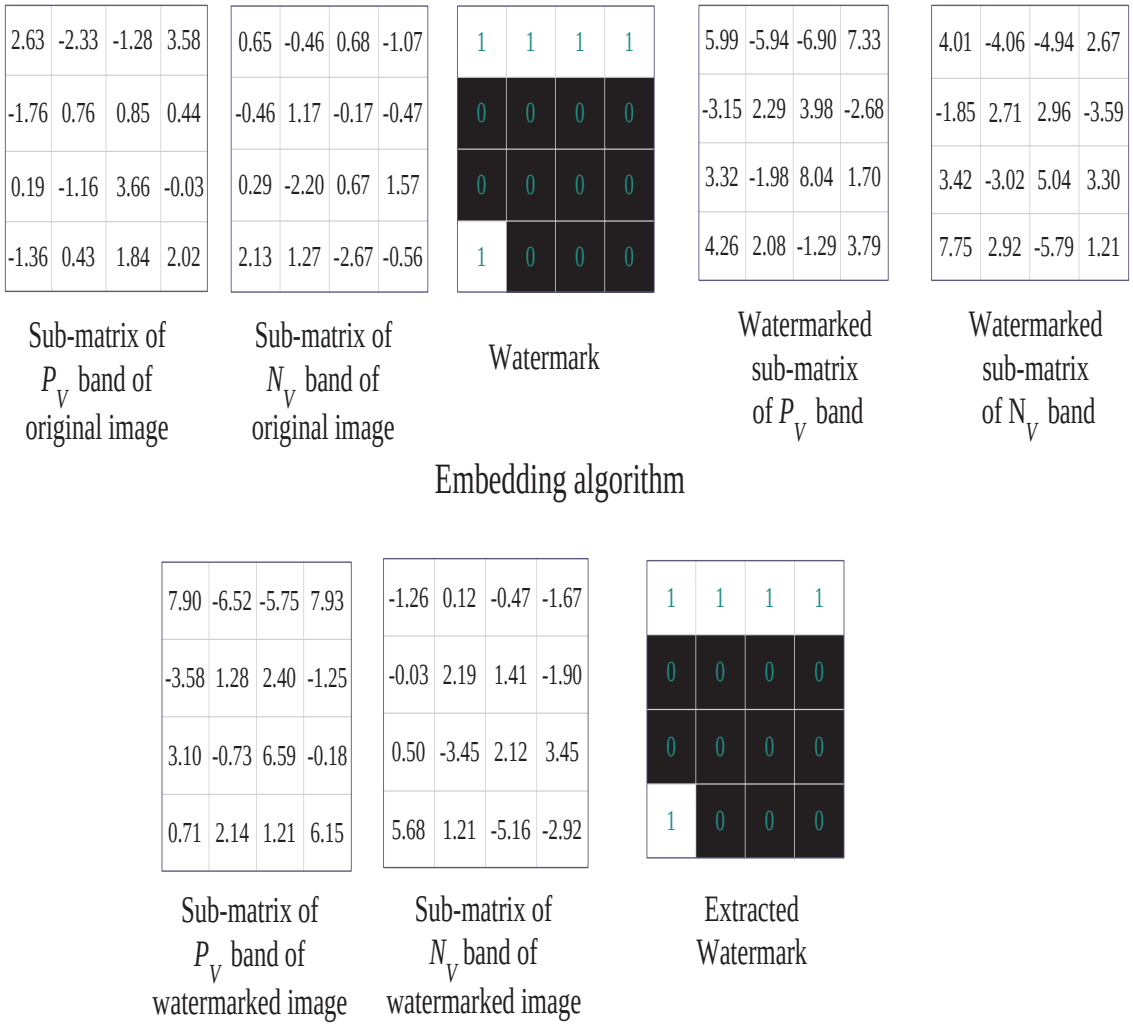


Figure 3.10: A numerical example to illustrate the proposed blind watermarking scheme in the ROWT domain. In this example, $\alpha = 5$, $\delta = 0.25$, $G(P) = G(N) = 1$ and $k = 1$.

3.4 Experiments, Results and Analysis

We have performed six experiments for a detailed analysis of the proposed watermarking schemes. The first experiment (Experiment 1) tests the proposed watermarking schemes and studies the effect of embedding strength and error controller. This experiment helps to find optimal embedding strength and error controller. Second experiment (Experiment 2) elaborates the importance of the observed property of ROWT. Third experiment (Experiment 3) studies the performance of the proposed watermarking schemes and studies the effect of embedding strength and error controller under the formatting operation on watermarked images. Fourth experiment (Experiment 4) evaluates the performance of the proposed watermarking schemes under various attacks on formatted watermarked images. Fifth experiment (Experiment 5) compares the proposed watermarking schemes and existing watermarking schemes without any post operations/attacks on the watermarked images. Sixth experiment (Experiment 6) compares the performance of the proposed watermarking schemes and existing watermarking schemes under various post operations/attacks on the watermarked images.

We have performed all the experiments on MATLAB platform. In the experiments, we have used a data-set that consists of six host images and five watermarks. Fig. 3.11 (a) shows all host images (h_1, h_2, h_3, h_4, h_5, h_6) and Fig. 3.11 (b) shows all watermarks (W_1, W_2, W_3, W_4 and W_5) of the data-set. Each host image is an eight bit gray scale image of size 256×256 pixels and each watermark is a black and white (binary) image of size 128×128 pixels. We have used all the combinations of host images and watermarks to obtain different watermarked images.

A common setup in all the experiments is as follows. We have repeated a watermark three times by embedding it once in V, H and D sub-bands of a host image. This makes watermarks of an effective size of $3 \times 128 \times 128$ pixels.

h_1 h_2 h_3

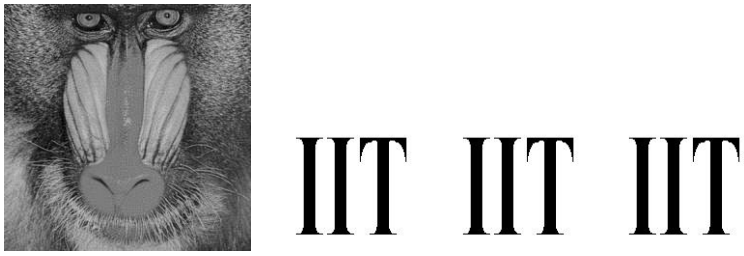
h_4 h_5 h_6

(a): Host images.

W_1 W_2 W_3 W_4 W_5

(b): Original watermarks.

Figure 3.11: Data set.



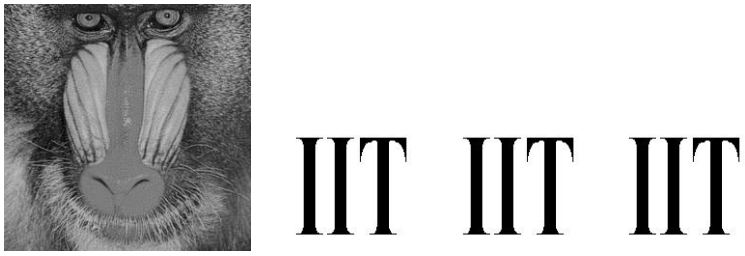
PSNR=41.0755 dB (a) NHS=1 (b) NHS=1 (c) NHS=1 (d)

Figure 3.12: A sample result of non-blind watermarking scheme at embedding strength of 3. (a): A sample watermarked image. (b): Watermark extracted from V sub-bands of (a). (c): Watermark extracted from H sub-bands of (a). (d): Watermark extracted from D sub-bands of (a).

L_1 (table 3.3) consists of all the locations of V, H, D sub-bands of a host image. π is a simple left-right-top-bottom scan map. We have set $G(P) = G(N) = 1$. For the proposed blind watermarking scheme, we have used $k = 1$.

3.4.1 Experiment 1: Testing of Proposed Watermarking Schemes and Effect of Embedding Strength and Error Controller

Non-blind watermarking scheme. We have implemented the proposed non-blind watermarking scheme on the data-set (shown in Fig. 3.11) for various embedding strengths ($\alpha = 1, 2, \cdots, 20$). Peak-signal-to-noise-ratio (PSNR, appendix A.1) measures the visual similarity between the original image and the watermarked image, and normalized-Hamming-similarity (NHS, section 6.1.1) measures the similarity between the embedded watermark and the corresponding extracted watermarks.



PSNR=36.2679 dB NHS=1 NHS=1 NHS=1
(a) (b) (c) (d)

Figure 3.13: A sample result of blind watermarking scheme at embedding strength of 5 and error controller of 0.25. (a): A sample watermarked image. (b): Watermark extracted from V sub-bands of (a). (c): Watermark extracted from H sub-bands of (a). (d): Watermark extracted from D sub-bands of (a).

We have observed that the embedding strength decreases PSNR and does not affect NHS. Fig. 3.12 (a) shows a watermarked image which corresponds to host image h_4, original watermark W_1, and the embedding strength of 3. Fig. 3.12 (a) ensures no visual degradation in the watermarked image. The obtained watermarked images are 64-bit (double format) gray scale images of size 256×256 pixels. Figs. 3.12 (b), (c) and (d) show watermarks extracted from V, H and D sub-bands, respectively, of a watermarked image (Fig. 3.12 (a)) and ensure very good quality of extracted watermarks. We have obtained very close results for all other combinations of host images and original watermarks of the data-set (Fig. 3.11).

Blind watermarking scheme. We have also implemented the proposed blind watermarking scheme on the same data-set for various embedding strengths ($\alpha = 1, 2, \cdots, 20$) and various error controllers ($\delta = 0.00, 0.05, 0.10, 0.15, 0.20, 0.25, 0.30, 0.33$).

We have observed that the embedding strength and error controller decrease PSNR and do not affect NHS. Fig. 3.13 (a) shows a sample watermarked

image which corresponds to host image h_4, original watermark W_1, embedding strength of 5 and error controller δ of 0.25 and ensures no visual degradation in the watermarked image. Like non-blind watermarking scheme, the obtained watermarked images are 64-bit (double format) gray scale images of size 256×256 pixels. Figs. 3.13 (b), (c) and (d) show watermarks extracted from V, H and D sub-bands, respectively, of a watermarked image (Fig. 3.13 (a)) and ensure very good quality of extracted watermarks. We have obtained very close results for all other combinations of host images and original watermarks of the data-set (Fig. 3.11).

3.4.2 Experiment 2: What if the Observed Property of ROWT is Not Utilized ?

This experiment implements the ROWT based traditional non-blind and blind watermarking schemes which do not utilize the observed property of the ROWT. For this traditional non-blind watermarking scheme, the fundamental embedding and extraction rules are based on algorithms 3 and 4 respectively, and for this traditional blind watermarking scheme, the fundamental embedding and extraction rules are based on algorithms 7 and 8 respectively. If we do not incorporate the observed property of the ROWT, then the length of a watermark can be doubled, as traditional watermarking schemes in the ROWT domain embed one watermark bit at one position and extract one watermark bit using one position, while the proposed schemes embed one watermark bit at two positions and extract one watermark bit using two positions. In this experiment, all six detailed sub-bands of an original image have been used for watermarking. Therefore, in traditional watermarking schemes, a watermark is repeated six times instead of three times as in the proposed watermarking schemes.

Non-blind watermarking scheme. Fig. 3.14 shows a sample result of a traditional non-blind watermarking scheme in the ROWT domain which does not use the observed property of ROWT. We have observed that watermarks extracted from positive sub-bands are very close to embedded watermark and watermarks extracted from negative sub-bands are not matched with embedded watermark. Therefore, only positive sub-bands can be used for watermarking. The quality of watermarks extracted using proposed non-blind watermarking scheme is better than traditional non-blind watermarking scheme (see Figs. 3.12 (b), (c) and (d) and Figs. 3.14 (b), (c) and (d)). This affirms that the proposed non-blind watermarking scheme with the observed ROWT property has slightly better performance than the ROWT based traditional non-blind watermarking scheme.

Blind watermarking scheme. Fig. 3.15 shows a sample result of a traditional blind watermarking scheme in the ROWT domain which does not utilize the observed ROWT property. We have observed that the extracted watermarks are very noisy (Fig. 3.15). Figs. 3.13 and 3.15 ensure that proper utilization of the observed ROWT property has significantly improved the quality of extracted watermarks.

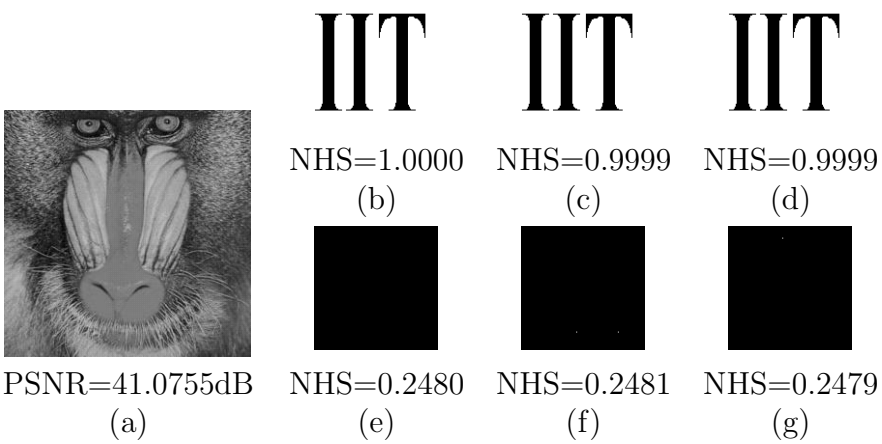


Figure 3.14: A traditional non-blind watermarking scheme in the ROWT domain without the observed property. (a): A sample watermarked image. (b): Watermark extracted from positive V sub-band of (a). (c): Watermark extracted from positive H sub-band of (a). (d): Watermark extracted from positive D sub-band of (a). (e): Watermark extracted from negative V sub-band of (a). (f): Watermark extracted from negative H sub-band of (a). (g): Watermark extracted from negative D sub-band of (a).

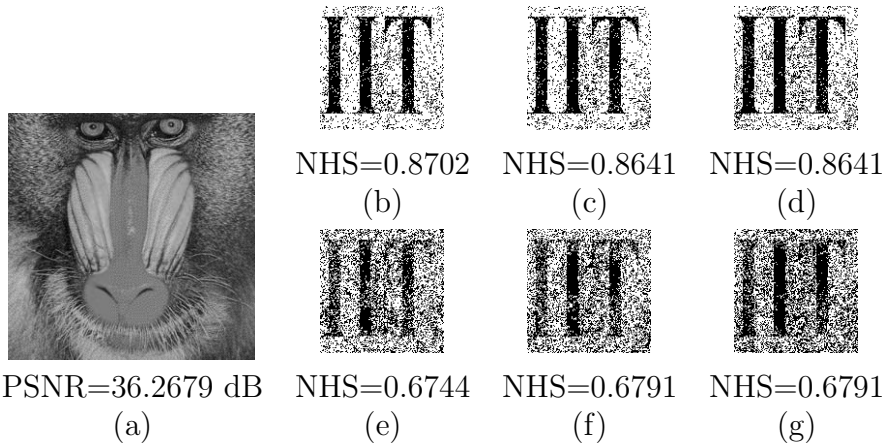
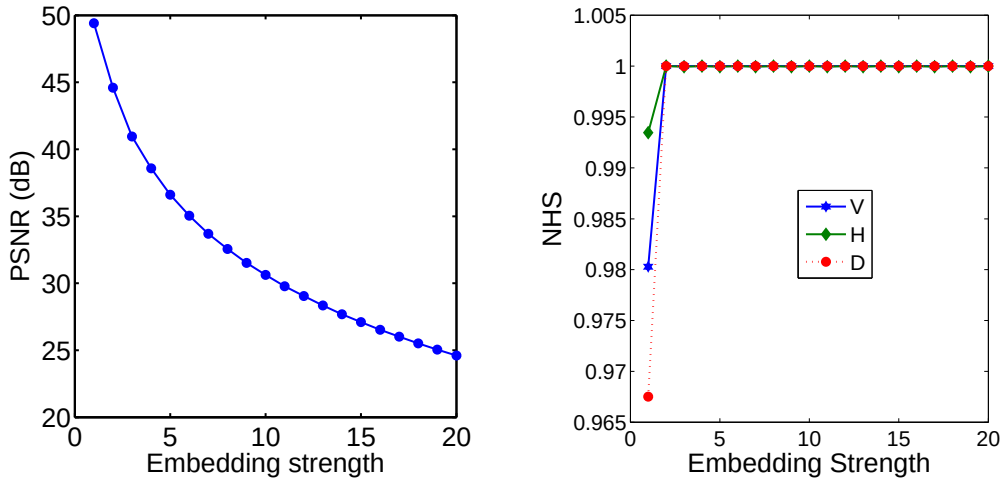


Figure 3.15: A traditional blind watermarking scheme in the ROWT domain without the observed property. (a): A sample watermarked image. (b): Watermark extracted from positive V sub-band of (a). (c): Watermark extracted from positive H sub-band of (a). (d): Watermark extracted from positive D sub-band of (a). (e): Watermark extracted from negative V sub-band of (a). (f): Watermark extracted from negative H sub-band of (a). (g): Watermark extracted from negative D sub-band of (a).



(a) (b)

Figure 3.16: Non-blind watermarking scheme for a sample combination of host image h_4 and original watermark W_1. (a): PSNR curve of formatted watermarked images of the combination. (b): NHS curves of watermarks extracted from V, H and D sub-bands of formatted watermarked images of the combination.

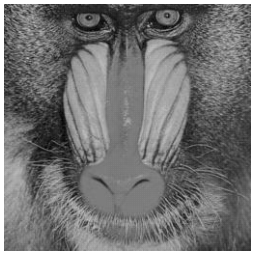
3.4.3 Experiment 3: The Effect of Embedding Strength and Error Controller on Formatted Watermarked Images

In Experiment 1, host images are eight bit gray scale images and watermarked images are 64-bit (double format) gray scale images. In most of the watermarking applications, the same format of host images and watermarked images is a common request. We have applied uint8 operation on all the watermarked images to obtain the formatted watermarked images (eight bit gray scale images).

Non-blind watermarking scheme. Fig. 3.16 (a) shows the PSNR curve of the formatted watermarked images and Fig. 3.16 (b) shows the NHS curves of the watermarks extracted from V, H and D sub-bands of the formatted watermarked images. The formatted watermarked images correspond to the combination of host image h_4 and watermark W_1. Fig. 3.16 (a) depicts a decrease in PSNR with embedding strength. Moreover, the PSNR curve is very close to that

Table 3.4: Quantitative results of proposed non-blind watermarking scheme based on ROWT after formatting operation. $\alpha = 3$.

Original Image	Watermark	PSNR (dB)	NHS of extracted watermark		
			V sub-band	H sub-band	D sub-band
h_1	W_1	40.96	1	1	1
h_1	W_2	40.84	1	1	1
h_1	W_3	41.41	1	1	1
h_1	W_4	40.98	1	1	1
h_1	W_5	40.88	1	1	1
h_2	W_1	40.96	0.9999	0.9999	0.9999
h_2	W_2	40.84	0.9999	0.9999	0.9999
h_2	W_3	41.40	1	1	1
h_2	W_4	40.98	0.9999	0.9999	0.9999
h_2	W_5	40.88	1	1	1
h_3	W_1	41.04	0.9886	0.9901	0.9955
h_3	W_2	40.93	0.9868	0.9882	0.9937
h_3	W_3	41.50	0.9883	0.9893	0.9941
h_3	W_4	40.97	0.9865	0.9885	0.9938
h_3	W_5	40.85	0.9884	0.9894	0.9949
h_4	W_1	40.96	1	0.9999	1
h_4	W_2	40.84	1	0.9999	1
h_4	W_3	41.40	1	0.9999	1
h_4	W_4	40.97	1	0.9999	1
h_4	W_5	40.89	1	0.9999	1
h_5	W_1	40.96	0.9996	0.9998	0.9999
h_5	W_2	40.84	0.9996	0.9997	0.9998
h_5	W_3	41.41	0.9997	0.9998	0.9999
h_5	W_4	40.98	0.9997	0.9997	0.9998
h_5	W_5	40.88	0.9997	0.9998	0.9999
h_6	W_1	40.96	1	1	1
h_6	W_2	40.84	1	1	1
h_6	W_3	41.40	1	1	1
h_6	W_4	40.97	1	1	1
h_6	W_5	41.96	1	1	1




PSNR=40.9572 dB NHS=1.0000 NHS=0.9999 NHS=1.0000
(a) (b) (c) (d)

Figure 3.17: A sample result of the proposed non-blind watermarking scheme for a formatted watermarked image at an embedding strength of 3. (a): A sample formatted watermarked image. (b): Watermark extracted from V sub-bands of (a). (c): Watermark extracted from H sub-bands of (a). (d): Watermark extracted from D sub-bands of (a).

obtained in Experiment 1. Fig. 3.16 (b) depicts that NHSs depend on low range embedding strength and near independence of embedding strength after its value of two. This ensures a slight effect of the uint8 operation on the quality of extracted watermarks in the lower range of embedding strength. Table 3.4 gives quantitative results of the data-set for each watermarked image at embedding strength of 3. Fig. 3.17 (a) shows a formatted watermarked image corresponds to host image h_4, original watermark W_1 and embedding strength of 3, and ensures no visual degradation in the watermarked image. In other experiments, we have used embedding strength of 3, unless stated. Figs. 3.17 (b), (c) and (d) show watermarks extracted from V, H and D sub-bands, respectively, of the formatted watermarked image (Fig. 3.17 (a)) and ensure very good quality of extracted watermarks. In summary, the uint8 operation slightly affects the performance of a non-blind watermarking scheme. We have obtained very close results for all other combinations of host images and original watermarks of the data-set (Fig. 3.11).

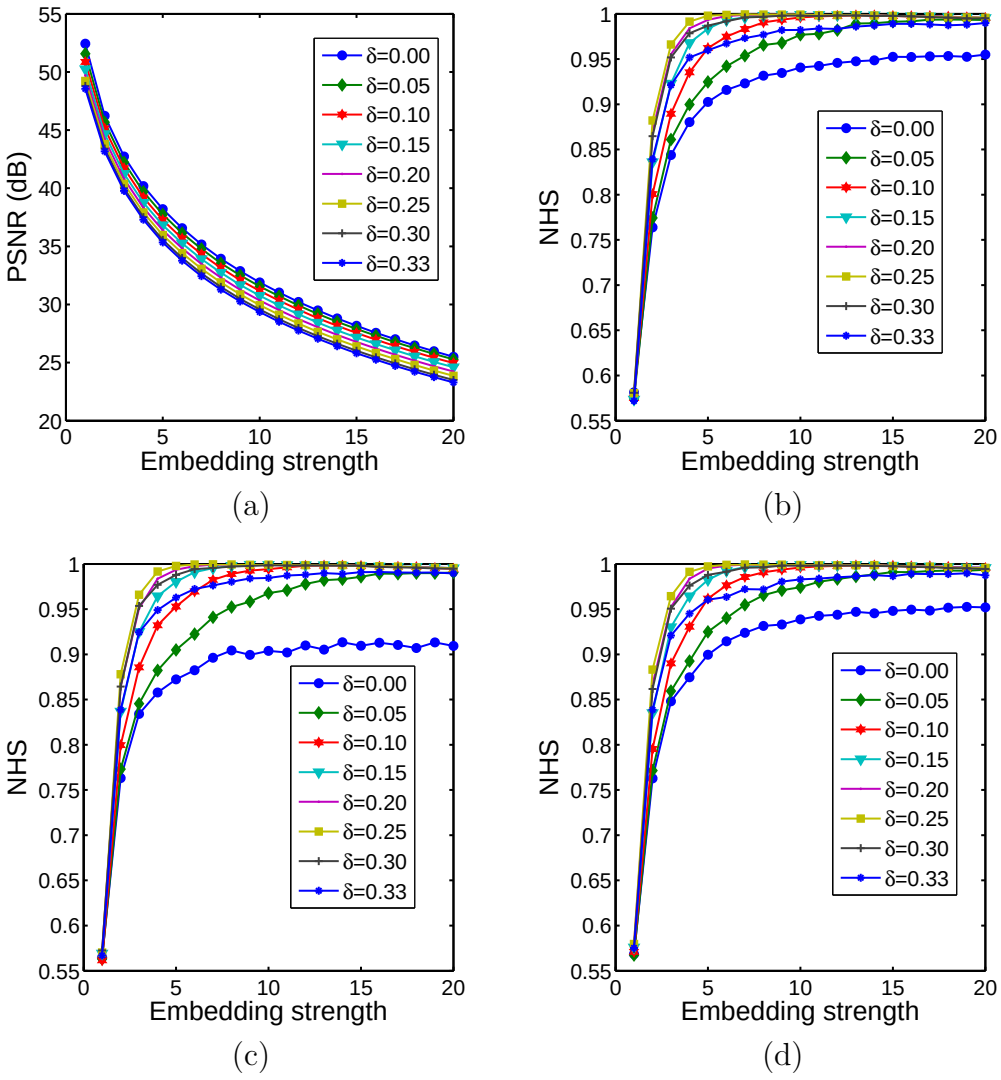


Figure 3.18: Blind watermarking scheme for a combination of host image h_4 and original watermark W_1. δ is the error controller. (a): PSNR curves of formatted watermarked images of the combination. (b): NHS curves of watermarks extracted from V sub-bands of formatted watermarked images of the combination for different error controllers (δs). (c): NHS curves of watermarks extracted from H sub-bands. (d): NHS curves of watermarks extracted from D sub-bands.

Table 3.5: Quantitative results of proposed blind watermarking scheme based on ROWT after formatting operation. $\delta = 0.25$, $\alpha = 5$.

Original Image	Watermark	PSNR (dB)	NHS of extracted watermark		
			V sub-band	H sub-band	D sub-band
h_1	W_1	36.05	0.9979	0.9988	0.9976
h_1	W_2	35.97	0.9979	0.9973	0.9977
h_1	W_3	35.91	0.9976	0.9972	0.9978
h_1	W_4	35.92	0.9975	0.9978	0.9979
h_1	W_5	35.95	0.9978	0.9980	0.9978
h_2	W_1	35.91	0.9982	0.9982	0.9975
h_2	W_2	35.83	0.9982	0.9980	0.9980
h_2	W_3	36.17	0.9980	0.9979	0.9983
h_2	W_4	35.97	0.9981	0.9985	0.9978
h_2	W_5	35.90	0.9982	0.9983	0.9982
h_3	W_1	36.02	0.9583	0.9592	0.9606
h_3	W_2	35.95	0.9582	0.9583	0.9604
h_3	W_3	36.32	0.9574	0.9583	0.9606
h_3	W_4	35.98	0.9581	0.9584	0.9605
h_3	W_5	36.19	0.9577	0.9586	0.9606
h_4	W_1	36.25	0.9977	0.9971	0.9979
h_4	W_2	35.81	0.9955	0.9951	0.9956
h_4	W_3	35.74	0.9954	0.9946	0.9946
h_4	W_4	35.85	0.9958	0.9957	0.9966
h_4	W_5	35.78	0.9962	0.9952	0.9956
h_5	W_1	36.09	0.9957	0.9951	0.9951
h_5	W_2	35.77	0.9850	0.9855	0.9832
h_5	W_3	35.69	0.9851	0.9855	0.9830
h_5	W_4	35.94	0.9856	0.9856	0.9838
h_5	W_5	35.87	0.9853	0.9854	0.9850
h_6	W_1	36.04	0.9854	0.9851	0.9849
h_6	W_2	35.69	0.9851	0.9855	0.9830
h_6	W_3	36.04	0.9854	0.9851	0.9849
h_6	W_4	35.83	0.9852	0.9853	0.9840
h_6	W_5	36.01	0.9853	0.9852	0.9850

PSNR=36.2452 dB NHS=0.9977 NHS=0.9971 NHS=0.9979
(a) (b) (c) (d)

Figure 3.19: A sample result of the blind watermarking scheme for a formatted watermarked image at embedding strength of 5 and error controller of 0.25. (a): A formatted watermarked image. (b): Watermark extracted from V sub-bands of (a). (c): Watermark extracted from H sub-bands of (a). (d): Watermark extracted from D sub-bands of (a).

Blind watermarking scheme. Fig. 3.18 (a) shows the PSNR curves of formatted watermarked images and Figs. 3.18 (b), (c) and (d) show the NHS curves of watermarks extracted from V, H, and D sub-bands, respectively, of formatted watermarked images. The formatted watermarked images correspond to the combination of host image h_4 and watermark W_1. Fig. 3.18 (a) depicts a decrease in the PSNR with embedding strength and error controller. Moreover, PSNR curves are very close to those obtained in Experiment 1 for the proposed blind watermarking scheme. Figs. 3.18 (b), (c) and (d) depict that embedding strength and error controller affect NHSs significantly. We have observed that at an embedding strength near 5, NHSs curves are at the maximum. Moreover, NHS curves corresponding to an error controller of 0.25 have dominated. Table 3.5 gives quantitative results of the data-set for each watermarked image at embedding strength of 5 and error controller δ of 0.25. Fig. 3.19 (a) shows a formatted watermarked image which corresponds to host image h_4, original watermark W_1, embedding strength of 5 and error controller δ of 0.25. Fig. 3.19 (a) ensures no visual degradation in the watermarked image. In other experiments, we have used embedding strength of 5 and error controller δ of 0.25, unless stated. Figs. 3.19 (b), (c) and (d) show watermarks extracted from V, H and D sub-bands, respectively, of the formatted watermarked image (Fig. 3.19 (a)), and show very slight noise in the extracted watermarks. In summary, we have observed that the uint8 operation affects the performance of the blind watermarking scheme and it has very little effect when the embedding strength was near a value of 5 and error controller was near a value of 0.25. We have obtained very close results for all other combinations of host images and original watermarks of the data-set (Fig. 3.11).

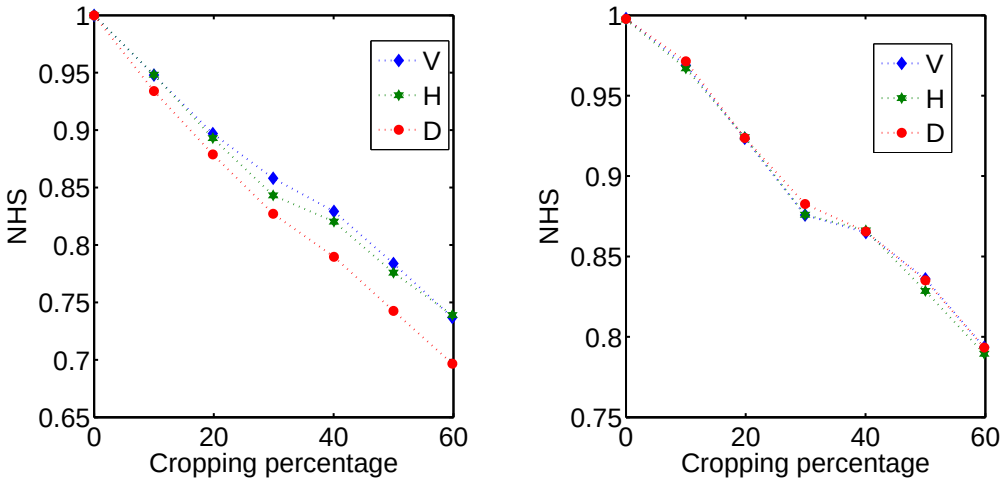


Figure 3.20: NHS curves after cropping of formatted watermarked images for combination of the host image h_4 and watermark W_1. (a): Non-blind watermarking scheme with embedding strength=3. (b): Blind watermarking scheme with embedding strength=5 and error controller=0.25.

3.4.4 Experiment 4: Attack Analysis

This experiment evaluates the performance of the proposed non-blind and blind watermarking schemes against various common image processing attacks such as cropping, Gaussian filtering, Gaussian noise and salt & pepper noise. We have applied all underlying attacks on formatted watermarked images of each combination of host images and original watermarks of the data-set (Fig. 3.11).

Cropping. In cropping, we have blackened a certain percentage of pixels from the center of the formatted watermarked images. The used cropping percentage is approximately $0, 10, \cdots, 60$. Figs. 3.20 (a) and (b) show the NHS curves for non-blind and blind watermarking schemes, respectively. The watermarks are extracted from V, H and D sub-bands of cropped formatted watermarked images. Figs. 3.20 (a) and (b) correspond to the combination of host image h_4 and original watermark W_1. Figs. 3.20 (a) and (b) depict that an increase in

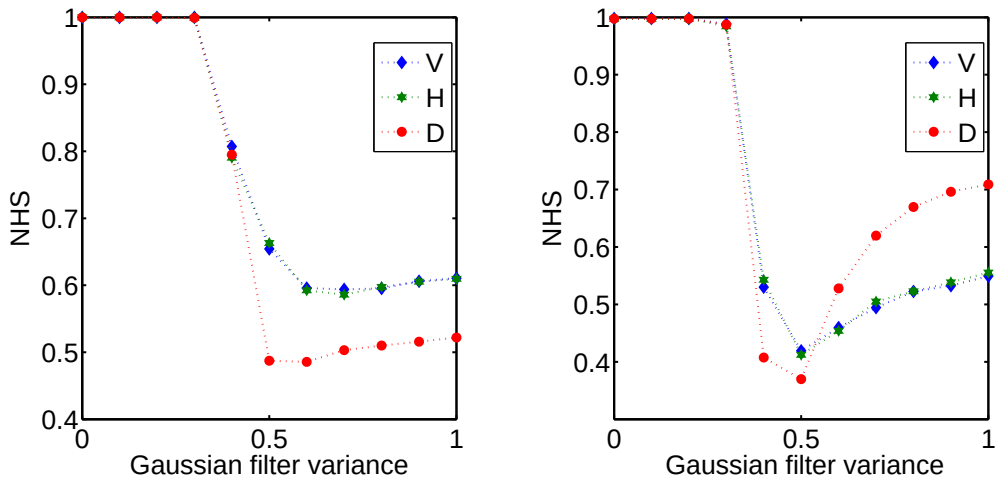
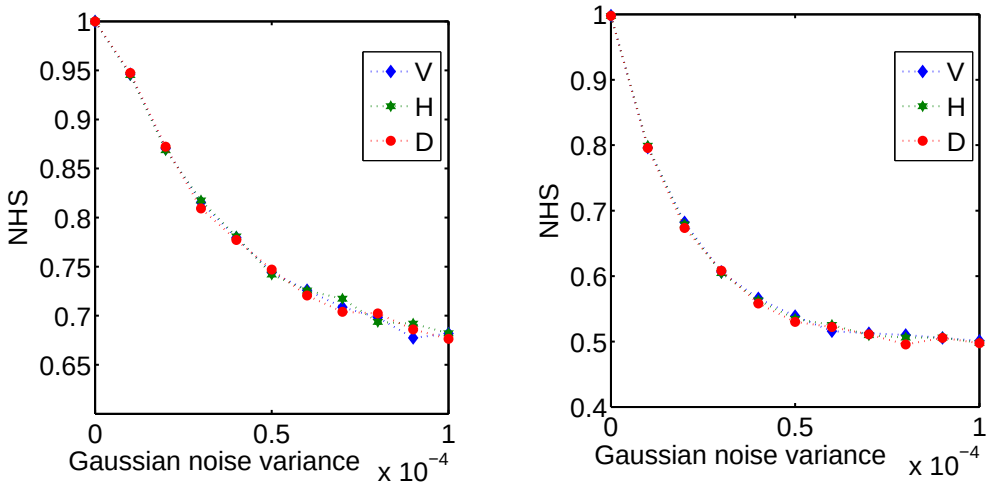


Figure 3.21: NHS curves after Gaussian filtering of formatted watermarked images for the combination of host image h_4 and watermark W_1. (a): Non-blind watermarking scheme with embedding strength=3. (b): Blind watermarking scheme with embedding strength=5 and error controller=0.25.

the cropping percentage degrades quality of extracted watermarks for both the non-blind and the blind watermarking schemes. We have obtained very close results for all other formatted watermarked images.

Gaussian filtering. This experiment applies Gaussian filter of window size 3×3 and of different variance on the formatted watermarked images. We have used different variance values as $0.1, 0.2, \cdots, 1.0$. Figs. 3.21 (a) and (b) show the NHS curves for non-blind and blind watermarking schemes, respectively. The watermarks are extracted from V, H and D sub-bands of Gaussian filtered formatted watermarked images. Figs. 3.21 (a) and (b) correspond to the combination of host image h_4 and original watermark W_1. Figs. 3.21 (a) and (b) depict that after a variance of 0.3, the quality of extracted watermarks is significantly degraded for both non-blind and blind watermarking schemes. We have obtained very close results for all other formatted watermarked images.



(a) (b)

Figure 3.22: NHS curves after adding Gaussian noise in formatted watermarked images for the combination of host image h_4 and watermark W_1. (a): Non-blind watermarking scheme with embedding strength=3. (b): Blind watermarking scheme with embedding strength=5 and error controller=0.25.

Gaussian noise. This experiment adds Gaussian noise of zero mean and of different variance in all the formatted watermarked images. The used Gaussian noise variance is 10^{-5}, 2×10^{-5}, $\cdots$, 10^{-4}. Figs. 3.22 (a) and (b) show the NHS curves for non-blind and blind watermarking schemes, respectively. The watermarks are extracted from V, H and D sub-bands of Gaussian noised formatted watermarked images. Figs. 3.22 (a) and (b) correspond to the combination of host image h_4 and original watermark W_1. Figs. 3.22 (a) and (b) depict that noise variance degrades the quality of extracted watermarks. We have obtained very close results for all other formatted watermarked images.

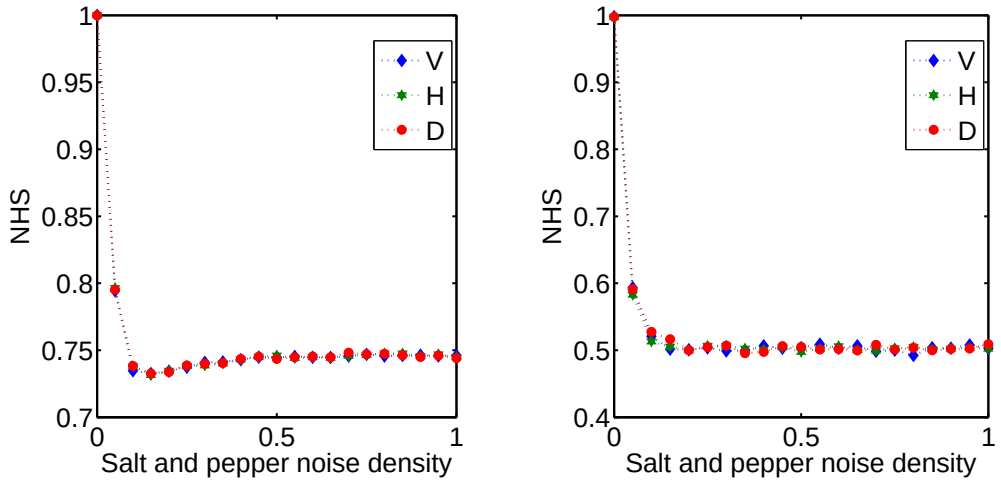


Figure 3.23: NHS curves after adding salt & pepper noise in formatted watermarked images for the combination of host image h_4 and watermark W_1. (a): Non-blind watermarking scheme with embedding strength=3. (b): Blind watermarking scheme with embedding strength=5 and error controller=0.25.

Salt & pepper noise. This experiment mixes salt & pepper noise of different density in all the formatted watermarked images. The used salt & pepper noise density is $0.05, 0.10, \cdots 1.0$. Figs. 3.23 (a) and (b) show the NHS curves for non-blind and blind watermarking schemes, respectively. The watermarks are extracted from V, H and D sub-bands of salt & pepper noised formatted watermarked images. Figs. 3.23 (a) and (b) correspond to the combination of host image h_4 and original watermark W_1. Figs. 3.23 (a) and (b) depict that the addition of noise significantly degrades the quality of extracted watermarks. We have obtained very close results for all other formatted watermarked images.

Table 3.6: Comparison of different watermarking schemes for host images of size 256×256 pixels. logo: meaningful binary logo, random: random binary sequence.

Scheme	Domain	Length of watermark (pixels)	Capacity (bits)	Watermarks
Blind*	ROWT	$3 \times 128 \times 128$	44,410	logo
Non-blind*	ROWT	$3 \times 128 \times 128$	44,410	logo
Loo [133]	DTCWT	–	5,300	random
Terzija [213]	DTCWT	180	≤ 180	random
Coria [37]	DTCWT	1,024	$\leq 1,024$	random
LFC-DE [239]	DTCWT	200	≤ 200	random
GHFC-DE [239]	DTCWT	700	≤ 700	random

*Proposed schemes

3.4.5 Experiment 5: Comparison Without any Attack

This experiment compares different related watermarking schemes under a condition that no attack/image processing operation is applied on watermarked images. For comparison, we have considered host images of size 256×256 pixels. We have compared the size of the watermarks, the capacity (appendix A.2) and the type of embedded watermarks. Capacity measures the maximum amount of information that can be reliably hidden/extracted. Higher capacity guarantees more information. Capacity and NHS play the same role if the lengths of the watermarks are equal. However, higher NHS does not always guarantee more information (small sized watermarks can have higher NHS but less information). Therefore, we have used capacity to measure the amount of hidden/extracted information.

Table 3.6 gives a comparison between different related watermarking schemes. From table 3.6, we observe that the length of the watermarks and the capacity in the proposed watermarking schemes are much higher than the existing watermarking schemes. The proposed non-blind and blind watermarking schemes have same watermark length and equal capacity. In the proposed watermarking schemes, meaningful binary logos have been used as watermarks. Note that, in this experiment, we have considered all the combinations of host images and original watermarks of the data-set (Fig. 3.11) for the proposed non-blind and blind watermarking schemes.

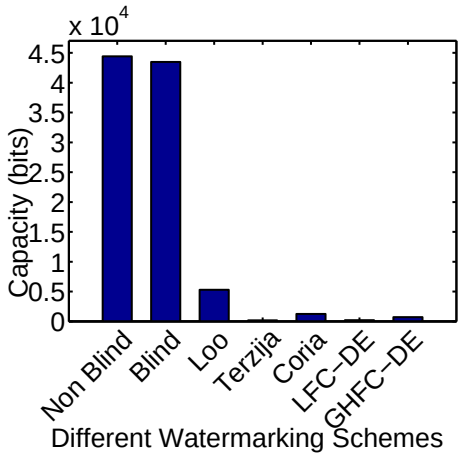


Figure 3.24: Comparison of robustness different watermarking schemes after a formatting attack on the watermarked images. Capacities of the proposed non-blind and blind watermarking schemes are evaluated for the data-set (Fig. 3.11).

3.4.6 Experiment 6: Robustness Comparison

This experiment compares the robustness of different related watermarking schemes against various common attacks. We have used capacity (section A.2) to compare robustness of watermarking schemes. Higher capacity ensures higher robustness. In this experiment, we have evaluated the capacity of the proposed non-blind and blind watermarking schemes after corresponding attacks on watermarked images. Note that the capacity evaluation for the proposed watermarking schemes considers all the combinations of host images and watermarks of the data-set (Fig. 3.11) at the points of evaluation. The reported capacity of existing watermarking schemes is without any attack and have been computed by using the results available in literature.

Formatted watermarked images. Fig. 3.24 gives the capacity of the proposed watermarking schemes after formatting attack on the watermarked images. From Fig. 3.24, we observe the following:

- Robustness of the proposed non-blind watermarking scheme is the best.

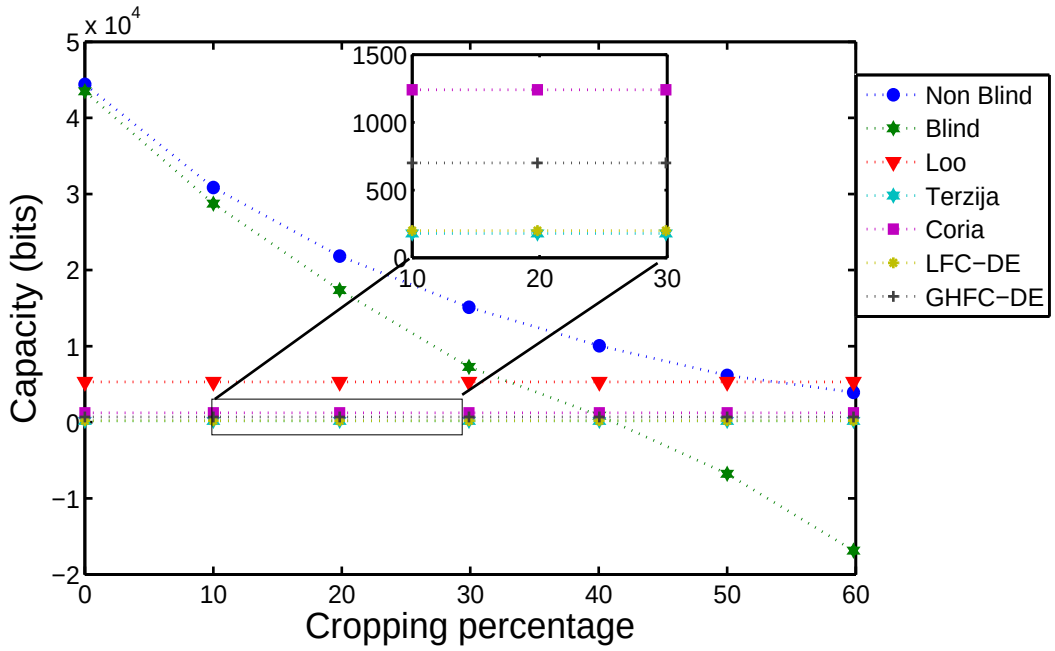


Figure 3.25: Comparison of robustness of different watermarking schemes after cropping the formatted watermarked images. Capacities of the proposed non-blind and blind watermarking schemes are evaluated for the data-set (Fig. 3.11).

- Robustness of the proposed blind watermarking scheme is slightly less than proposed non-blind watermarking scheme.
- Robustness of other schemes is very less than the robustness of the proposed schemes.

Cropping. Cropping attack of different cropping percentage is applied on formatted watermarked images. Fig. 3.25 gives capacity of the proposed watermarking schemes with respect to cropping percentage. Fig. 3.25 depicts the following:

- Increase in cropping percentage decreases the capacity of non-blind and blind watermarking schemes.
- Non-blind watermarking scheme has the highest robustness.
- Blind watermarking scheme has the second highest robustness up to 30 percent cropping.

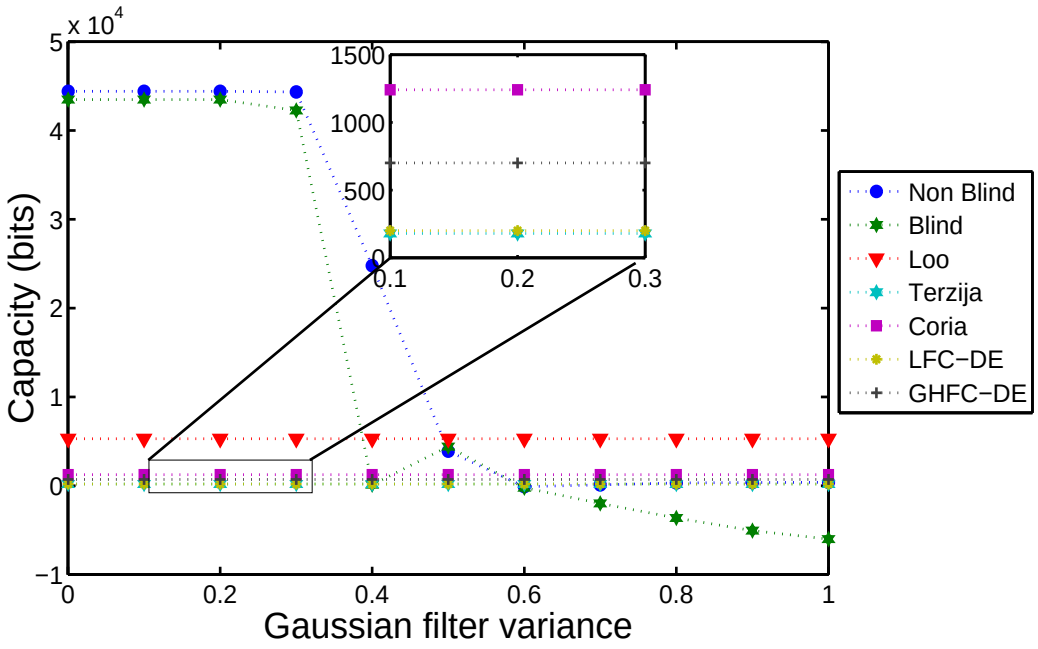


Figure 3.26: Comparison of robustness of different watermarking schemes after Gaussian filtering the formatted watermarked images. Capacities of the proposed non-blind and blind watermarking schemes are evaluated for the data-set (Fig. 3.11).

Gaussian filtering. Gaussian filter of window size 3×3 of different variance is applied on formatted watermarked images. Fig. 3.26 gives capacity of the proposed schemes with respect to variance of Gaussian filter. Fig. 3.26 depicts the following:

- Variance of Gaussian filter does not affect the capacities of the proposed non-blind and blind watermarking schemes up to a filter variance of 0.3. After that, capacity of both watermarking schemes decrease with respect to variance.
- Non-blind watermarking scheme has the highest robustness up to a filter variance of 0.5.
- Blind watermarking scheme has the second best robustness up to a filter variance of 0.5.

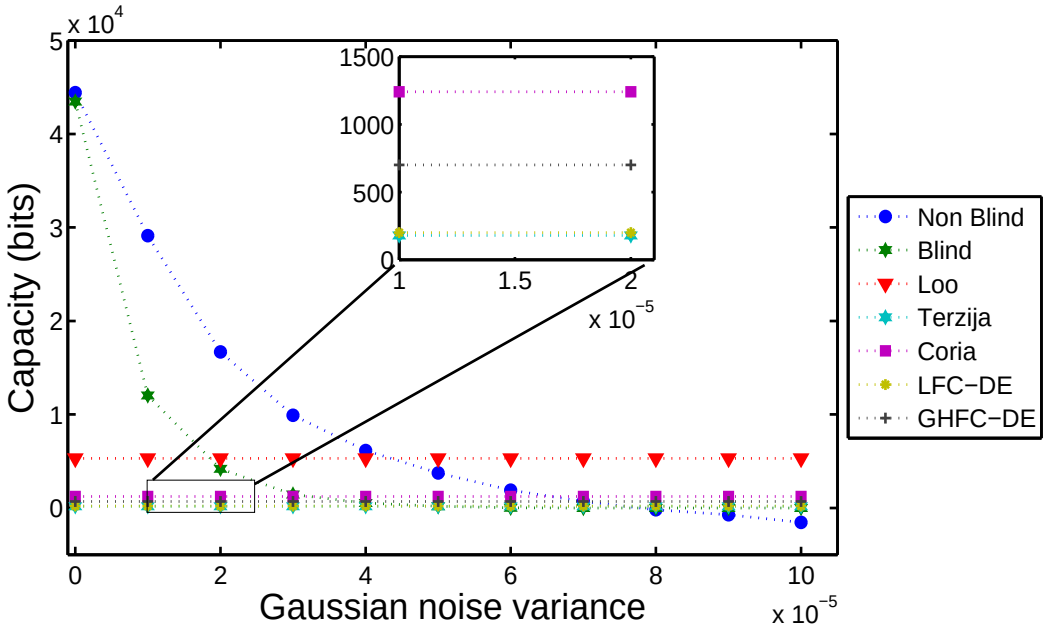


Figure 3.27: Comparison of robustness of different watermarking schemes after adding Gaussian noise in the formatted watermarked images. Capacities of the proposed non-blind and blind watermarking schemes are evaluated for the data-set (Fig. 3.11).

- Capacity of non-blind watermarking scheme is saturated with respect to variance after a filter variance of 0.6. Moreover, the capacity of the non-blind watermarking scheme converges to the reported capacity of the Terzija et al. [213] scheme, Coria et al. [37] scheme, and LFC-DE and GHFC-DE [239] schemes after a filter variance of 0.6.

Gaussian noise. Gaussian noise of different Gaussian noise variance is added in the formatted watermarked images. Fig. 3.27 gives the capacity of the proposed watermarking schemes with respect to variance of Gaussian noise. Fig. 3.27 depicts the following.

- Capacity of non-blind and blind watermarking schemes decreases with respect to noise variance.

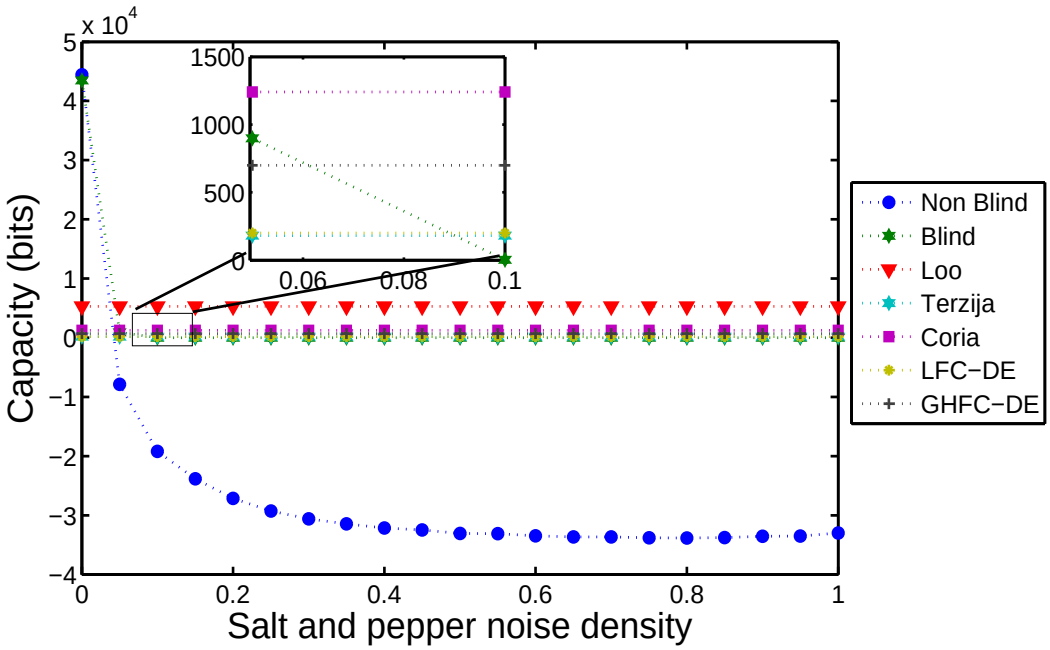


Figure 3.28: Comparison of robustness of different watermarking schemes after adding salt & pepper noise in the formatted watermarked images. Capacities of the proposed non-blind and blind watermarking schemes are evaluated for the data-set (Fig. 3.11).

- Non-blind watermarking scheme has the best robustness up to a noise variance of 5×10^{-5}.
- Blind watermarking scheme has the second best robustness up to a noise variance of 2×10^{-5}.
- Capacity of the blind watermarking scheme converges to the reported capacity of the Terzija et al. [213] scheme, Coria et al. [37] scheme, and LFC-DE and GHFC-DE [239] schemes, after a noise variance of 3×10^{-5}.

Salt & pepper noise. Salt & pepper noise of different noise densities is added in the formatted watermarked images. Fig. 3.28 gives the capacity of the proposed watermarking schemes with respect to noise densities. Fig. 3.28 depicts the following:

- Capacity of non-blind and blind watermarking schemes drastically decreases with respect to noise density.
- Non-blind and blind watermarking schemes have the best robustness up to noise density of 0.05.
- Non-blind watermarking scheme has moderate robustness from a noise density of 0.1.
- Capacity of the blind watermarking scheme converges to the reported capacity of Terzija et al. [213] scheme, Coria et al. [37] scheme, and LFC-DE and GHFC-DE [239] schemes, after a noise density of 0.1.

3.5 Conclusions

In this chapter, non-blind and blind watermarking schemes have been developed in the ROWT domain. The proposed watermarking schemes have improved capacity and watermark length. The drastic improvement in the capacity and the length of the watermarks is achieved due to the observed property of the ROWT. Experiments are conducted on a data-set of six gray scale images and five meaningful binary logo watermarks. Experimental results reveal the following:

- The capacity of the proposed non-blind watermarking scheme and the visual quality of the corresponding watermarked images change with the embedding strength. We have found that the embedding strength of a value near 3 is optimal for formatted watermarked images. Near optimal embedding strength, the capacity is at its maximum and formatted watermarked images are visually undistinguishable from the corresponding original images.

- The performance of the blind watermarking scheme can be controlled by the embedding strength and the error controller. We have found that the embedding strength and error controller pair is optimal near tuple of (5,0.25) for formatted watermarked images. Near an optimal pair, capacity is at its maximum and formatted watermarked images are visually undistinguishable from corresponding original images.

- Positive sub-bands can be used for a traditional non-blind watermarking scheme as extracted watermarks from the positive sub-bands are very close to the original watermarks. However, for a traditional blind watermarking scheme, extracted watermarks from all sub-bands are very noisy. Therefore, the observed property of the ROWT is significant for blind watermarking scheme and is slightly important for the non-blind watermarking scheme.

- We have tested both proposed watermarking schemes against various attacks such as cropping, Gaussian filter, Gaussian noise and salt & pepper noise. We have observed that the proposed non-blind and blind watermarking schemes have better robustness than existing DTCWT based watermarking schemes. Moreover, the proposed non-blind watermarking scheme has better robustness than the proposed blind watermarking scheme.

Chapter 4

Watermarking Schemes to Secure the Face Database and Test Images in a Biometric System

This chapter attempts to solve the integrity issues of a compromised face biometric system using two watermarking schemes. Two new blind watermarking schemes, namely S_1 and S_2, are proposed to ensure the integrity of the training face database and of the test images, respectively. Scheme S_1 is fragile spatial-domain based and scheme S_2 works in the discrete cosine transformation (DCT) domain and is robust to channel noise. The novelty of S_1 lies in the fact that it is reversible and the ratio of watermark bits to the size of the host image is 2.67, while S_2 has better robustness than existing blind watermarking schemes. The performance of both schemes has been evaluated on a subset of the Indian face database and the results show that both schemes verify the integrity with very high accuracy without affecting the performance of the biometric system.

The rest of the chapter is organized as follows. Section 4.1 provides overview of problem and its solution. Related work has been discussed in section 4.2. The

proposed schemes S_1 and S_2 are described in sections 4.3 and 4.4, respectively. The experiments, results and analysis are provided in Section 4.5. Finally, the concluding remarks are given in Section 4.6.

4.1 Overview of the Problem and its Solution

In recent years, the use of biometrics has increased to enhance the security and convenience in society. However, the design of a practical biometric system faces many critical issues such as accuracy, computation speed, cost, scalability, and security.

This chapter focuses on the security issues associated with a biometric system. The common attacks on biometric systems include coercive attacks, impersonation attacks, replay attacks and attacks on the feature extractor, template database, matcher and matching results [180]. The attackers can alter the biometric images or templates and can degrade the performance of a biometric system. Therefore, securing biometric data from such attacks is of utmost importance.

A typical biometric identification/verification system is shown in Fig. 4.1(a). The biometric data captured by the biometric sensor is sent to a machine S via a channel C_2. Then the matcher (in S) compares the output of the feature extractor (in S), i.e., the features, with the template available from the database (in S). In this system, although security issues can occur in many components, we assume that the two components, the template database and channel C_2, are compromised. Therefore, an adversary can alter the template database and the captured biometric data on C_2. In addition, C_2 may be noisy. In this chapter, our aim is to provide a solution for verifying the integrity of the underlying biometric system. The main requirements in the solution are as follows:

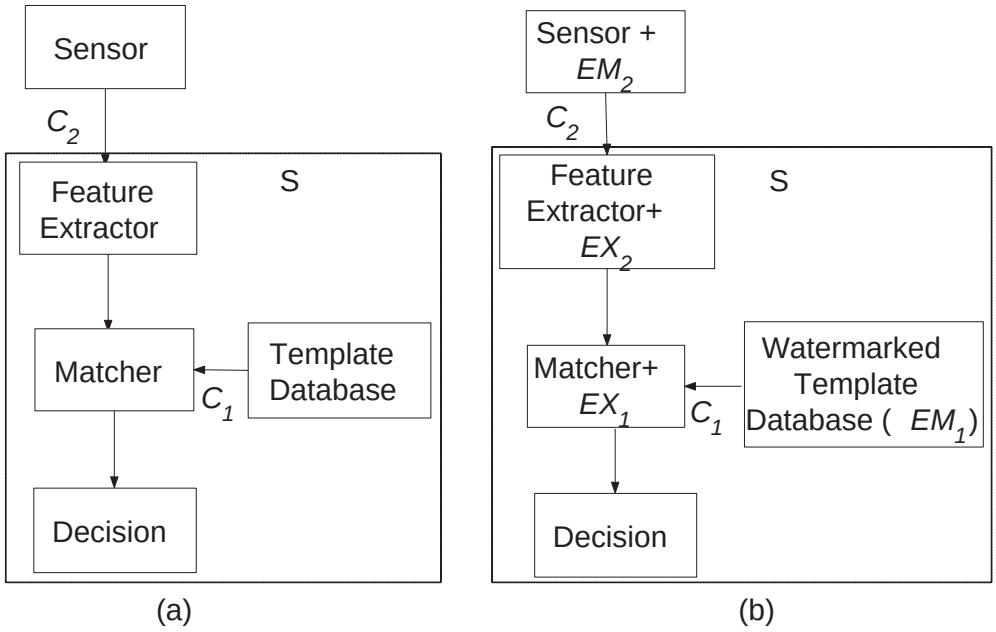


Figure 4.1: (a) A partially compromised biometric system (b) The proposed watermarking based secure biometric system EM_1: Watermark Embedder of S_1, EX_1: Watermark Extractor of S_1, EM_2: Watermark Embedder of S_2, EX_2: Watermark Extractor of S_2

1. Any kind of modification in the training (template) database is considered as an attack. Therefore, template database must be treated as tampered, if any modification has been done on it.

2. Channel C_2 is noisy and additive white noise is added in the transmitted images. Therefore, white noise added test images must be treated as authentic images.

3. Adversary can alter the test image over channel C_2. Therefore, altered test images must be treated as tampered images.

In this chapter, we have analyzed a watermarking scheme based solution for a face biometric system. The functioning of the face biometric system is based on Turk et al. [220]. We have proposed two watermarking schemes, namely S_1 and S_2, to solve the problems associated with template database and test images respectively. Fig. 4.1(b) shows the overview of the proposed updated biometric system.

The stepwise details of working of the updated biometric system to solve the problem associated with template database are as follows:

1. Template database is watermarked using the watermark embedding algorithm EM_1 of scheme S_1.

2. The watermarked template database is transmitted to the matcher unit via channel C_1.

3. Watermark is extracted from the received template database using the watermark extraction algorithm EX_1 of scheme S_1.

4. Extracted watermark is verified to ensure the integrity of the received template database.

Similarly, the stepwise details of working of the updated biometric system to solve the problem associated with test images are as follows:

1. The test image captured at the sensor is watermarked using the watermark embedding algorithm EM_2 of S_2.
2. The watermarked test image is transmitted to the feature extractor unit via channel C_2.
3. Watermark is extracted from the received test image using the watermark extraction algorithm EX_2 of S_2.
4. Extracted watermark is verified to ensure the integrity of the received test image.

The practical constrains of the underlying biometric system are as follows:

1. The unit feature extractor and matcher do not have verified original watermark.
2. The unit feature extractor does not have verified original test image.
3. The unit matcher does not have verified original template data base.
4. The identification/verification accuracy of a biometric system is very sensitive to change in template database.

The watermarking schemes S_1 and S_2 should be designed/selected according to the following fundamental rules.

1. Requirements of the underlying biometric system must be fulfilled.
2. The practical constraints of the underlying biometric system should not be violated.
3. The identification/verification accuracy of the underlying biometric system should not be degraded.

Table 4.1: A summary of different watermarking schemes from different aspects. (RDWT: redundant discrete wavelet transform, MFCC: mel frequency cepstral coefficients, SVD: singular value decomposition)

Work	Extractor	Kind of scheme	R	Robustness	Embedding domain	Kind of watermark
Barni et al. [11]	no	blind	< 0.25	semi-fragile	DWT	random
Jain et al. [85]	yes	blind	< 0.2	robust	spatial	biometric information
Rangaswamy [177]	yes	blind	< 0.25	robust	spatial	logo
Kim et al. [104]	yes	blind	0.0625	semi-fragile	spatial	thumbnail
Lin et al. [127]	yes	blind	< 1	robust	DWT	logo
Vatsa et al. [221]	yes	semi-blind	< 1	robust	RDWT	MFCC
Abdallah et al. [2]	yes	blind	0.03125	robust	DWT	random
Bhatnagar [14]	yes	semi-blind	> 1	robust	RDWT+SVD	binary logo
Su et al. [205]	yes	blind	< 1	semi-fragile	DWT	logo
Yanga et al. [231]	yes	blind	0.0625	robust	QFT	logo
Proposed S_1	yes	blind	2.67	fragile	spatial	eigenface
Proposed S_2	yes	blind	0.0035	robust	DCT	eigenface coefficient

4.2 Related Work

A significant amount of work has been done in the area of image watermarking. Researchers have proposed many watermarking schemes including biometric watermarking, robust and fragile watermarking, and blind and semi-blind watermarking [11, 85, 177, 104, 127, 221, 2, 14, 205, 231]. In most of the past work (except Bhatnagar et al. [14]), the value of R that is the ratio of watermark bits to the size of the host image, is usually less than one.

Table 4.1 summarizes the characteristics of watermarking schemes. Work of Barni et al. [11], Jain et al. [85], Rangaswamy et al. [177], Kim et al. [104], Lin et al. [127], Abdallah et al. [2], Su et al. [205] and Wanga et al. [231] fall in the category of robust/semi-fragile and blind watermarking schemes. In Barni et al. [11], watermarking is done in the wavelet domain. The watermark detector is modeled on the assumptions that watermark coefficients and wavelet coefficients of a host image are independent random variables and have zero mean. However, the set of test face images and its projection images violate these assumptions. Kim et al. [104] have proposed a watermarking scheme to verify the integrity of the fingerprint image and the face image. The integrity of watermarked fingerprint image is verified by the face image and vice versa. Hence, the scheme of Kim et al. [104] cannot be used in the case of a single biometric system. Moreover, if one of the two biometrics is genuine and the another is tampered, then both are detected as tampered. In another work, Su et al. [205] have proposed a watermarking scheme using integer wavelet transform and state coding. In this scheme, the original watermark is encoded before embedding and the dynamic range of the watermark is small. Yang et al. [231] have proposed a quaternion Fourier transform (QFT) based watermarking scheme. The time complexity of QFT is usually more than that of DCT and discrete wavelet transform (DWT). Moreover, QFT based image processing techniques are in their

early stages. Jain et al. [85] have proposed the watermarking scheme based solution for the security of fingerprint and face biometrics. Rangaswamy et al. [177], Lin et al. [127] and Abdallah et al. [2] have proposed watermarking algorithms in which a binary watermark is being used.

4.3 Watermarking Scheme S_1

We have proposed a watermarking scheme S_1 that provides security solution associated with template database. The template data-base consists of M training face images $\Lambda_1, \Lambda_2, \cdots \Lambda_M$. The watermarking scheme S_1 has been designed according to the fundamental rules as discussed in section 4.1. The characteristics of the watermarking scheme are as follows:

1. S_1 is very fragile to fulfill the first requirement of the solution.

2. S_1 is a blind watermarking scheme as original template database is not available at the matcher.

3. Watermark is eigen-faces (a function of original original database) of the training face images. It helps to verify the extracted watermark without the need of original watermark at the matcher.

4. The eigen-faces are embedded in the training face-image to obtain the watermarked training face images.

5. The watermarking scheme is reversible. Reversibility helps to exactly reconstruct the original training face images from the watermarked training face images.

6. The watermark is embedded in spatial domain.

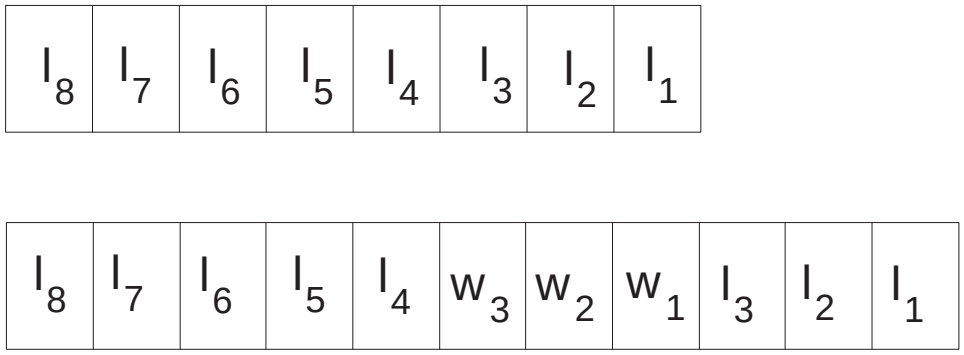


Figure 4.2: Core idea of scheme S_1

The watermarking scheme S_1 consists of two algorithms:

- Watermark embedding algorithm EM_1.
- Watermark extraction and original training face images reconstruction algorithm EX_1.

The algorithm EM_1 embeds M' dominant eigen-faces of the original training face images $\Lambda_1, \Lambda_2, \cdots, \Lambda_M$ in it to obtain the watermarked training face images. The core idea of the algorithm EM_1 is to increase the bit depth of each pixel of the original training face images. Fig. 4.2 explains the overview of this idea. In Fig. 4.2, $\mathrm{l}_1, \mathrm{l}_2, \cdots, \mathrm{l}_8$ represent eight bits of a pixel of an original image and $\mathrm{w}_1, \mathrm{w}_2$ and w_3 represent three bits of a watermark. The three bits $(\mathrm{w}_1, \mathrm{w}_2, \mathrm{w}_3)$ have been inserted between fourth and third least significant bits of the pixels as shown in Fig. 4.2. This process has been repeated till all bits of the watermark are inserted. The algorithm EX_1 extracts eigen-faces and reconstructs the original training face images (original template database) from watermarked training face images. The step wise details of the algorithms EM_1 and EX_1 are discussed in the algorithms 11 and 12 respectively.

Algorithm 11 EM_1: Watermark embedding algorithm of scheme S_1.

Input: M training face images $\Lambda_1, \Lambda_2, \cdots, \Lambda_M$; M'; key K to select pixels for watermarking

Output: Watermarked training face images $\Lambda'_1, \Lambda'_2, \cdots, \Lambda'_M$

1: Compute M' dominant eigen-faces of $\Lambda_1, \Lambda_2, \cdots, \Lambda_M$ using Turk et al. [220]. Store M' dominant eigen-faces as $u_1, u_2, \cdots u_{M'}$.

2: Compute eight-bits binary representation of $u_1, u_2, \cdots u_{M'}$ as discussed in Agarwal et al. [3]. Store the binary representation as $u^*_1, u^*_2, \cdots u^*_{M'}$.

3: Construct a watermark $W = [u^*_1, u^*_2, \cdots u^*_{M'}]$.

4: Compute $\eta = \lceil 8 \times \frac{M'}{M} \rceil$.

5: Insert η bit planes $(w_1, w_2, \cdots, w_\eta)$ between third and fourth least significant bit planes of all the training face images. Store the resultant training face images as $\Lambda^0_1, \Lambda^0_2, \cdots, \Lambda^0_M$.

6: Construct template database $\mathbf{\Lambda}^0 = [\Lambda^0_1, \Lambda^0_2, \cdots \Lambda^0_M]$.

7: Compute the total number of bits in W. Store it as c.

8: Select $\left\lceil \frac{c}{\eta} \right\rceil$ pixels of the $\mathbf{\Lambda}^0$ using the key K. Denote the set of selected pixels as H.

9: Embed the watermark W into the bit planes $w_1, w_2, \cdots, w_\eta$ of $\mathbf{\Lambda}^0$ as follows:
h=first element of H, $j = 1$;
for i=1:1:c
$w_j(h) = \begin{cases} 0 & \text{if watermark bit } W(i) \text{ is } 0 \\ 1 & \text{if watermark bit } W(i) \text{ is } 1 \end{cases}$;
if$(j == \eta)$
$j = 1$;
h=next element of H;
else
$j = j + 1$;
end
end

10: Store the resultant template database as $\mathbf{\Lambda}^{00}$.

11: **Return** Watermarked template database $\mathbf{\Lambda}^{00} = [\Lambda'_1, \Lambda'_2, \cdots, \Lambda'_M]$.

Algorithm 12 EX_1: Watermark extraction algorithm of scheme S_1

Input: Watermarked training face images $\hat{\Lambda}'_1, \hat{\Lambda}'_2, \cdots, \hat{\Lambda}'_M$ (may be tampered); M', key K same as used in algorithm 11.

Output: Extracted eigen-faces $\hat{u}_1, \hat{u}_2, \cdots \hat{u}_{M'}$; reconstructed training face images $\hat{\Lambda}_1, \hat{\Lambda}_2, \cdots, \hat{\Lambda}_M$

1: Compute $\eta = \left\lceil 8 \times \frac{M'}{M} \right\rceil$.

2: Construct $\hat{\mathbf{\Lambda}}^0 = [\hat{\Lambda}^0_1, \hat{\Lambda}^0_2, \cdots \hat{\Lambda}^0_M]$.

3: Extract $4^{th}, 5^{th}, \cdots, (3+\eta)^{th}$ LSB planes from the $\hat{\mathbf{\Lambda}}^0$. Store these planes as $\hat{w}_1, \hat{w}_2, \cdots, \hat{w}_\eta$.

4: Remove $4^{th}, 5^{th}, \cdots, (3+\eta)^{th}$ LSB planes from the $\hat{\mathbf{\Lambda}}^0$. Store the result as $\hat{\mathbf{\Lambda}}^{00}$.

5: Obtain reconstructed face images $\hat{\Lambda}_1, \hat{\Lambda}_2, \cdots, \hat{\Lambda}_M$ from the $\hat{\mathbf{\Lambda}}^{00}$.

6: Find set of watermarking pixels H in $\hat{\Lambda}^0$ using the key K.

7: Compute $c = 8 \times \left\lfloor \frac{\eta \times |H|}{8} \right\rfloor$, where, $|H|$ is cardinality of set H.

8: Find the ordered set $\hat{W}$ of extracted watermark bits as follows:
h=first element of H, $j = 1$;
for i=1:1:c
$\hat{W}(i) = \begin{cases} 0 & \text{if watermark bit } \hat{w}_j(h) \text{ is } 0 \\ 1 & \text{if watermark bit } \hat{w}_j(h) \text{ is } 1 \end{cases}$;
if$(j == \eta)$
$j = 1$;
h=next element of H;
else
$j = j + 1$;
end
end

9: Construct M' eigen-faces $\hat{u}_1, \hat{u}_2, \cdots \hat{u}_{M'}$ from the $\hat{W}$.

10: **Return** Extracted eigen-faces $\hat{u}_1, \hat{u}_2, \cdots \hat{u}_{M'}$; reconstructed face images $\hat{\Lambda}_1, \hat{\Lambda}_2, \cdots, \hat{\Lambda}_M$.

4.4 Watermarking Scheme S_2

We have proposed a watermarking scheme S_2 that provides security solution associated with a test face image Λ. The watermarking scheme S_2 is according to those fundamental rules as discussed in section 4.1. The characteristics of the watermarking scheme are as follows:

1. S_2 is robust against white noise to fulfill the second requirement of the solution.
2. S_2 is a blind watermarking scheme as original test face image is not available at feature extractor.
3. Watermark is a projection image Ω [220] (a function of original test image) of the test face image. It helps to verify the extracted watermark without the need of original watermark at the feature extractor.
4. The projection image is embedded in the test face image to obtain the watermarked test face image such that watermarked as well as original test face images have same projection image. This eliminates the need of original test face image at the feature extractor.
5. The watermark is embedded in the DCT domain.

The watermarking scheme S_2 consists of two algorithms:

- Watermark embedding algorithm EM_2.
- Watermark extraction algorithm EX_2.

The algorithm EM_2 embeds projection image of the original test face image into itself. The key idea of the algorithm EM_2 is to select the pixels for watermarking in the DCT domain and replace their magnitude by a preselected number. The selection

of pixels is based on their magnitude. The algorithm EX_2 extracts projection image from the watermarked test face image. The extraction is done from the DCT domain pixels of the watermarked test face images whose magnitude is less than the sum of the preselected numbers within a threshold. The step wise details of the algorithms EM_2 and EX_2 are discussed in the algorithms 13 and 14 respectively.

Algorithm 13 EM_2: Watermark embedding algorithm of scheme S_2

Input: Test face image Λ, M' eigen-faces, watermarking parameter z.
Output: Watermarked test face image Λ_W.

1: Compute projection image $\Omega = [\omega_1, \omega_2 \cdots, \omega_{M'}]$ according to [220] using the M' eigen-faces of $\Lambda'_1, \Lambda'_2, \cdots \Lambda'_M$.
2: Compute

$$t = \left\lceil \log_2 \left(\max_{i=1,2,\cdots,M'} \lfloor |\omega_i| \rfloor \right) \right\rceil + 8. \tag{4.1}$$

3: Find t bits binary representation of each coefficient of Ω. Store the result as $\Omega* = [\omega_1*, \omega_2 * \cdots, \omega_{M'}*]$.
4: Compute total number of bits in $\Omega*$ as $t_1 = t \times M'$.
5: Apply DCT on Λ. Store the result as Λ_{DCT}.
6: Find t pixels of lowest magnitude in the Λ_{DCT}. Denote the set of these pixels by P.
7: Embed the $\Omega*$ in the Λ_{DCT} as follows:
for $i = 1 : 1 : t_1$

$$\Lambda_{DCT}(P(i)) = \begin{cases} z & \text{if } \Omega^*(i) = 1 \\ -z & \text{if } \Omega^*(i) = 0 \end{cases};$$

end
8: Apply the inverse DCT on the Λ_{DCT} to obtain the watermarked image Λ_W
9: **Return** Watermarked test face image Λ_W.

Algorithm 14 EX_2: Watermark extraction algorithm of scheme S_2

Input: Watermarked test face image: $\hat{\Lambda}_W$ (may be noisy or altered), M', watermarking parameter: z, error resistance parameter: δ, number of bits per coefficient of projection image: t

Output: Extracted projection face image $\hat{\Omega}$

1: Compute $t_1 = t \times M'$.

2: Apply DCT on the $\hat{\Lambda}_W$. Store the result as $\hat{\Lambda}_{WDCT}$.

3: Find the pixels in $\hat{\Lambda}_{WDCT}$, whose magnitude is between $z - \frac{\delta}{2}$ to $z + \frac{\delta}{2}$. Denote the set of these pixels by P.

4: Find the ordered set $\hat{W}$ of extracted watermark bits as follows:

for $i = 1 : 1 : t_1$

$$\hat{W}(P(i)) = \begin{cases} 1 & \text{if} \quad z - \frac{\delta}{2} < \hat{\Lambda}_{WDCT}(P(i)) < z + \frac{\delta}{2} \\ 0 & \text{if} \quad -z - \frac{\delta}{2} < \hat{\Lambda}_{WDCT}(P(i)) < -z + \frac{\delta}{2} \end{cases} ;$$

end

5: Apply binary decoding on $\hat{W}$ to obtain the extracted projection face image. Store the result as $\hat{\Omega} = [\hat{\omega}_1, \hat{\omega}_2 \cdots, \hat{\omega}_{M'}]$.

6: **Return** extracted projection face image $\hat{\Omega}$.

4.5 Experiments, Results and Analysis

4.5.1 Performance Metric

In general, a watermarking scheme is evaluated by the visual degradation in the host image that occurs due to the insertion of a watermark, error in the extracted watermark and the attacks that it may resist. However, the main purpose of a biometric system is to make the decisions for integrity/verification/identification. Hence, in any biometric watermarking scheme, the accuracy of the watermarked biometric system also needs to be examined. The peak-signal-to-noise ratio (PSNR) is used to analyze the difference in visual quality between the original image and the watermarked image. The normalized correlation coefficient (NC) measures the similarity between the original watermark and the extracted watermark. In this chapter, accuracy is measured by true results in the integrity verification results of the training database and the test face images. The methods to verify the integrity of training and test data in a watermarked face biometric system are as follows.

Verifying the integrity of the training face database

Watermarking scheme S_1 helps to verify the integrity of a training database. EX_1 extracts M' eigenfaces and reconstructs the training database from the training database received via channel C_1. The NC values are calculated between the extracted eigenfaces and the corresponding eigenfaces that has been computed using the reconstructed training database. If all NC values are greater than the predetermined threshold τ_1, then the integrity of the training database will be accepted and the test face image integrity verification will be followed. Otherwise, it is decided that the training database is tampered/attacked.

Verifying the integrity of the test face image

Watermarking scheme S_2 helps to verify the integrity of the face image received via channel C_2. EM_2 extracts the projection image from the received face image. Since the projection face images are usually compared using Euclidian distance [220], we have computed the Euclidian distance between the extracted projection image and the projection image of the received face image. If the Euclidian distance is less than τ_2 (the predetermined threshold), then the integrity of the received face image will be considered as verified. Otherwise, it will be decided that the received face image is tampered/attacked.

Figure 4.3: Training face database

4.5.2 Data Set

The performance of watermarking schemes S_1 and S_2 has been evaluated on a subset of the Indian face database [88]. The subset consists of 40 face images (10 individuals with four impressions of each). Each face image is 24-bit RGB color with a size of 640×480. Each face image has been preprocessed for use in the biometric system. It has been found that for all the face images, the window of size 300×384 contains all useful information related to a face. Hence, all the face images have been cropped by the window. The cropped face images have been resized to 256×256. The red band of these cropped and resized face images has been used to create a training

Figure 4.4: Test face images

database and a set of test face images in the biometric system. The training database consists of 30 face images (10 individuals with three impressions of each) and the set of test face images consists of 10 face images (10 individuals with a single impression of each). Fig. 4.3 shows training face images and Fig. 4.4 shows test face images. Note that the training database and the set of test face images are disjoint.

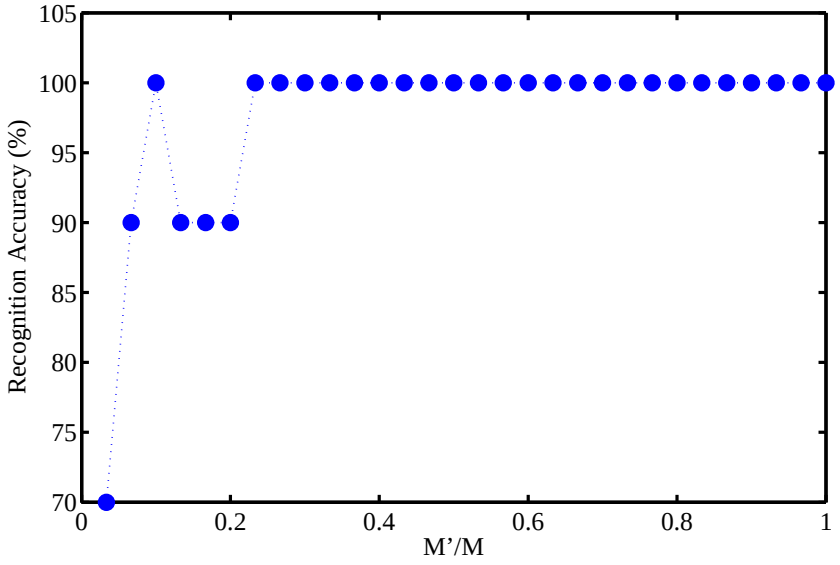


Figure 4.5: Recognition accuracy vs. ratio M'/M

4.5.3 Discussion on Results

To analyze the effect of watermarking schemes on a face biometric system, we have performed several experiments on MATLAB platform. Many variants and parameters are associated with the proposed watermarking schemes. For the given database, the value of M is 30 and the value of t as given in (4.1) is found to be 22. The value of all other parameters have been fixed that corresponds to the optimal performance of the updated biometric system. The empirically found optimal value of z is 14, δ is 12, τ_1 is 0.97 and τ_2 is 0.7.

The accuracy of face biometric system depends on the number M' of dominant eigen-faces used. Fig. 4.5 shows the accuracy of the given face biometric system with respect to the ratio $\frac{M'}{M}$, where M is 30. From Fig. 4.5, it has been observed that the accuracy of the biometric system is maximum for $\frac{M'}{M}$ greater than 0.267. To reduce the computation and communication cost, the ratio $\frac{M'}{M}$ should be minimum.

Figure 4.6: Watermarked training face images

Therefore, to maintain a trade-off balance between accuracy of the biometric system and, computation and communication cost with respect to the ratio $\frac{M'}{M}$, the value of M' is set to be 10. Therefore, $\eta = \lceil 8 \times \frac{M'}{M} \rceil$ is 3.

Secure and Noiseless Environment

This experiment has been conducted under the condition that the channels C_1 and C_2 are secured and noiseless. The aims of this experiment are as follows:

- To evaluate the performance of proposed watermarking schemes.
- To evaluate the accuracy of integrity verification of the updated face biometric system.
- To compare the recognition accuracy of the updated and traditional face biometric systems.

Figure 4.7: Reconstructed face images

Figure 4.8: Watermarked test face images

Fig. 4.6 shows the watermarked face images correspond to Fig. 4.3 that are obtained using the algorithm EM_1. Fig. 4.7 shows the reconstructed face images correspond to Fig. 4.6 that are obtained using the algorithm EX_1. The sum of absolute pixel difference between the face images in Fig. 4.6 and those in Fig. 4.7 is zero, which verifies that the watermarking scheme S_1 is reversible. Fig. 4.8 shows the watermarked images correspond to Fig. 4.4 that are obtained using scheme S_2. No visual difference has been observed between the original images and their watermarked images. The average PSNR in scheme S_1 is 38.026 dB and the average PSNR in scheme S_2 is 45.783 dB.

In scheme S_1, the NC values between all extracted eigenfaces and the corresponding computed eigenfaces have been found to be 1. Hence, the integrity of the training database is verified. In scheme S_2, the Euclidian distance between the extracted and the computed projection images from a watermarked face image is found to be less than 0.48. Hence, the integrity of all watermarked test face images is verified. Further, we have observed that the updated and traditional face biometric systems have the same face identification/verification accuracy.

Attacks on Template Database

The aim of this experiment is to study the performance of updated biometric system with respect to various kind of modifications on the training database. Table 4.2 summarizes the results of S_1 on the modified training database. As shown in the table, the maximum value of NC ranges from 0.01 to 0.93. After any modification in the training database, since the value of NC is less than τ_1, S_1 detects the forgery of the training database. However, the PSNR corresponds to the maximum value of NC is found to be 37.31 dB.

Table 4.2: Performance of S_1 against various attacks

Attack	Maximum value of NC	Corresponding PSNR (dB)
Average filter (3×3)	0.1138	30.63
Median filter (3×3)	0.9292	37.31
Gaussian filter (3×3, standard deviation=0.25)	0.3300	39.20
Laplace filter	0.0112	7.19
Salt & pepper noise (density=0.05)	0.8672	18.13
Gaussian noise (variance=0.0001)	0.0672	36.42
Face image replacement	0.5821	19.95

Unauthorized face via channel C_2

The aim of this experiment is to study the performance of updated biometric system when, 10 unmarked face images were transmitted via noiseless C_2. The minimum Euclidean distance between their extracted projection images and the computed projection images is found to be approximately 10^3, which is significantly higher than τ_2. Hence, all unauthorized submissions are correctly detected.

Noise in channel C_2

The aim of this experiment is to compare the performance of updated biometric systems with respect to different watermarking schemes for test images. This experiment has been conducted under the condition that different amount of additive white Gaussian noise (frequent noise in a transmission channel) has been added to C_2.

Comparison of scheme S_2 with the existing four schemes [85, 177, 127, 2] provides that the visual quality of the images that are watermarked by all the schemes is almost the same. The average PSNR value of the images watermarked by the schemes [85, 177, 127, 2] is approximately 45 dB.

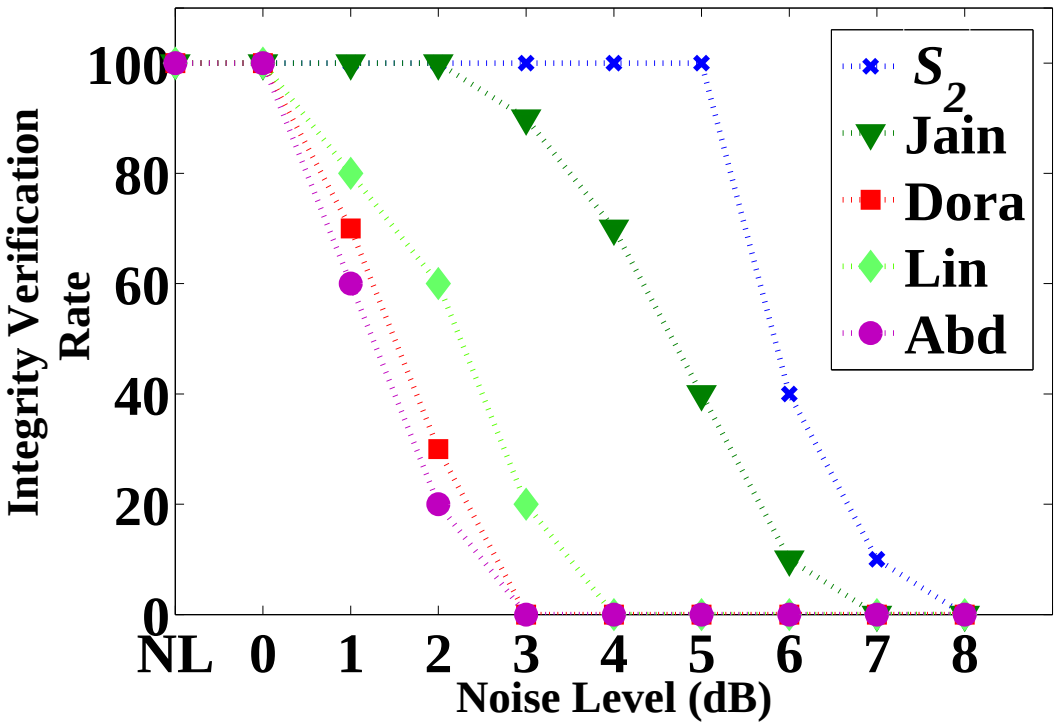


Figure 4.9: Comparison of S_2 with $[85, 177, 127, 2]$. NL: noiseless, Jain: [85], Dora: [177], Lin: [127], Abd: [2].

Fig. 4.9 compares the integrity verification accuracy of schemes S_2, Jain et al. [85], Rangaswamy et al. [177], Lin et al. [127] and Abdallah et al. [2]. From Fig. 4.9, it is observed that, till 5 dB of noise, the integrity verification accuracy of the updated biometric system is very high for scheme S_2. Beyond this, the accuracy of S_2 drops. The figure shows that for noiseless C_2, S_2 and the existing schemes have the same integrity verification rate. S_2, however, has better performance than the existing schemes for noisy C_2. Scheme S_2 works reliably till 5 dB noise level whereas the existing schemes in the literature fail to work reliably beyond the 2 dB noise level.

4.6 Conclusions

Two new blind watermarking schemes are proposed to improve the security of a face biometric system. The first watermarking scheme S_1 secures the training biometric data and the second watermarking scheme S_2 secures the test biometric data. High PSNR values ensure no visual degradation in the watermarked images. The NC value that is close to 1 without attacks on the watermarked data ensures reliable extraction of the watermark. Incorporated watermarking schemes in the face biometric system do not change face identification/verification accuracy. Various tampering operations such as smoothing, sharpening, histogram equalization, content modification and unauthorized submission are detected with very high accuracy. Furthermore, S_2 is more robust to additive white noise than the existing watermarking schemes [85, 177, 127, 2].

Chapter 5

Visible Watermarking Based on Importance and Just Noticeable Distortion of Image Regions

Visible watermarking is the process of embedding data (watermark) into a multimedia object (video/image) such that the embedded watermark is perceptible to a human observer. In certain applications, such as content protection [140], television channel logo for broadcast monitoring [40], advertisement of upcoming programs or advertisement of logos for commercial companies and digital libraries [151, 244], visible watermarking is worthy, as it immediately resolves the claim of ownership without software/hardware [134]. However, many times, visible watermarks occlude the important portion of multimedia objects. This chapter introduces a visible watermarking algorithm to embed a binary logo watermark at N non-overlapping positions in an image such that important portions of the image are not occluded. The image areas for embedding the watermark are found through visual saliency computation or available human eye fixation density maps. In the proposed visible watermarking, just noticeable distortion is used to adaptively filter the watermark

embedding energy based on the image content. A mathematical model in terms of information-content-weighted-structural-similarity-index and visual importance is proposed to find optimal watermark embedding strength. We have tested our algorithm on several color images of different sizes and on several binary watermarks of different sizes. We have compared the proposed algorithm with the state of art. The watermarking results are found to be very promising and watermarks do not hide details of any test image unlike the state of art.

The rest of the chapter is organized as follows. Section 5.1 discusses background of the problem. Section 5.2 introduces the overview of the solution of the problem. Visible watermarking algorithm for an image is explained in section 5.3. Experimental results are discussed in section 5.4 followed by conclusions in section 5.5.

5.1 Background

This section discusses the literature on visible watermarking, formulation of problem in visible watermarking, overview of proposed solution of the formulated problem and explicit contributions to solve the problem.

5.1.1 Related Work

Kankanhalli et al. [96] proposed a visible watermarking algorithm that classifies each block of 8×8 of pixels into one of 8 classes depending on the sensitivity of the block to distortion. Texture, edge and luminance information in the block were used for this purpose. The embedding process was automated and the bits were embedded in the discrete cosine transform (DCT) domain. The watermark embedding strength (represents energy of embedded watermark) of the watermark in a block depends on the class to which the block belongs. Results were pleasant, although it was suggested that incorporation of other human visual system (HVS) factors, such as contrast masking can improve the results.

Mohanty et al. [151] proposed a visible watermarking algorithm in the DCT domain, in which scaling factor and embedding factor were found using a mathematical model developed by exploiting the texture sensitivity of the human visual system (HVS) to ensure that the perceptual quality of the image is better preserved. It extended the work of Kankanhalli et al. [96].

Bing et al. [80] proposed a visible watermarking technique where, energy of the embedded watermark in different regions of the image was varied depending on the underlying content of the image and human's sensitivity to spatial frequencies. This was achieved by analyzing the image content, such as textures, edges, smooth areas, and wavelet coefficients contrast-sensitive function (CSF) of perceptual importance weight. These measures were used for varying the strength of the watermark to ensure the perceptual uniformity of the embedded watermark over different regions of the image. This strength can be varied to automate the process over a wide range of images.

Hu et al. [77] proposed a reversible visible watermarking algorithm. In this, the visible watermark can be completely removed from the watermarked image to recover the original image. It includes two procedures: data hiding and visible watermark embedding. The data hiding technique reversibly hides the payload in the image region not covered by the visible watermark. To satisfy the requirements of large capacity and high image quality, the hiding technique was based on data compression and used a payload-adaptive scheme. Error diffusion was adopted for improving the subjective image quality and arithmetic compression using a character-based model was used for increasing the computational efficiency. The visible watermark was securely embedded based on a user-key-controlled embedding mechanism. The data hiding and the visible watermark embedding procedures were integrated into a secure watermarking system by a specially designed user key.

Tsai et al. [219] proposed a reversible visible watermarking algorithm. Pixel values of original image beneath the watermark were mapped to a small range $[\alpha, \alpha+127]$ to generate a visible watermarked image. Since the mapping was many-to-one, taking inverse mapping can only approximate the original image. To restore the original image, the difference image obtained by subtracting the approximated image from the original image and other side information were loss-lessly compressed and embedded in the visible watermarked image using a reversible data embedding algorithm. This is a key-based scheme, where key is a random variable with discrete normal distribution. Key is required to restore the original image. Transparent degree of watermark was controlled by variance of the key.

Liu et al. [132] proposed a method for visible watermarking with a capability of lossless image recovery. Different types of visible watermarks were embedded, such as opaque monochrome image and translucent full color image etc. A two-fold monotonically increasing compound mapping was used to yield more distinctive visible watermarks in the watermarked image. Security protection measures were used to deter attackers from illicit image recoveries.

Yang et al. [238] proposed a removable visible watermarking algorithm by combining block truncation coding (BTC) and chaotic map. BTC codes of watermark were embedded in the BTC codes of image. Watermarked region was found in the original image and visible watermark was adaptively embedded using two quantization levels of the BTC compressed image. Further, original bi-level watermark was encrypted and then loss-lessly and invisibly embedded to prevent illegal watermark removal. The relationship of two quantization levels of BTC codes is required to exactly extract original bi-level watermark and reconstruct the original image by removing visible watermark. This relationship ensured authorized removal of watermark and authorized reconstruction of watermark. This watermarking algorithm is applicable for copyright notification and secure access control in mobile communication.

Lumini et al. [134] proposed an algorithm for finding suitable watermarking positions. Local variance of the images was used to define suitable watermarking positions. Visible watermarks were placed on the suitably found positions. It was suggested that the watermark should be inserted in the watermarking positions using a human visual system based watermarking technique. Human visual system in watermarking technique helps to control the opacity of watermark depending on sensitivity of the watermarking positions.

5.1.2 Problem

In all these visible watermarking techniques (except [134]), watermark is embedded at predefined portions in images/video-frames. Many times, visible watermark occludes the significant portions in images/video-frames (for example, television broadcasting). In this chapter, we address the problem of occlusion of significant portions of images in visible watermarking. We define the problem as follows- visually embed a watermark in a given image (monochrome or color) at N positions such that important/significant portions of the image are not occluded, where, $N \geq 1$. As depicted in [83, 67, 73] saliency of portions in an image, computed using existing algorithms, would represent importance of the portions. As mentioned in [25], human eye fixation density map of an image available as meta-data could also be used to represent importance of image portions. We consider both saliency and eye fixation density based representation in this chapter. For an image, if the eye fixation density meta-data is available, it should be used, otherwise saliency computation should be involved.

In visible watermarking, clear visibility of watermark and 'good' visual quality of the watermarked image (high similarity of watermarked image with original image) are main requirements. However, both these requirements are contradictory to each other. In other words, as the visibility of watermark increases the visual quality of the watermarked image decreases. This trade-off makes visible watermarking a challenging and interesting problem.

Based on those discussed in [80, 144, 151, 244], let us discuss the general rules for 'good' visible watermark embedding with respect to our implementation. If a sub-image (a region in a given image corresponding to a given position in the image) is least significant/important, then watermark is embedded using full energy to make the watermark most visible. Here, visual quality of watermarked sub-image will be least and visibility of watermark will be maximum. If a sub-image is the most important, then the watermark should be embedded in such a that it is just visible. Here, visual quality of watermarked sub-image will be maximum and visibility of embedded watermark will be minimum.

Significance of sub-images can be at any level between maximum and minimum. Therefore, visibility of watermark and visual quality of watermarked sub-images should be controlled by the significance level of the sub-images such that visual quality of the watermarked sub-images increase with the sub-image's significance level.

We divided underlying problem into three main issues- $\mathcal{I}1$: in which sub-images of a given image, watermark should be embedded? $\mathcal{I}2$: what should be embedding energy in selected sub-images for visible watermark embedding? $\mathcal{I}3$: what watermark embedding strategy should be employed for selected sub-images?

5.1.3 Overview of Solution

The solution for $\mathcal{I}1$ is obviously that watermark should be embedded in N least important sub-images. The solution of $\mathcal{I}2$ directly depends on the significance level of selected sub-images and required visual quality of corresponding watermarked sub-images. For this, we proposed a mathematical model in terms of significance level of sub-images and visual quality of their respective watermarked sub-images. The embedding energy corresponds to the optimal solution of the proposed mathematical model.

Qi et al. [173] used the concept of just noticeable distortion (JND) to propose an adaptive invisible digital image watermarking algorithm. The JND for an image is defined as the minimum level of distortion for the image such that it is just visible by human perception. Qi et al. [173] computed the just noticeable distortion (JND) spatial masking by using brightness, edges, and region activities of a given original image. JND masking filtered the embedding energy based on image content. It was proven that the use of JND masking improved the quality of watermarked image for same watermark embedding energy. Therefore, we utilized JND masking in the proposed visible watermark embedding strategy (issue $\mathcal{I}3$, as discussed in section 5.2.3). The proposed watermark embedding strategy is a spatial domain based one.

After obtaining the solution of the issues $\mathcal{I}1$, $\mathcal{I}2$ and $\mathcal{I}3$, we plugged them judicially to arrive at final solution of the underlying visible watermarking problem.

5.1.4 Contributions

The main contributions in this chapter are as follows:

1. The best watermarking positions are found in the image using visual saliency or available human eye fixation density.

2. A mathematical model is proposed to find optimal watermark embedding strength.

3. A visible watermark embedding strategy is proposed to embed a watermark in a given sub-image.

4. A fully automated visible watermarking algorithm according to the general rules of a good visible watermarking is proposed which utilize the advantages of first three contributions.

5.2 Solutions of Three Main Issues

This section discusses the solutions of the three main issues $\mathcal{I}1$, $\mathcal{I}2$ and $\mathcal{I}3$. The solution of the issues $\mathcal{I}1$, $\mathcal{I}2$ and $\mathcal{I}3$ will be used in the proposed visible watermarking algorithm.

5.2.1 Overview of Solution of Issue $\mathcal{I}1$

Issue $\mathcal{I}1$ is to find appropriate sub-images for watermarking. We have embedded watermark in N least important sub-images. Significance level of a sub-image in an image is defined as the ratio of importance (saliency or fixation density map) of underlying sub-image (computed as the sum of absolute coefficients value in the corresponding saliency/human eye fixation density sub-map) to the importance of the most important sub-image in the image. According to this, the significance level of the most important sub-image is one and the significance level of the least important sub-image depends on its importance. Importance is calculated using eye fixation density maps, if it is available as given in [25]. If eye fixation density map is not available, then saliency computation algorithm of [83] is considered to compute saliency at every pixel. The saliency value is taken as the importance. The range of the importance is [0,1].

5.2.2 Overview of Solution of Issue $\mathcal{I}2$

Issue $\mathcal{I}2$ is to develop a mathematical model for automatic computation of embedding energy. For volume applications (where many images/frames need to be watermarked, for example watermarking of broadcasted frame, digital library of photographs etc.), embedding energy determination should be automated. This automation is based on a trade-off between visibility of watermark and similarity of watermarked image. For automation, we need a quantitative measure (say f) to assess visual quality of

watermarked sub-images and similarity of watermarked sub-images. We have defined a trade-off function in terms of f, significance level of corresponding sub-image, and maximum and minimum visual quality of watermarked sub-images. The defined trade-off function is as follows

$$(f - f_{\min})^w (f_{\max} - f)^{1-w}, \tag{5.1}$$

where, $f > 0$ (without loss of generality, f can be any measure for image quality assessment) measures visual quality of a watermarked sub-image, $0 \leq w \leq 1$ measures significance level of corresponding sub-image, and $f_{\min}$ and $f_{\max}$ correspond visual quality of watermarked sub-images, when watermark is embedded using maximal embedding energy and just noticeable distortion embedding energy respectively. Since, degradation in the watermarked sub-image is introduced due to embedded watermark only, therefore, the term $f - f_{\min}$ in (5.1) measures the visual quality of the watermarked sub-image and the term $f_{\max} - f$ in (5.1) measures the visibility of the embedded watermark. Maximization of the trade-off function gives maximal of combined visual quality of the watermarked sub-image and visibility of the embedded watermark. The proposed trade-off function is maximized at f equals to f_{opt} given as

$$f_{\text{opt}} = f_{\min} + w(f_{\max} - f_{\min}), \tag{5.2}$$

provided f is continuous and differentiable. The optimal embedding energy (watermark embedding strength) corresponds to f_{opt}.

Finding a 'good' quantitative measure f for image visual quality assessment is challenging [29]. Wang et al. [230] discussed and compared several image quality assessment (IQA) measures such as peak-signal-to -noise-ratio (PSNR), structural-similarity-index (SSIM), multi-scale-SSIM (MS-SSIM), visual-signal-to-noise-ratio (VSNR), visual-information-fidelity (VIF), PSNR-HVS-M, most-apparent-distortion (MAD), distortion-weighted-PSNR

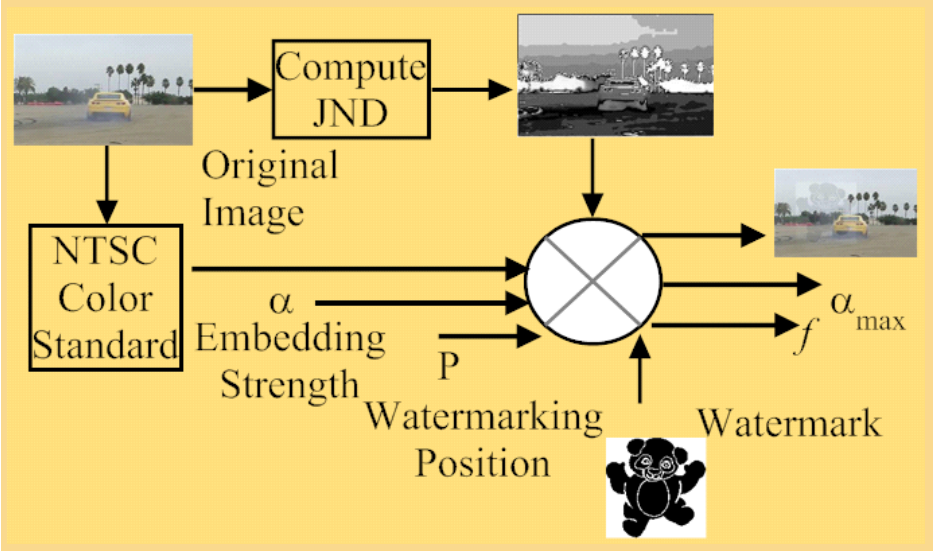


Figure 5.1: Block diagram of watermark embedding strategy for a sub-image.

(DW-PSNR), contrast-weighted-PSNR (CTW-PSNR), saliency-weighted-PSNR (SW-PSNR), information-content-weighted-PSNR (IW-PSNR), DW-SSIM, CTW-SSIM, SW-SSIM, IW-SSIM and concluded that IW-SSIM appears to be the best measure for image quality assessment. Therefore, in this chapter, we have used IW-SSIM to measure the visual quality of watermarked sub-images and obtained satisfactorily results for the underlying problem.

5.2.3 Overview of Solution of Issue $\mathcal{I}3$

Issue $\mathcal{I}3$ is to develop a visible watermark embedding strategy. We used just noticeable distortion (JND) [34, 173] map to filter the watermark embedding energy based on content in sub-images.

The input to proposed embedding strategy are original image I (color or monochrome), watermark W, position P of a sub-image, where, watermark is to be embedded (watermarking position), and watermark embedding strength α, which is representative of embedding energy.

The quality of the watermarked image decreases with increase in watermark embedding strength α. As discussed in section 5.1, the 'good' quality of watermarked images is a main requirement. Therefore, maximum limit on the embedding strength is required such that the quality of watermarked images do not fall below minimum acceptable quality. Finding an optimal algorithm that sets a limit on the maximum embedding energy is a problem. In this chapter, an arbitrary used algorithm that sets maximum limit on the embedding energy is discussed in step 6 of the strategy. This algorithm provides maximum possible distortion in each pixel of the sub-image. This maximum possible distortion in each pixel and JND are plugged in step 9 to produce continuous and differentiable f.

This embedding strategy outputs watermarked sub-image H_P that corresponds to position P, watermarked sub-image quality measure f, and watermark embedding strength $\alpha_{\max}$ corresponding to minimal watermarked sub-image quality measure $f_{\min}$. We express the embedding strategy as follows

$$[H_P, f, \alpha_{\max}] = A1(I, W, P, \alpha), \tag{5.3}$$

where, $A1(.)$ is the proposed embedding strategy for visible watermarking of a sub-image of an image. Fig. 5.1 gives block diagram of the watermark embedding strategy $A1(.)$. The step wise details of the watermark embedding strategy $A1(.)$ are as follows.

1. Compute just noticeable distortion (JND) map J_{map} of I.

2. Find the sub-image H of I of size equal to size of W that corresponds to the input position P.

3. Find the sub-map J of J_{map} equal to size of W that corresponds to input position P.

4. Convert the sub-image H into the national television system committee (NTSC) standard YIQ color space.

5. Take luminance part H_L of the sub-image H.

6. Fix a watermark embedding algorithm (A2) that corresponds to maximum embedding energy of watermark. In this chapter, we have used a spatial domain based pixel-wise embedding algorithm, which is stated as follows: *if watermark bit is zero, then set least b significant bits of the corresponding pixel in the luminance part H_L of the sub-image H to zero, else set least b significant bits to one.* The default value of b is set to 5.

7. Embed watermark W in the luminance sub-image H_L using watermark embedding algorithm (A2) to obtain the watermarked image H_1.

8. Obtain the difference image $D = \text{abs}(H_L - H_1)$.

9. Obtain the image of modulated coefficients as

$$MC = \min(D, \alpha J).$$

This step controls maximum possible distortion in each pixel of the sub-image.

10. Obtain the watermarked luminance sub-image H_{LP} by using the following formula

$$H_{LP}(x,y) = \begin{cases} H_L(x,y) - MC(x,y) & \text{if} \\ \quad W(x,y) = 0 & \\ H_L(x,y) + MC(x,y) & \text{if} \\ \quad W(x,y) = 1 & \end{cases} \tag{5.4}$$

where, $x = 1, 2, \cdots \text{height}$ of W, $y = 1, 2, \cdots \text{width}$ of W.

11. If input image is monochrome image, then $H_P = H_{LP}$ is the required watermarked image and then goto step 13. Else if input image is a color image then goto step 12.

12. Use watermarked luminance sub-image H_{LP}, and chrominance components of the H to obtain the watermarked image H_P in original color space.

13. Compute the visual quality $f = \text{IW-SSIM}(H, H_P)$ of the watermarked sub-image.

14. Compute $\alpha_{\max} = \dfrac{\max(D)}{\min(J)}$.

Output: Watermarked sub-image H_P, quantitative value f, which is IW-SSIM of the watermarked sub-image H_P and maximum embedding strength $\alpha_{\max}$. The value of f depends on α and it is observed that, f is continuous and differentiable with respect to α in the interval $[0, \alpha_{\max}]$.

Note:

1. The optimum value of f (f_{opt}) is given by the following equation

$$f_{\text{opt}} = f(\alpha_{\text{opt}}) = f_{\min} + w(f_{\max} - f_{\min}), \tag{5.5}$$

   where, α_{opt} is named as optimal watermark embedding strength.

2. In step 6, we can replace the algorithm A2 with other algorithm, which provide a better limit on the maximum embedding energy.

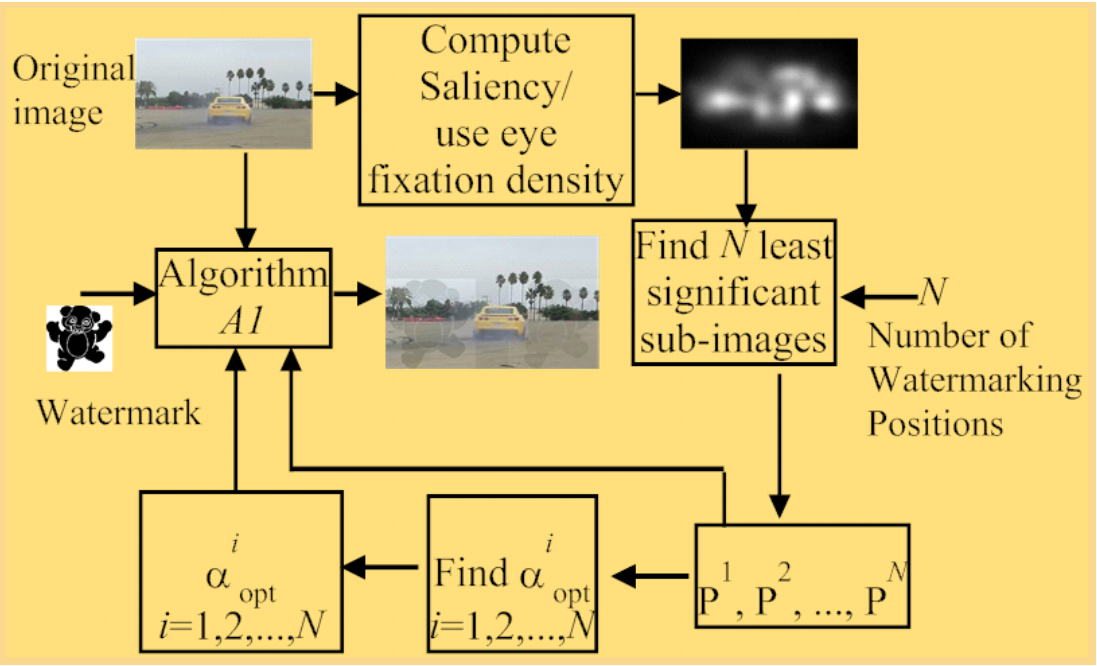


Figure 5.2: Block diagram for watermarking of an image using a watermark at N non-overlapping positions. In this diagram, $N = 2$.

5.3 Visible Watermarking of an Image Using a Watermark at N Positions

This section discusses the proposed algorithm to solve the visible watermarking problem. Importance of image portions, f_{opt} which corresponds to (5.5) and watermarking algorithm $A1$ are combined to derive the proposed 'good' visible watermarking algorithm. The input to algorithm are original image I, watermark W, and number of watermarking positions N. This algorithm outputs watermarked image I_w. We express the watermark embedding algorithm as follows

$$I_w = A(I, W, N), \tag{5.6}$$

where, $A(.)$ is the proposed visible watermarking algorithm for an image. Fig. 5.2 gives the block diagram of the proposed visible watermarking algorithm $A(.)$. This

is a fully automated algorithm in the sense that optimal embedding strength and optimal position for embedding are automatically determined. The step wise details of the algorithm $A(.)$ are as follows.

1. Compute visual saliency map or use the human eye fixation density map. Let the map be S_{map}.

2. Find the most important sub-image in I of size equal to size of W. Store its position as P and its importance as s.

3. Find N least important sub-images in I each of which size is equal to size of W. Store the position of these sub-images as $\text{P}^1, \text{P}^2, \cdots \text{P}^N$ and importance as $s^1, s^2, \cdots s^N$.

4. Compute significance level of N least important sub-images as follows

$$w^i = \frac{s^i}{s}, i = 1, 2, \cdots N, s \neq 0.$$

5. Compute $\alpha^i_{\text{max}}, i = 1, 2, \cdots N$ and maximum visual quality $f^i_{\text{max}}, i = 1, 2, \cdots N$ for N least important sub-images by using the embedding strategy $A1$ as follows:

$$[f^i_{\text{max}}, \alpha^i_{\text{max}}] = A1(I, W, \text{P}^i, \alpha = 1), i = 1, 2, \cdots N.$$

6. Find minimum visual quality of each N least important sub-images using the embedding strategy $A1$ as follows:

$$f^i_{\text{min}} = A1(I, W, \text{P}^i, \alpha = \alpha^i_{\text{max}}),$$

$i = 1, 2, \cdots N$.

7. Compute

$$f^i_{\text{opt}} = f^i_{\text{min}} + w^i(f^i_{\text{max}} - f^i_{\text{min}}), i = 1, 2, \cdots N. \tag{5.7}$$

8. Solve the following equations

$$f(I, W, \mathrm{P}^i, \alpha^i_{\mathrm{opt}}) = f^i_{\mathrm{opt}}, i = 1, 2, \cdots N \tag{5.8}$$

for finding the optimal embedding strengths (α^i_{opt}s) for each N least important sub-images. $f(I, W, \mathrm{P}^i, \alpha^i_{\mathrm{opt}})$ forms the function of $(I, W, \mathrm{P}^i, \alpha^i_{\mathrm{opt}})$, which is the visual quality of the watermarked sub-image obtained from embedding strategy $A1$ when input of $A1$ is $I, W, \mathrm{P}^i, \alpha^i_{\mathrm{opt}}$.

9. Obtain the watermarked sub-images as follows:

$$I_w(\mathrm{P}^i) = A1(I, W, \mathrm{P}^i, \alpha = \alpha^i_{\mathrm{opt}}), i = 1, 2, \cdots N.$$

10. Replace N least important sub-images in the original image I with the corresponding watermarked sub-images $I_w(\mathrm{P}^i), i = 1, 2, \cdots N$ to obtain the watermarked image I_w.

Output: Watermarked image I_w.

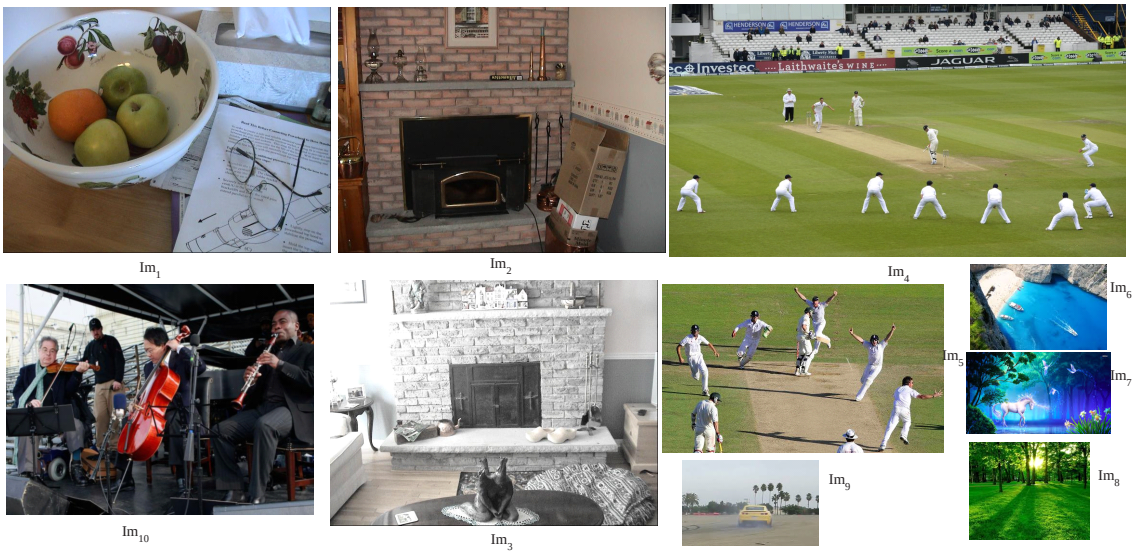


Figure 5.3: Sample original images. Size of Im_1, Im_2 and $Im_3 = 511 \times 681$ pixels, $Im_4 = 526 \times 950$ pixels, $Im_5 = 350 \times 585$ pixels, $Im_6 = 177 \times 284$ pixels, $Im_7 = 168 \times 300$ pixels, $Im_8 = 201 \times 251$ pixels, $Im_9 = 177 \times 284$ pixels, $Im_{10} = 480 \times 640$ pixels.

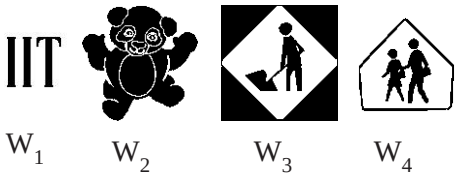


Figure 5.4: Sample binary watermarks. Size of $W_1 = 64 \times 64$ pixels, W_2 and $W_3 = 120 \times 120$ pixels, Size of $W_4 = 100 \times 100$ pixels.

5.4 Experiments, Results and Discussion

MATLAB platform is used to perform all the experiments. The host images are taken from the data set [25] and [120] and randomly collected from the internet. All the used images are color images. Fig. 5.3 shows few sample original images. Several binary watermarks of different dimensions are used as shown in Fig. 5.4. We have done five experiments for detailed evaluation, analysis and comparison of the proposed visible watermarking algorithm. Note that in our implementation, *fminbnd* function of MATLAB has been used to solve the equations (5.8).

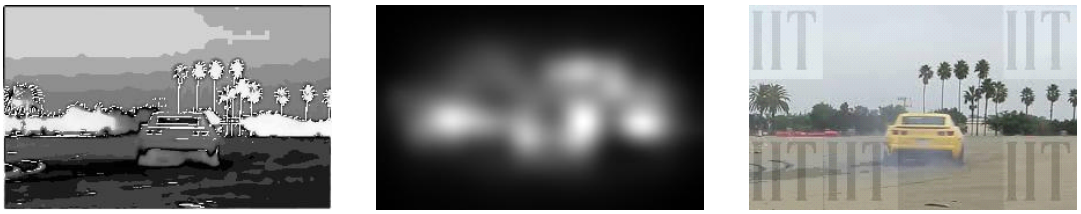
The first experiment (Experiment 1) compares the results of the proposed watermarking algorithm with discussed general rules (see section 5.1) of watermarking and verifies the accuracy of the proposed algorithm with respect to proposed theory and philosophy. Qualitative & quantitative assessments and user study responses are used for the evaluation and analysis of the proposed watermarking algorithm.

The second experiment (Experiment 2) comprises results of the proposed watermarking algorithm with respect to three different methods of finding image areas for embedding the watermark (watermarking area/position). In this experiment, we have used eye tracking density map, visual saliency map and variance map [134] for finding watermarking area. We have used qualitative assessment of the users response for evaluation and analysis.

The third experiment (Experiment 3) studies the effects of miscellaneous parameters such as size of watermark and significance level of watermarking area on watermarked images. We have used qualitative assessment for the analysis.

The fourth experiment (Experiment 4) compares the proposed watermark embedding strategy with state of the art visible watermark embedding strategy [132]. We have used qualitative & quantitative assessments and user study responses for the evaluation and analysis.

The last experiment (Experiment 5) compares the proposed watermark embedding strategy and state of the art visible watermark embedding strategy [132] under various attack scenarios such as cropping, Gaussian noise, Gaussian filter, histogram equalization, JPEG compression, scaling, rotation, and salt & pepper noise.



(a) (b) (c)

Figure 5.5: Watermarking results corresponding to original image Im_9 and watermark W_1. (a) Just noticeable distortion map (b) Saliency map (c) Watermarked image.

5.4.1 Experiment 1

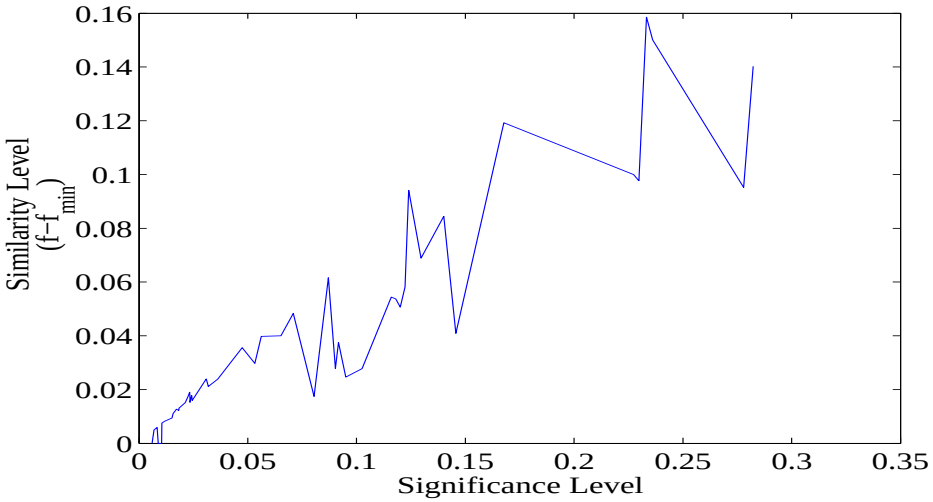
As explained earlier, the main goals of this experiment are:

1. to compare the results of the proposed watermarking algorithm with discussed general rules of watermarking;

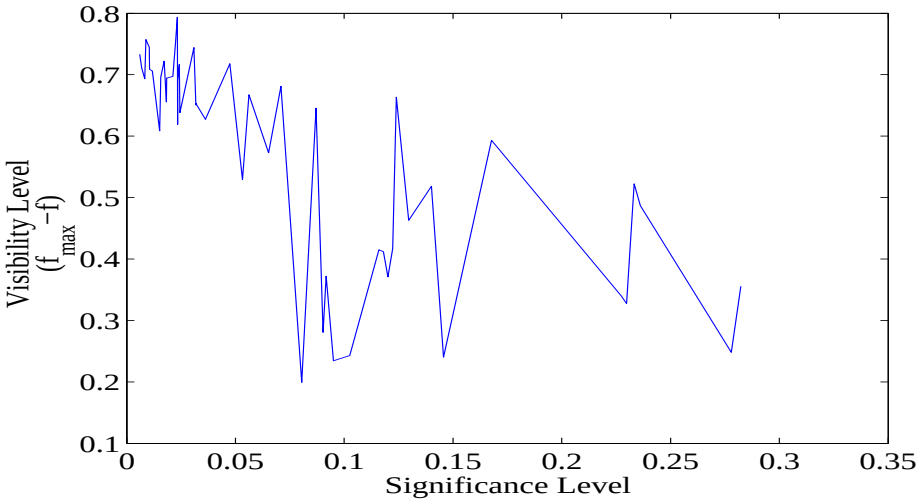
2. to verify the accuracy of the proposed algorithm with respect to proposed theory and philosophy.

To address the first goal, we have quantitatively assessed the quality of watermarked images and visibility of watermark, quantitatively assessed the visual quality of the watermarked images and visibility of watermark with respect to significance level of corresponding images, and provide the statistics of user response about quality of watermarked images and visibility of watermark with respect to the significance level.

Fig. 5.5 shows detailed results of the proposed watermarking algorithm. In Fig. 5.5, results are corresponding to the original image Im_9 (Fig. 5.3), watermark W_1 (Fig. 5.4) and N (number of watermarking positions) = 5. Visual saliency map is used for finding watermarking positions. Fig. 5.5 (a) shows JND map and Fig. 5.5 (b) shows saliency map of the original image Im_9. Fig. 5.5 (c) is the watermarked image. We observe that loss of information in watermarked image Fig. 5.5 (c) is negligible and watermarks are visible.



(a)



(b)

Figure 5.6: Quantitative results corresponding to several watermarked image. Significance level is computed using visual saliency. (a) Similarity level ($f - f_{\min}$, f = IW-SSIM) of watermarked sub-images with respect to significance level of corresponding sub-images (b) visibility level ($f_{\max} - f$) of watermarks with respect to significance level of corresponding sub-images

We have implemented the proposed watermarking algorithm on several original images and watermarks, and have computed significance level of watermarking positions, similarity of watermarked sub-images with original sub-images and visibility of watermark in watermarked sub-images. Fig. 5.6 (a) gives relation of similarity of watermarked sub-images ($f - f_{\min}$) with significance level of watermarking positions, and Fig. 5.6 (b) gives relation of visibility of watermark ($f_{\max} - f$) with significance level of watermarking positions. From Fig. 5.6, we observe that

- Similarity of watermarked sub-images with corresponding original sub-images is more for higher significance level of the corresponding watermarking area.
- Visibility of watermark decreases with respect to significance level of watermarking area.

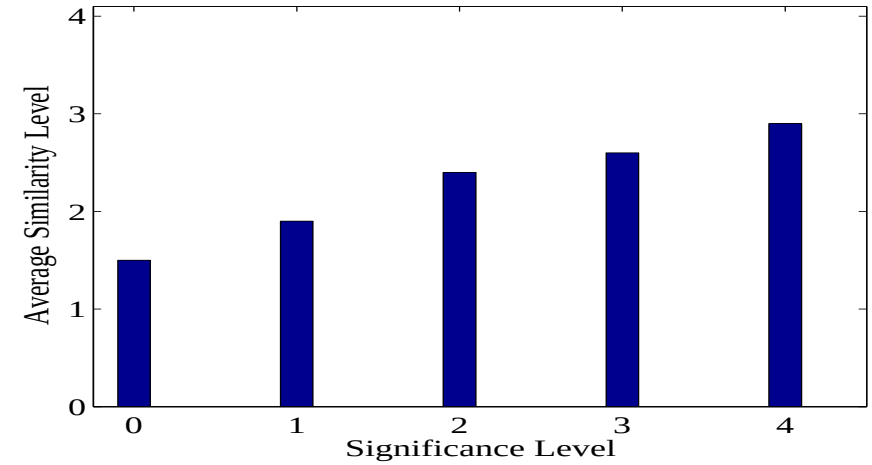
We have done a user study to evaluate the users response about quality of watermarked sub-images and visibility of watermark with respect to the significance level. In the user study, we have displayed an original image, a watermark and the corresponding watermarked image to a user and asked the following questions:

Q1. Rate the significance level of watermarking area.

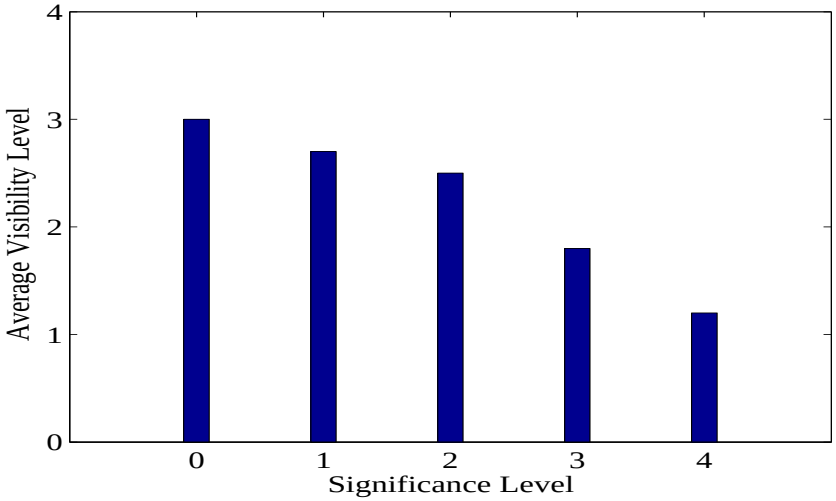
Q2. Rate the similarity of watermarked image with corresponding original image.

Q3. Rate the visibility of watermark.

The rating is done at five levels-0,1,2,3, and 4. Zero (0) corresponds minimum rating and four (4) corresponds maximum rating. Fig. 5.7 gives the user-study response. Fig. 5.7 (a) gives relation of similarity level of watermarked sub-images with significance level of watermarking areas and Fig. 5.7 (b) gives relation of visibility of watermark in watermarked images with significance level of watermarking areas. From Fig. 5.7 also, we observe that



(a)



(b)

Figure 5.7: Watermarking results based on user-study on several watermarked images. (a) User-study response based average similarity level of watermarked sub-images with respect to user-study response based significance level of corresponding sub-images (b) user-study response based average visibility level of watermarks with respect to user-study response based significance level of corresponding sub-images

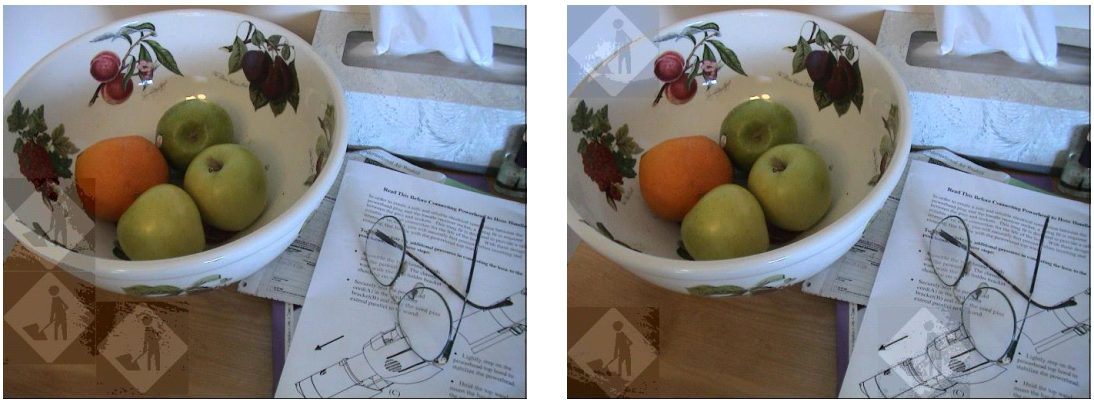
Table 5.1: Detail of results corresponding to Fig. 5.5. $f = \text{IW-SSIM}$

i	Position (P^i)	Significance level (w^i)	$f^i_{\min}$	$f^i_{\max}$	f^i_{opt}	α^i_{opt}	$f(\alpha^i_{\text{opt}})$	$f(\alpha^i_{\text{opt}})-f_{\min}$	$f_{\max}-f(\alpha^i_{\text{opt}})$
1	[1 1]	0.0710	0.0932	0.8227	0.1449	3.5593	0.1415	0.0483	0.6182
2	[1 221]	0.0870	0.1252	0.8326	0.1868	2.7066	0.1868	0.0616	0.6458
3	[114 1]	0.1180	0.5136	0.9790	0.5685	4.3082	0.5673	0.0537	0.4117
4	[114 221]	0.1240	0.0859	0.8435	0.1798	2.8242	0.1800	0.0941	0.6635
5	[114 66]	0.2361	0.3282	0.9652	0.4785	3.2872	0.4782	0.1500	0.4870

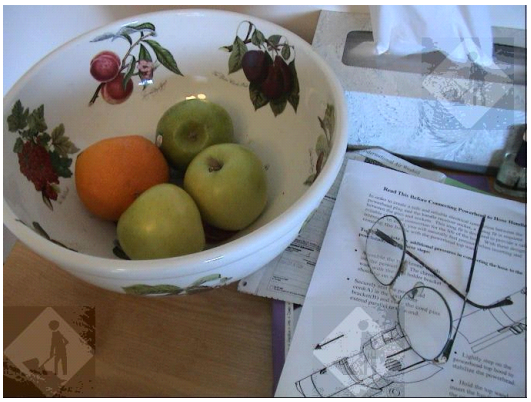
- Similarity of watermarked sub-images with corresponding original sub-images is more for higher significance level of corresponding watermarking area.
- Visibility of watermark decreases with respect to importance of watermarking area.

From Figs. 5.6 and 5.7, we observe that the quantitative measure and user study response follow same trend for the proposed watermarking algorithm. Moreover, evidences from Figs. 5.6 and 5.7 ensure that working of the proposed watermarking algorithm follow the general rules of visible watermarking.

To address the second goal, we have discussed the results correspond to Fig. 5.5 in detail. Table 5.1 gives detailed quantitative results of the proposed algorithm that corresponds to original image Im_9 (Fig. 5.3), watermark W_1 (Fig. 5.4) and N (number of watermarking positions) = 5. In Table 5.1, P^i gives top-left position of watermarking area, w^i gives significance level of watermarking area, $f^i_{\min}$ gives minimum IW-SSIM for watermarked sub-image (obtained from step 6 in section 5.3), $f^i_{\max}$ gives maximum IW-SSIM for watermarked sub-image (obtained from step 5 in section 5.3), f^i_{opt} gives optimal IW-SSIM for watermarked sub-image (obtained from step 7 in section 5.3, α^i_{opt} is optimal embedding strength and solution of (5.8) at modeled optimal IW-SSIM (f^i_{opt}), and $f(\alpha^i_{\mathrm{opt}})$ is the actual IW-SSIM of the watermarked sub-image at computed optimal embedding strength α^i_{opt}. $f(\alpha^i_{\mathrm{opt}}) - f_{\min}$ measures actual similarity of watermarked sub-images with original sub-images and $f_{\max} - f(\alpha^i_{\mathrm{opt}})$ measures actual visibility of watermark in watermarked sub-images. We have found that the difference between f^i_{opt} and $f(\alpha^i_{opt})$ is negligible. This ensures that equations of (5.8) are successfully solved, IW-SSIM (f) is continuous and differentiable with respect to embedding strength α for the proposed watermarking algorithm, and proposed visible watermarking algorithm is consistent with proposed mathematical model (5.1) and (5.2).



(a) (b)



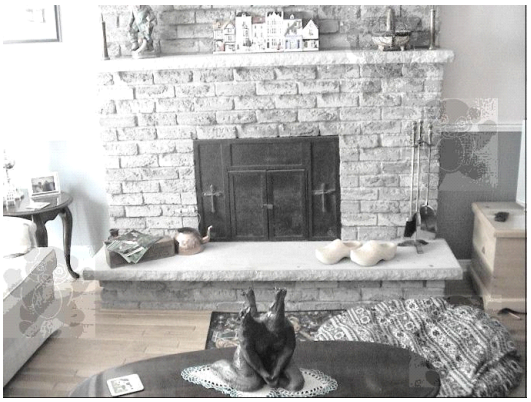
(c)

Figure 5.8: Watermarked images corresponding to the original image Im_1 (Fig. 5.3) and watermark W_3 (Fig. 5.4). Watermarking positions are found using (a): human eye fixation density map (b): visual saliency [83] (c): variance [134].

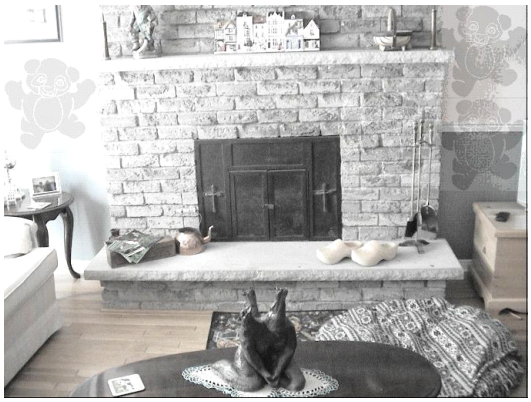
5.4.2 Experiment 2

This experiment aims to compare results of the proposed watermarking algorithm with respect to three different methods of finding watermarking area. For evaluation of the results, we have taken the responses of those users who have background on image analysis. These responses are used to compare the three methods of determining the watermarking positions.

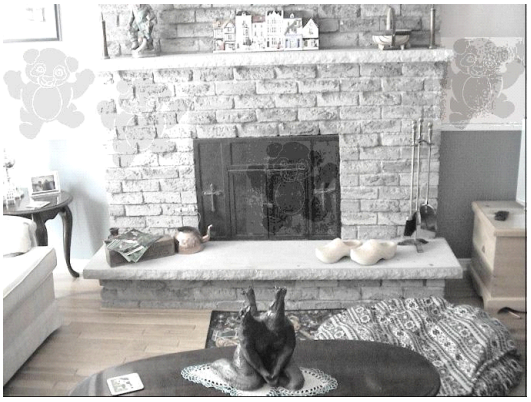
Fig. 5.8 shows watermarked images corresponding to original image Im_1, watermark W_3, and $N = 3$. Fig. 5.9 shows watermarked images corresponding to original image Im_3, watermark W_2, and $N = 4$. Fig. 5.10 shows watermarked images corresponding to original image Im_{10}, watermark W_2, and $N = 5$. Watermarking



(a)

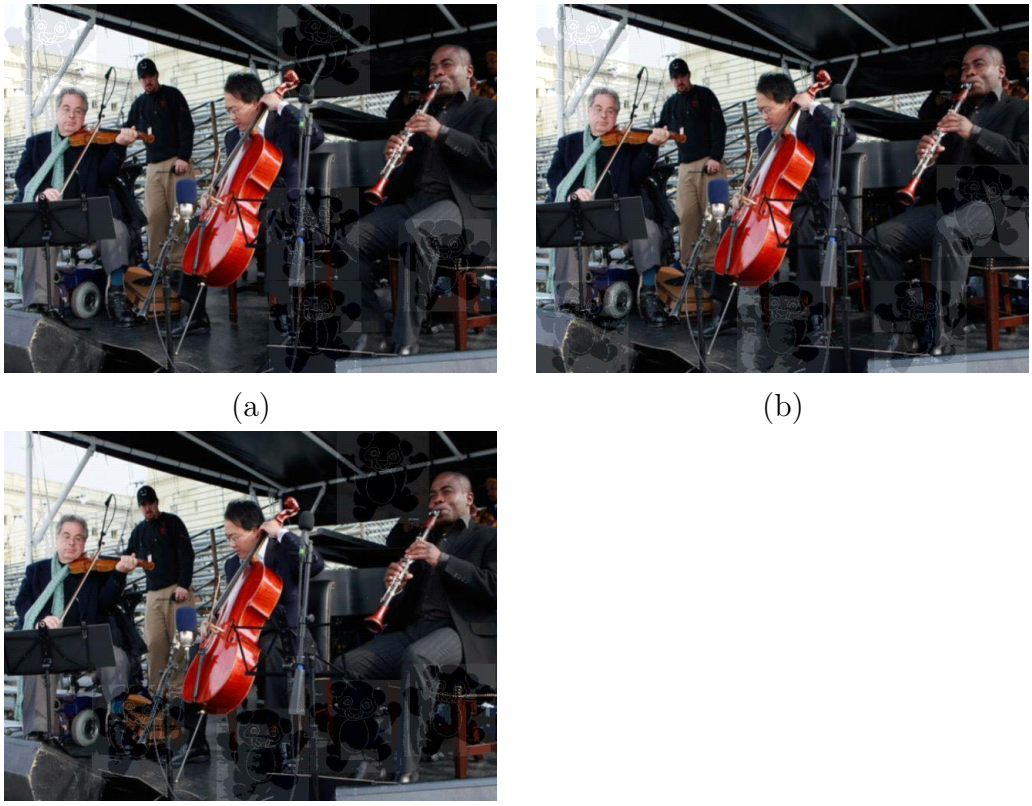


(b)



(c)

Figure 5.9: Watermarked images corresponding to original image Im_3 (Fig. 5.3) and watermark W_2 (Fig. 5.4). Watermarking positions are found using (a): human eye fixation density map (b): visual saliency [83] (c): variance [134].



(a) (b)

(c)

Figure 5.10: Watermarked images corresponding to original image Im_{10} (Fig. 5.3) and watermark W_2 (Fig. 5.4). Watermarking positions are found using (a): human eye fixation density map (b): visual saliency [83] (c): variance [134].

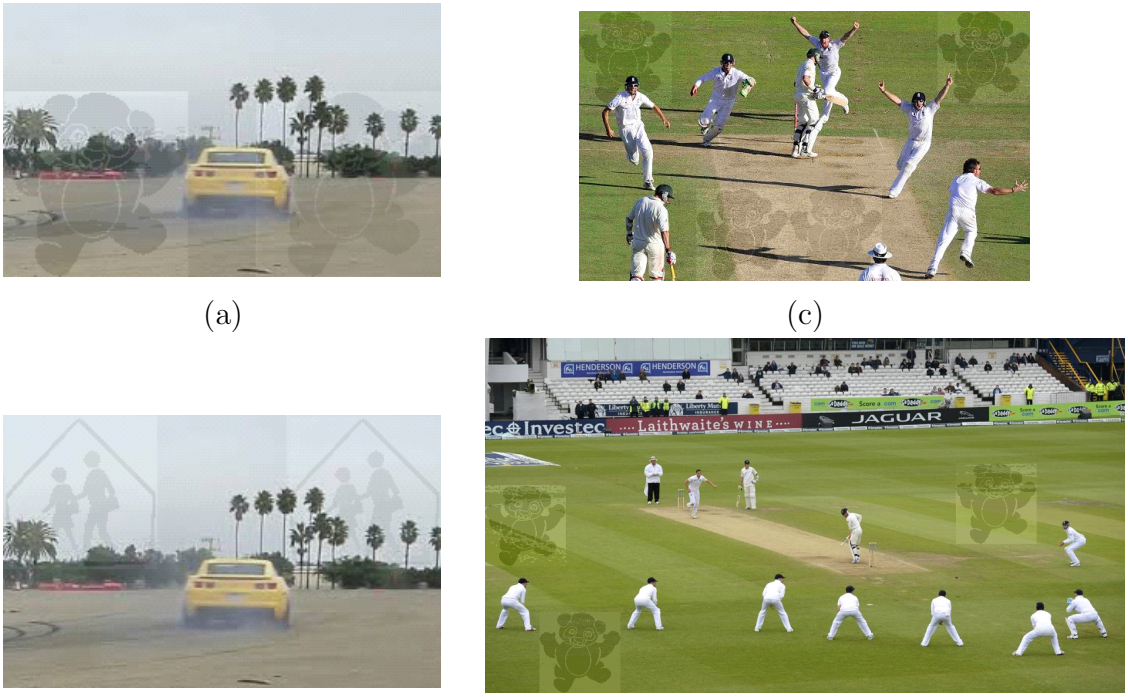
positions are found using eye tracking density map in Figs. 5.8 (a), 5.9 (a) and 5.10 (a), using visual saliency map in Figs. 5.8 (b), 5.9 (b) and 5.10 (b), and using variance map of [134] in Figs. 5.8 (c), 5.9 (c), and 5.10 (c). The highlights of the responses are as follows:

- In Fig. 5.8 (a), watermarked positions of image are not important, in Fig. 5.8 (b), two watermarked positions, first on the page and second near the spectacle are important, and in Fig. 5.8 (c), two watermarked positions, one on the page and near the spectacle and second on the brick have high importance. Thus, according to user study on Fig. 5.8, human eye fixation density map is the best and eye tracking density map and visual saliency map are better than variance map [134].

- In Fig. 5.9 (a), one watermarked position of the image on top of the blanket has slightly higher importance, in Fig. 5.9 (b), watermarked positions are not important and in Fig. 5.9 (c), watermarked position on the window has importance. Thus, according to user study on Fig. 5.9, visual saliency map is the best.

- In Fig. 5.10 (a), watermarked positions of image are not important. In Fig. 5.10 (b), one watermarked position near bottom left corner of the image is important. In Fig. 5.10 (c), brown bag (near bottom-middle) and face of a man (near top-right) are hidden. Thus, according to user study on Fig. 5.10, human eye fixation density map is the best and eye tracking density map and visual saliency map are better than variance map [134].

In summary, we conclude that watermarking position finding methods based on eye tracking density map and visual saliency map are very competitive. However, for semantic images (such as image Im_{10}), human eye fixation density map is the best. Moreover, eye tracking density map and visual saliency map are better than variance map [134] for determining watermarking positions.



(a) (c)

(b) (d)

Figure 5.11: Watermarked images to describe effects of miscellaneous watermarking parameters. Watermarking positions are found using visual saliency. (a): Watermarked image corresponding to original image Im_9 and watermark W_2 (b): Watermarked image corresponding to original image Im_9 and watermark W_4 (c): Watermarked image corresponding to original image Im_5 and watermark W_2 (d): Watermarked image corresponding to original image Im_4 and watermark W_2.

5.4.3 Experiment 3

We have done image analysis of the watermarked images that correspond to different watermark size and same original image, and different original images and same watermark. In this experiment, watermarking positions are found using visual saliency map.

Fig. 5.11 (a) shows the watermarked image that corresponds to the original image Im_9, the watermark W_2, and $N = 2$. Fig. 5.11 (b) shows the watermarked image that corresponds to the original image Im_9, the watermark W_4, and $N = 2$. From the

Figs. 5.11 (a) and (b), we observe that detected watermarking positions depend the on size of the watermarks.

Fig. 5.11 (c) represents the watermarked image that corresponds to the original image Im_5, the watermark W_2, and $N = 4$. Fig. 5.11 (d) represents the watermarked image that corresponds to the original image Im_4, the watermark W_2, and $N = 3$. From the Figs. 5.11 (c) and (d), we observe the following:

- Watermarking areas in Fig. 5.11 (c) have more importance than watermarking areas in Fig. 5.11 (d).
- Visibility of watermarks is more in Fig. 5.11 (d) than Fig. 5.11 (c).

We conclude that watermarking positions depend on size of watermarks and visibility of watermark decreases with respect to significance level of watermarking position.

5.4.4 Experiment 4

The goal of this experiment is to compare the proposed watermark embedding strategy with state of the art watermark embedding strategy of Liu et al. [132]. Similar to Experiment 1, we have done qualitative and quantitative assessments, and statistics of user response. Watermarking positions are found using visual saliency.

Fig. 5.12 shows watermarked images that correspond to the original images Im_2, Im_6 and Im_7. For Figs. 5.12 (a), (b), (d) and (e), watermark is W_2 and for Figs. 5.12 (c) and (f), watermark is W_3. For Figs. 5.12 (a) and (d), the value of N is 4 and for Figs. 5.12 (b), (c), (e) and (f), the value of N is 2. In Figs. 5.12 (a), (b) and (c), watermark embedding strategy of [132] is used and in Figs. 5.12 (d), (e) and (f) the proposed watermark embedding strategy is used to embed the watermark. From Fig. 5.12, we observe the following:

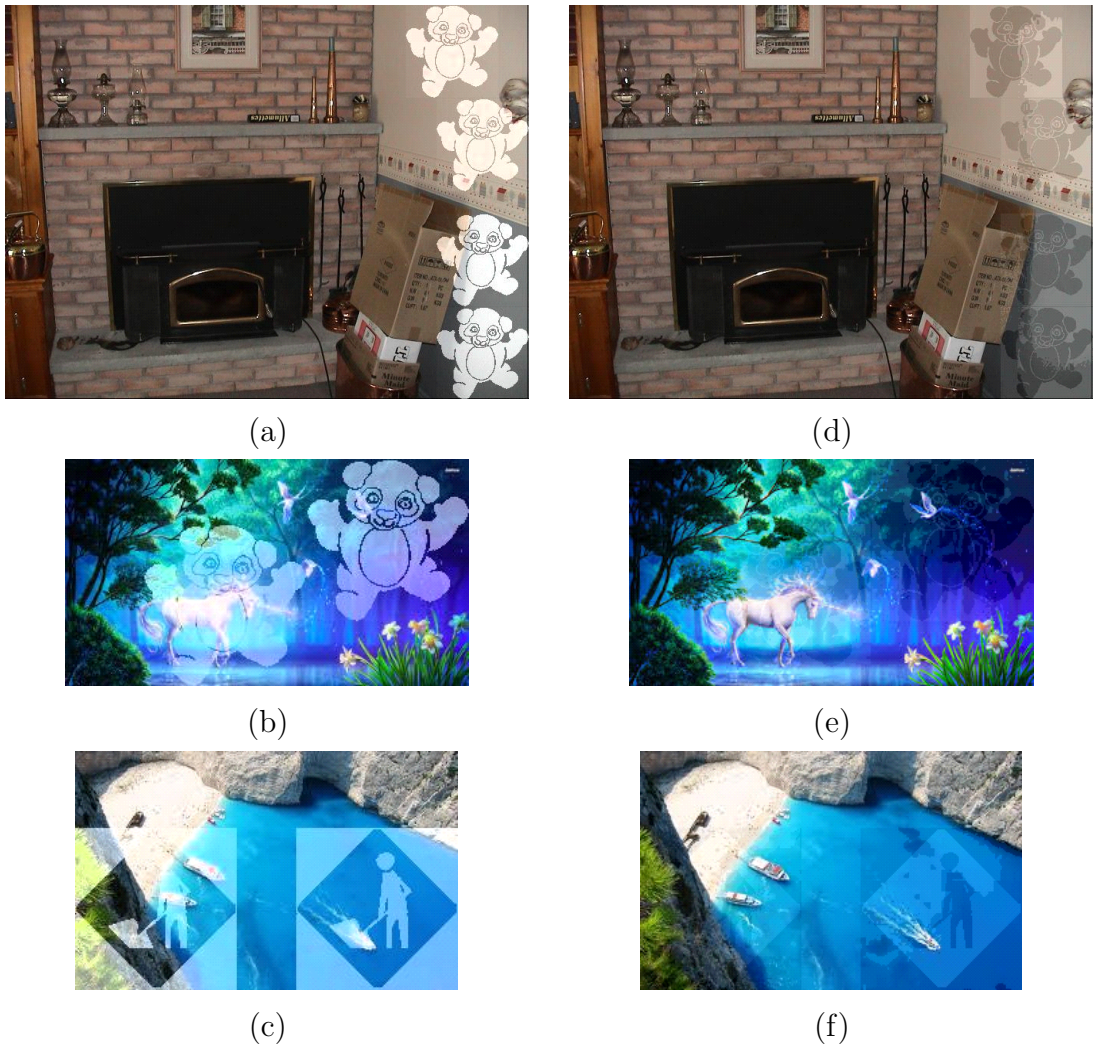


Figure 5.12: Comparison between proposed watermark embedding strategy and watermark embedding strategy of [132]. Watermarking positions are found using visual saliency. (a): original image Im_2, watermark W_2, existing watermark embedding strategy of [132] (b): original image Im_7, watermark W_2, existing watermark embedding strategy of [132] (c): original image Im_6, watermark W_3, existing watermark embedding strategy of [132] (d): original image Im_2, watermark W_2, proposed watermark embedding strategy (e): original image Im_7, watermark W_2, proposed watermark embedding strategy (f): original image Im_6, watermark W_3, proposed watermark embedding strategy.

- In Figs. 5.12 (a), (b) (c) and (d), watermark is easily visible and in Figs. 5.12 (e) and (f), watermark is visible after careful examination. Note that according to Kankanhalli et al. [96], visibility of watermark after careful examination is a general requirement of 'good' visible watermarking algorithm.

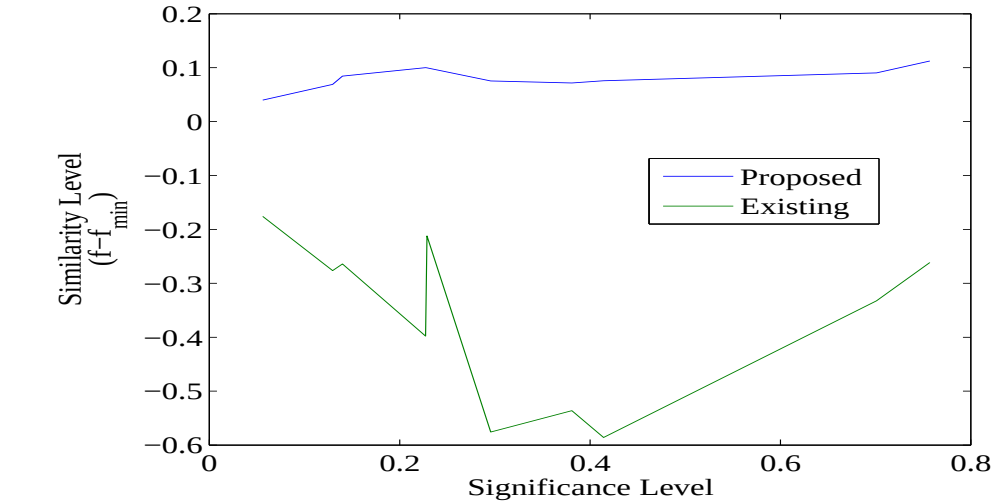
- In Figs. 5.12 (a), (b) and (c) similarity of watermarked sub-images with the corresponding original sub-images is low, while in Figs. 5.12 (d), (e) and (f), similarity of watermarked sub-images with the corresponding original sub-images is high.

Fig. 5.13 provides a quantitative comparison between proposed embedding strategy and existing watermark embedding strategy of [132]. In Fig. 5.13, relation of similarity of watermarked sub-images and visibility of watermarks with significance level of watermarking positions are compared. Data in Fig. 5.13 is corresponding to Fig. 5.12. From Fig. 5.13, we observe the following:

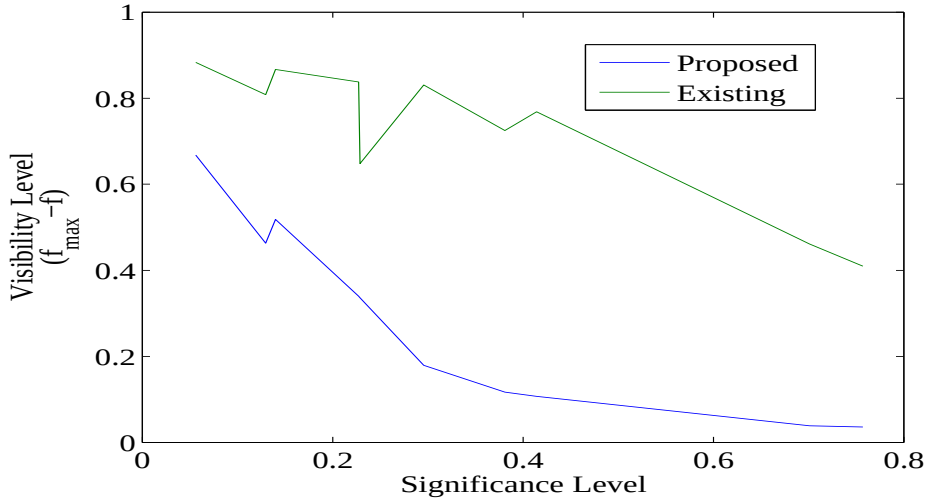
- Similarity of watermarked sub-images for the proposed watermark embedding strategy is more than zero, while, similarity of watermarked sub-images for the existing watermark embedding strategy of [132] is less than zero.

- Visibility of watermark for the existing watermark embedding strategy of [132] is more than proposed watermark embedding strategy. However, visibility of watermark for the proposed watermark embedding strategy is more than zero.

Fig. 5.14 provides a comparison between proposed embedding strategy and existing watermark embedding strategy of [132] based on user study response. In the user study, we have used images as shown in Fig. 5.12. Further, we have asked same questions as discussed in section 5.4.1. A comparison of relation between the similarity of watermarked sub-images and visibility of watermarks with significance level of watermarking positions is provided in Fig. 5.14. From Fig. 5.14, we observe the following:

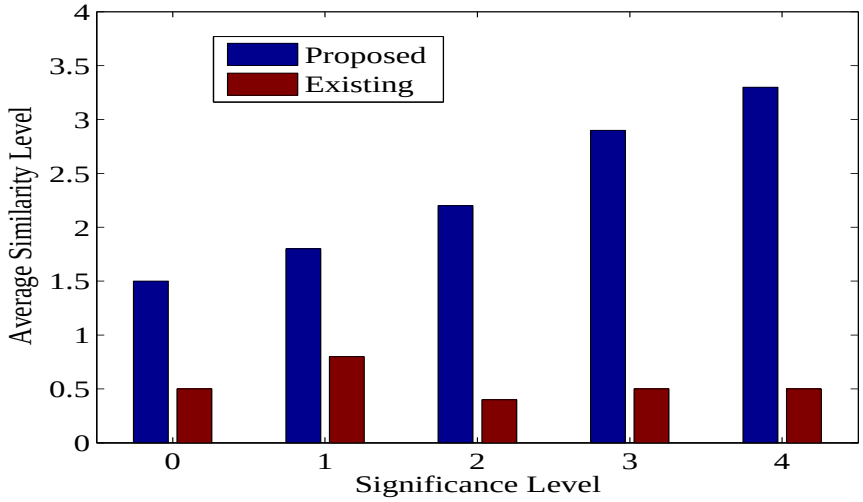


(a)

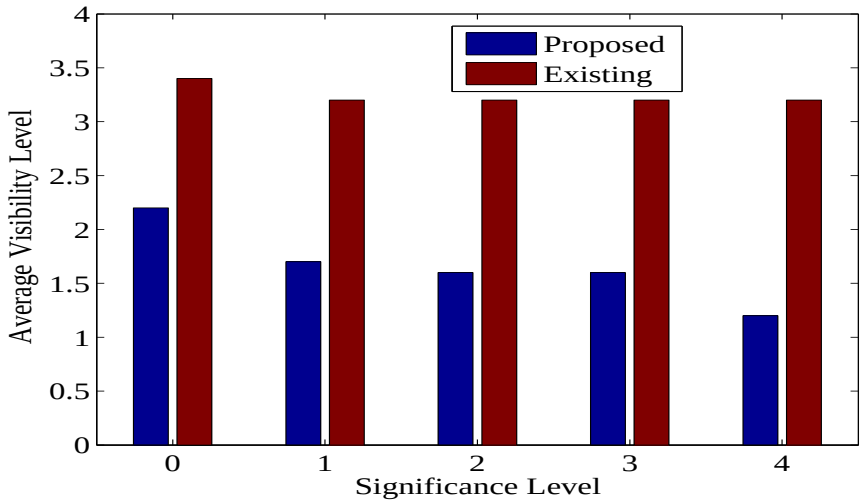


(b)

Figure 5.13: Quantitative results corresponding to Fig. 5.12 for comparison between proposed and existing [132] watermark embedding stratgies. Significance level is computed using visual saliency. (a) Similarity level ($f - f_{\min}$, f = IW-SSIM) of watermarked sub-images with respect to significance level of corresponding sub-images (b) visibility level ($f_{\max} - f$) of watermarks with respect to significance level of corresponding sub-images



(a)



(b)

Figure 5.14: Watermarking results based on user-study that correspond to Fig. 5.12 for comparison between proposed and existing [132] watermark embedding strategies. Significance level is computed using visual saliency. (a) user-study response based average similarity level ($f - f_{\min}$, f = IW-SSIM) of watermarked sub-images with respect to significance level of corresponding sub-images (b) user-study response based average visibility level of watermarks with respect to user-study response based significance level of corresponding sub-images

- Average similarity level of watermarked sub-images for the proposed watermark embedding strategy increases with increase in significance level.
- Average similarity level of watermarked sub-images for the existing watermark embedding strategy of Liu et al. [132] is almost constant and near 0.5 with respect to significance level. This small value indicates that watermarked sub-images are very distorted.
- Average visibility level of the watermark for existing watermark embedding strategy of [132] is almost constant with respect to significance level.
- Average visibility level of watermark for proposed watermark embedding strategy slightly decreases with respect to significance level.
- Average visibility level of watermark for existing watermark embedding strategy of [132] is more than our proposed watermark embedding strategy. However, watermark is visible for both the watermark embedding strategies.

From these observations, we conclude that the proposed embedding strategy follows general visible watermarking rules for all kind of images while the existing embedding strategy of [132] does not follow general rules of visible watermarking, especially for high informative images (for example, Im_6, Im_7 and Im_8).

5.4.5 Experiment 5

This experiment compares the proposed embedding strategy and watermark embedding strategy of [132] with respect to robustness (robustness is measured by effects of attacks on the watermarked images). Attacked watermarked images are evaluated using image analysis.

Fig. 5.15 shows various attacked versions of the watermarked images (Fig. 5.12 (a) and Fig. 5.12 (e)). Top row of Fig. 5.15 corresponds to the watermarked image of Fig. 5.12 (e) and bottom row of the Fig. 5.15 corresponds to the watermarked image of Fig. 5.12 (a). From Fig. 5.15, we observe that watermark is visible in all attacked versions of Fig. 5.12 (a) and Fig. 5.12 (e) except cropping of 80%. For cropping of 80%, watermark is not visible in both attacked version of Fig. 5.12 (a) and Fig. 5.12 (e) (top and bottom row of Fig. 5.15 (b)). This verifies that effects of attack on the visibility of watermark are equal for the proposed watermark embedding strategy and watermark embedding strategy of [132].

Figure 5.15: Attack analysis and comparison between proposed and existing [132] watermark embedding strategies. Results are corresponding to Fig. 5.12. Top row in each sub-figures is corresponding to proposed watermark embedding strategy and the bottom rows are corresponding to existing watermark embedding strategy of [132]. (a): Cropping 20% (b): cropping 80 % (c) Gaussian noise, variance=0.001 (d) Gaussian noise, variance=0.001 (e) Gaussian filter, variance 1, filter size 11X11 (f) histogram equalization (g) JPEG compression, quality factor=70 (h) scaling down and up, scale factor=0.5 (i) rotation 5 degree (j) rotation -5 degree (k) salt and pepper noise, density=0.1

5.5 Conclusions

A visible watermarking algorithm is proposed, in which watermarking positions are automatically found using visual saliency/eye fixation density map such that important portions of image are not occluded by watermarks. A mathematical model is proposed in terms of importance of portion of an image, which automatically determines the optimal embedding energy during the implementation. Distribution of embedding energy in watermarking position is controlled by just noticeable distortion to achieve minimum visual degradation.

The proposed visible watermarking algorithm obeys rules of 'good' visible watermarking. Proposed watermarking embedding strategy is better than state of the art visible watermark embedding strategy. Error between watermarking results of proposed algorithm and the proposed mathematical model is negligible. This supports that the proposed mathematical model is valid. The proposed watermark embedding strategy and state of the art visible watermark embedding strategy have same robustness.

Chapter 6

Study of Comparators for Binary Watermarks

According to information theory, images of negative pair such as binary images of negative pair provide same information. Based on this, we assume that in watermarking, negative of binary watermark must be treated same as itself. This chapter examines the effect of different comparators on watermarking system under the above discussed assumption. We have examined five comparators based on five different similarity measure functions. These comparators are based on the normalized Hamming similarity (NHS), the normalized correlation coefficient (NCC), the mean subtracted NCC (MSNCC), symmetric NHS (SNHS, a version derived from NHS), and absolute MSNCC (AMSNCC, a version derived from MSNCC). Among these five comparator functions, SNHS and AMSNCC based comparators treat negative of binary watermark same as itself.

We have evaluated the performance of watermarking systems using ROC curve. A generic algorithm has been discussed to plot ROC curve for a generic watermarking system. Further, a formula has been derived using analytic proof to find the threshold interval corresponds to (FPR, FNR)=(0,0) for SNHS based comparator for a given watermarking system. We have proposed the algorithms which help to compute the threshold interval using the derived formula. We have also verified the derived formula with respect to ROC curve for several watermarking systems.

The rest of the chapter is organized as follows. In section 6.1, different comparators are defined. In section 6.2, ROC curve is defined and an algorithm to plot ROC curve for a generic watermarking system is discussed. The derived analytical formula with proof is discussed in section 6.3. Experimental evaluation of comparators and validation of analytical formula have been done in section 6.4. Conclusions of the chapter are drawn in section 6.5.

6.1 Comparators

This section defines the various comparators based on different similarity measure functions which are used in watermarking.

6.1.1 Normalized Hamming Similarity (NHS)

Kundur et al. [112, 113], Patra et al. [162], Rani et al. [178] and Rawat et al. [181, 183] have used NHS, which is widely used similarity measure function in watermarking. This measures the similarity between two binary images (in particular, binary watermarks) of equal length/size. NHS between two binary watermarks x_1 and x_2 is defined as follows:

$$\mathrm{NHS}(x_1, x_2) \quad = \quad 1 - \frac{1}{N_x} \sum_{i=1}^{N_x} x_1(i) \oplus x_2(i), \tag{6.1}$$

where, N_x is the length/size of each watermark, $\oplus$ is a bit-wise XOR (exclusive OR) operation. NHS ranges from 0 to 1. If NHS is 1, then both watermarks are exactly same. If NHS is 0, then all the corresponding bits in x_1 and x_2 are opposite, i.e. watermarks are exactly negative of each other. If NHS is 0.5, then half of the corresponding bits are the same and the other half are opposite. Therefore, NHS can estimate the degree of common information in two watermarks. The degree of common information is symmetrical about NHS = 0.5, minimum at NHS = 0.5 and maximum at NHS $= 1, 0$.

The corresponding comparator is defined as follows:

$$C_{(\tau,\ \mathrm{NHS})}(x_1, x_2) = \begin{cases} \text{match} & \text{if} \quad \mathrm{NHS}(x_1, x_2) \geq \tau \\ \text{no match} & \text{otherwise} \end{cases}. \tag{6.2}$$

The range of threshold (τ) is [0,1].

Two fundamental properties of the NHS are as follows:

$$\mathrm{NHS}(x_1, x_2) + \mathrm{NHS}(x_2, x_3) \leq 1 + \mathrm{NHS}(x_1, x_3), \tag{6.3}$$

$$\mathrm{NHS}(x_1, x_2) + \mathrm{NHS}(x_2, x_3) \geq 1 - \mathrm{NHS}(x_1, x_3), \tag{6.4}$$

where, x_1, x_2 and x_3 are three arbitrary binary watermarks of the same length/size.

6.1.2 Normalized Correlation Coefficient (NCC/NC)

Bhatnagar et al. [15], Cox et al. [39], Craver et al. [42], Kundur et al. [114] and Sharma et al. [193] have used NCC which is another widely used similarity measure function in watermarking. This measures the similarity between two images (in particular, watermarks) of equal length/size. NCC between any two watermarks x_1 and x_2 is defined as follows:

$$\text{NCC}(x_1, x_2) = \frac{\sum_{i=1}^{N_x} x_1(i).x_2(i)}{\sqrt{\sum_{i=1}^{N_x} x_1(i)^2}\sqrt{\sum_{i=1}^{N_x} x_2(i)^2}}, \tag{6.5}$$

where, N_x is the length/size of each watermark.

NCC ranges from 0 to 1. If NCC is 1, then both the watermarks are exactly same. Similarity between two watermarks increases with increase in NCC value.

The corresponding comparator is defined as follows:

$$C_{(\tau,\ \text{NCC})}(x_1, x_2) = \begin{cases} \text{match} & \text{if} \quad \text{NCC}(x_1, x_2) \geq \tau \\ \text{no match} & \text{otherwise} \end{cases}. \tag{6.6}$$

The range of τ is [0,1]. Note that this comparator can not work, if either of watermark is a pure black image.

6.1.3 Mean Subtracted Normalized Correlation Coefficient (MSNCC)

NCC does not return a well predicted value, if watermarks are negative of each other. MSNCC is an extended version of NCC, that provides a well predicted value for a negative pair of watermarks. MSNCC [19, 159] between any two watermarks x_1 and x_2 is defined as follows:

$$\text{MSNCC}(x_1, x_2) = \frac{\sum_{i=1}^{N_x}(x_1(i) - \bar{x_1}).(x_2(i) - \bar{x_2})}{\sqrt{\sum_{i=1}^{N_x}(x_1(i) - \bar{x_1})^2}\sqrt{\sum_{i=1}^{N_x}(x_k(i) - \bar{x_1})^2}} \tag{6.7}$$

where, N_x is length/size of each watermark, $\bar{x_1}$ and $\bar{x_2}$ are mean (average) value of watermarks x_1 and x_2 respectively.

MSNCC ranges from -1 to 1. If MSNCC is 1, then both watermarks are exactly same, if MSNCC is -1, watermarks are exactly negative of each other.

The corresponding comparator is defined as follows:

$$C_{(\tau,\ \mathrm{MSNCC})}(x_1, x_2) = \begin{cases} \text{match} & \text{if} \quad \mathrm{MSNCC}(x_1, x_2) \geq \tau \\ \text{no match} & \text{otherwise} \end{cases} . \tag{6.8}$$

The range of τ is [-1,1]. Note that this comparator can not work, if either of watermark is an uniform intensity image.

6.1.4 Absolute Mean Subtracted Normalized Correlation Coefficient (AMSNCC)

AMSNCC is an extended version of MSNCC, that treats negative images same as itself. AMSNCC between any two watermarks x_1 and x_2 is defined as follows:

$$\mathrm{AMSNCC}(x_1, x_2) \quad = \quad |\mathrm{MSNCC}(x_1, x_2)| . \tag{6.9}$$

AMSNCC ranges from 0 to 1. If AMSNCC is 1, then both watermarks are exactly same or exactly negative of each other.

The corresponding comparator is defined as follows:

$$C_{(\tau,\ \mathrm{AMSNCC})}(x_1, x_2) = \begin{cases} \text{match} & \text{if} \quad \mathrm{AMSNCC}(x_1, x_2) \geq \tau \\ \text{no match} & \text{otherwise} \end{cases} . \tag{6.10}$$

The range of τ is [0,1]. Note that like MSNCC based comparator, this comparator also can not work, if either of watermark is an uniform intensity image.

6.1.5 Symmetric Normalized Hamming Similarity (SNHS)

SNHS is an extended version of NHS, that treat negative of binary watermark same as itself. SNHS between any two watermarks x_1 and x_2 is defined as follows:

$$\text{SNHS}(x_1, x_2) = 0.5 + |\text{NHS}(x_1, x_2) - 0.5|. \tag{6.11}$$

SNHS ranges from 0.5 to 1. If SNHS is 1, then both watermarks are exactly same or exactly negative of each other.

The corresponding comparator is defined as follows:

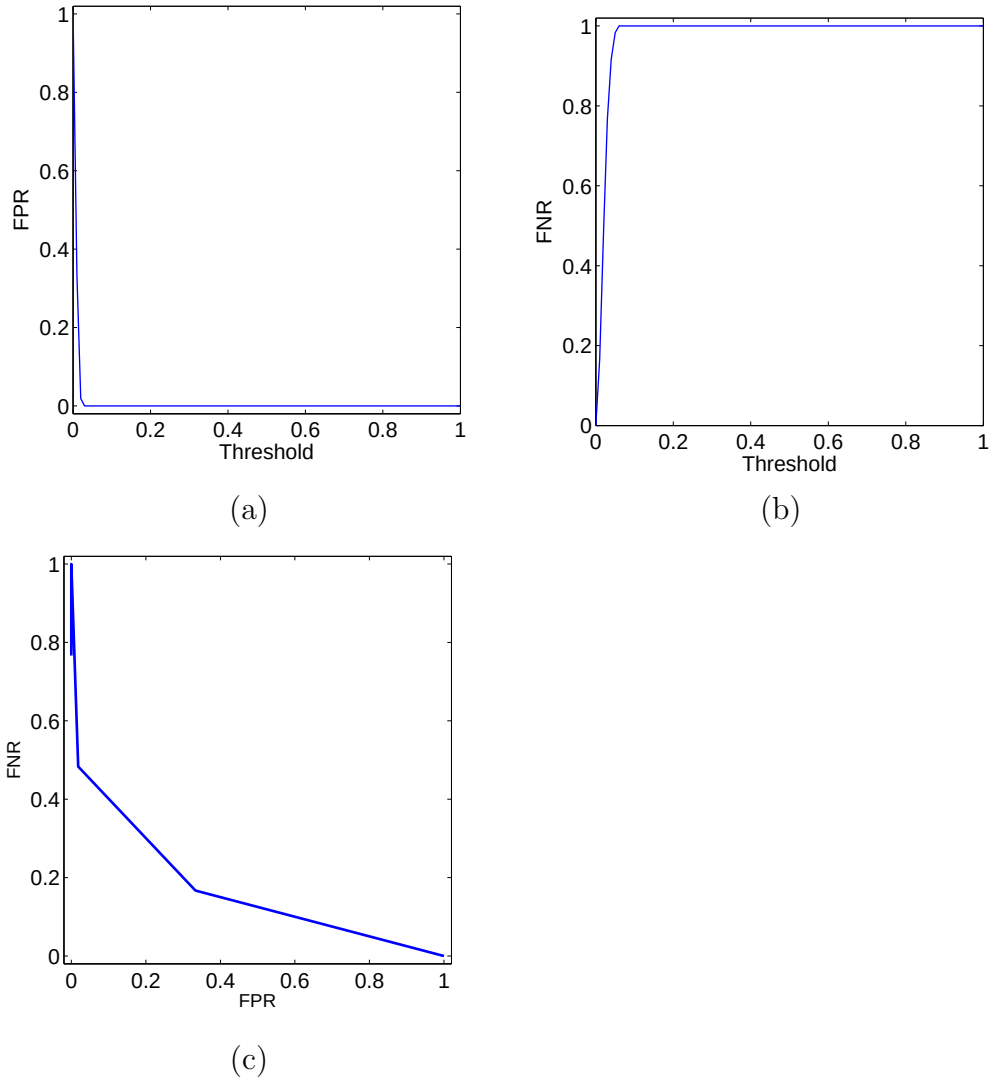
$$C_{(\tau,\ \text{SNHS})}(x_1, x_2) = \begin{cases} \text{match} & \text{if} \quad \text{SNHS}(x_1, x_2) \geq \tau \\ \text{no match} & \text{otherwise} \end{cases}. \tag{6.12}$$

The range of τ is [0.5 1].

6.2 Receiver Operating Characteristic (ROC)

As discussed in section 1.1, the final goal of a watermarking system is to decide, whether a watermark is present or not in a received media. The decision accuracy of a watermarking system is evaluated using receiver operating characteristic (ROC) curve [221, 212]. ROC curve is defined as a two dimensional plot of false positive rate FPR (defined as a ratio of total number of wrong matched case to the total number to actual matched case) versus false negative rate FNR (defined as a ratio of total number of wrong non-matched case to the total number to actual non-matched case). The range of FPR and FNR is [0,1].

(FPR, FNR)=(0,0) is the ideal point on a ROC curve. We must tune the parameters of watermarking system to obtain the ideal point (FPR, FNR)=(0,0). However, in practice, obtaining the ideal point is always not possible. In that case, we tune the parameters of watermarking system to obtain an optimal point (a point on ROC curve nearest to the ideal point) on the ROC curve.



(a) (b)

(c)

Figure 6.1: ROC curve of a watermarking system. (a) FPR versus Threshold τ (b) FNR versus Threshold τ (c) ROC curve (FPR versus FNR)

Table 6.1: List of symbols used in chapter 6.

X	Set of watermarks.
H	Set of host images.
τ	Threshold.
$\tau_{\min}$	minimum value of threshold (τ) in the range.
$\tau_{\max}$	maximum value of threshold (τ) in the range.
sim	Similarity measure function.
$C_{(\tau,\ \mathrm{sim})}$	Comparator of similarity measure function 'sim'.
M	Watermarking scheme.
M_{emb}	Watermark embedding algorithm.
M_{ext}	Watermark extraction algorithm.
K	Watermark embedding algorithm key.
K'	Watermark extraction algorithm key.
N	Number of iteration for threshold.

A generic algorithm to plot ROC curve with respect to threshold parameter τ for a given generic watermarking system is discussed in algorithm 15. The symbols used in the algorithm 15 are explained in table 6.1 and consistent with those discussed in section 1.2.

Fig. 6.1 (a) shows FPR with respect to threshold, Fig. 6.1 (b) shows FNR with respect to threshold, and Fig. 6.1 (c) shows ROC curve with respect to threshold (FPR versus FNR plot) for of a watermarking system. In the watermarking system, AMSNCC based comparator is used. Therefore, in Fig. 6.1 (a) and Fig. 6.1 (b), range of threshold is [0,1].

Algorithm 15 A generic algorithm to plot ROC curve of a given watermarking system

Input: X, H, τ_{min}, τ_{max}, t, N, $C_{(\tau,\text{sim})}$, $M = (\text{M}_{\text{emb}}, \text{M}_{\text{ext}})$, K, K' ▷ See table 6.1 for detailed explanation of symbols.

Output: ROC, graph(τ, FPR), graph(τ, FNR).

for $l = 1 : 1 : N + 1$
for $i = 1 : 1 : |X|$
for $j = 1 : 1 : |H|$
$\tau = \tau_{min} + (l-1)(\frac{\tau_{max} - \tau_{min}}{N})$
$Positive(\tau) = Negative(\tau) = False\_Positive(\tau) = False\_Negative(\tau) = 0$
Select $x_i \in X$, $h_j \in H$.
Obtain the watermarked image $\hat{h}_{ij}$ from x_i and h_j by using K and M_{emb}.
Apply noise/attack t on the $\hat{h}_{ij}$ to obtain noisy/attacked watermarked image $\hat{\hat{h}}_{ij}$.
Extract watermark $\hat{x}_{ij}$ from $\hat{\hat{h}}_{ij}$ by using M_{ext} and K'.
for $k = 1 : 1 : |X|$
if $(C_{(\tau,\ \text{sim})}(\hat{x}_{ij}, x_k) == \text{match AND } i == k)$
$Positive(\tau) = Positive(\tau) + 1$;
$False\_Positive(\tau) = False\_Positive(\tau)$;
end
if $(C_{(\tau,\ \text{sim})}(\hat{x}_{ij}, x_k) == \text{match AND } i \neq k)$
$Positive(\tau) = Positive(\tau)$;
$False\_Positive(\tau) = False\_Positive(\tau) + 1$;
end
if $(C_{(\tau,\ \text{sim})}(\hat{x}_{ij}, x_k) == \text{no match AND } i == k)$
$Negative(\tau) = Negative(\tau)$;
$False\_Negative(\tau) = False\_Negative(\tau) + 1$;
end
if $(C_{(\tau,\ \text{sim})}(\hat{x}_{ij}, x_k) == \text{no match AND } i \neq k)$
$Negative(\tau) = Negative(\tau) + 1$;
$False\_Negative(\tau) = False\_Negative(\tau)$;
end
end
end
end
$\text{FPR}(\tau) = False\_Positive(\tau)/Positive(\tau)$;
$\text{FNR}(\tau) = False\_Negative(\tau)/Negative(\tau)$;
end
$[FPR\_temp, index] = \text{sort}(\text{FPR})$;
$[FNR\_temp] = \text{FNR}(index)$;
$\text{ROC} = \text{graph}(FPR\_temp, FNR\_temp)$;
Return ROC, graph(τ, FPR), graph(τ, FNR).

Algorithm 16 An algorithm to compute MSNHS

Input: X ▷ See table 6.1 for detailed explanation of symbol.
Output: MSNHS.

SNHS=zeros($|X|, |X|$) ▷ Creates a matrix of size $|X| \times |X|$ with each element is 0.
for $i = 1 : 1 : |X|$
for $j = i + 1 : 1 : |X|$
SNHS$(i, j) = 0.5 + |\text{NHS}(x_i, x_j) - 0.5|$
end
end
MSNHS=max(SNHS) ▷ returns maximum value of the matrix SNHS.
Return MSNHS

Algorithm 17 An algorithm to compute P

Input: X, H, t, $M = (\text{M}_{\text{emb}}, \text{M}_{\text{ext}})$, K, K' ▷ See table 6.1 for detailed explanation of symbol.
Output: P

SNHS=zeros($|X|, |H|$) ▷ Creates a matrix of size $|X| \times |H|$ with each element is 0.
for $i = 1 : 1 : |X|$
for $j = 1 : 1 : |H|$
Select $x_i \in X$, $h_j \in H$
Obtain the watermarked image $\hat{h}_{ij}$ from x_i and h_j by using K and M_{emb}.
Apply noise/attack t on the $\hat{h}_{ij}$ to obtain noisy/attacked watermarked image $\hat{\hat{h}}_{ij}$.
Extract watermark $\hat{x}_{ij}$ from $\hat{\hat{h}}_{ij}$ by using M_{ext} and K'.
Compute SNHS$(i, j) = 0.5 + |\text{NHS}(\hat{x}_{ij}, x_i) - 0.5|$.
end
end
$P = \min(\text{SNHS})$ ▷ find minimum value of the matrix SNHS.
Return P

6.3 Theoretical Analysis of SNHS Based Comparator

According to Linnartz et al. [129], "*Theoretical modeling of watermarks allow prediction of the detector reliability and facilitates the development of more reliable systems*".

Linnartz et al. [129] have proposed a mathematical model to express the probability of incorrect detection (missed detection or false alarm) in terms of watermark-energy-to-image-luminance-ratio.

Miller et al. [143] have proposed a formula for the probability of false detection of watermarking system with respect to comparator threshold. The comparator is based on normalized correlation coefficient similarity measure function. The formula holds exactly if pixels of watermarks are drawn from independent, identical, zero-mean Gaussian distributions.

Tian et al. [216] have proposed a formula for the probability of false positive with respect to threshold. Ratio of the largest normalized correlation to the second largest when an extracted vector is compared to multiple reference vectors is used as a similarity measure function. The formula is based on an uniform distribution assumption.

Xiao et al. [237] have derived the expressions for false negative and false positive of dither modulation based watermarking system. The derived expressions are for no noise and Gaussian noise cases.

Motivated with these literature, in this section, theoretical analysis of SNHS based comparator is discussed.

For any watermarking system, set of watermarks should not consist duplicate watermarks to avoid trivial ambiguity in the decision. Further, the ideal point on ROC curve (FPR,FNR)=(0,0) is a common requirement of any efficient watermarking system. In this section, we will discuss the following:

1. A condition on set of watermarks in terms of a function of SNHS to avoid trivial ambiguity in the decision. An algorithm is proposed to ensure this condition.

2. A sufficient condition on threshold interval is discussed to ensure the existence of the ideal point (FPR,FNR)=(0,0) on ROC curve of a watermarking system. An algorithm is proposed to compute the terms used in this sufficient condition.

3. A formula is discussed and proved using the sufficient condition, which provides a threshold interval that corresponds to the ideal point (FPR,FNR)=(0,0) on ROC curve of a watermarking system. We name the threshold interval corresponds to the ideal point as *ideal threshold interval*.

In this section, all the discussions are based on the assumption that negative of a watermark is treated same as itself.

6.3.1 Condition for Avoiding Duplicate Watermarks in a Set of Watermarks

A sufficient condition to avoid duplicate watermarks (same watermarks/negative pair of watermarks) in a set of watermarks is as follows:

$$\text{MSNHS}(X) < 1 \tag{6.13}$$

where, X is a set of watermarks and MSNHS(X) is called maximum symmetric normalized Hamming similarity of set of watermarks X and defined as follows:

$$\text{MSNHS}(X) = \max \left\{ \begin{array}{c} \text{SNHS}(x_i, x_j) : \\ x_i, x_j \in X, i \neq j \end{array} \right\}. \tag{6.14}$$

By the definition of MSNHS(X), it is clear that

$$1 - \text{MSNHS(X)} \quad \leq \quad \text{NHS}\,(x_i, x_j) \leq \text{MSNHS(X)} \tag{6.15}$$

for all watermarks of X.

A method to compute MSNHS(X) is provided in algorithm 16.

6.3.2 Sufficient Condition for the Existence of (FPR, FNR)=(0,0)

A sufficient condition for the existence of (FPR, FNR)=(0,0) for a given watermarking system is as follows:

$$\text{MSNHS}(X) < 2P(M, t, X, H, K, K') - 1 \tag{6.16}$$

where, the term $P(M, t, X, H, K, K')$ represents the minimum similarity of any embedded watermark with respect to the corresponding extracted watermark for a given watermarking system. A method to compute $P(M, t, X, H, K, K')$ is provided in algorithm 17. In rest of the chapter, for convenience, we will use P instead of $P(M, t, X, H, K, K')$.

6.3.3 Threshold Interval Corresponds to (FPR, FNR)=(0,0)

If the sufficient condition (6.16) is satisfied, then a threshold interval of SNHS based comparator for a given generic watermarking system corresponds to (FPR, FNR)=(0,0) is given by

$$\frac{1 + \text{MSNHS}}{2} < \tau \leq P. \tag{6.17}$$

Note that the actual interval may be super-interval of this interval and condition (6.16) ensures that the interval in (6.17) exists.

For a generic watermarking system, the significance of (FPR, FNR)=(0,0) is that

1. Each extracted watermark is matched with correct watermark.

2. Each extracted watermark is uniquely matched.

In the next sections (section 6.3.4 and section 6.3.5), we will provide an analytic proof for above said statement.

6.3.4 Proof for Each Extracted Watermark is Correctly Matched if (6.16) Holds

Let x be an extracted watermark corresponding to an original embedded watermark $x_i \in X$. Sufficient condition (6.16) ensures that the threshold interval provided by the formula (6.17) exists. According to the formula (6.17) and by definition of P (section 6.3.2), we have,

$$\text{SNHS}(x, x_i) \geq P$$

$$\Rightarrow \text{SNHS}(x, x_i) \geq \tau$$

$$\Rightarrow x \text{ is matched with } x_i.$$

Thus we have proved that if (6.16) holds, then threshold satisfies the formula (6.17) provides correct matching of each extracted watermark.

6.3.5 Proof for Each Extracted Watermark is Uniquely Matched if (6.16) Holds

If possible, let us assume that an extracted watermark x is matched with two watermarks, x_i and x_j in X. Therefore, according to the definition of SNHS based comparator, we have

$$\text{SNHS}(x, x_i) \geq \tau$$

and

$$\text{SNHS}(x, x_j) \geq \tau$$

where τ satisfies inequality (6.17). Thus, we have the following four possible cases:

case(i):

$$\text{NHS}(x, x_i) \geq \tau \text{ and } \text{NHS}(x, x_j) \geq \tau.$$

case(ii):

$$\text{NHS}(x, x_i) \leq 1 - \tau \text{ and } \text{NHS}(x, x_j) \leq 1 - \tau.$$

case(iii):

$$\text{NHS}(x, x_i) \geq \tau \text{ and } \text{NHS}(x, x_j) \leq 1 - \tau.$$

case(iv):

$$\text{NHS}(x, x_i) \leq 1 - \tau \text{ and } \text{NHS}(x, x_j) \geq \tau.$$

Now, we will discuss one by one.

case(i):

$$\begin{gathered}
\text{NHS}(x, x_i) \ \geq \tau \text{ and } \text{NHS}(x, x_j) \geq \tau \Rightarrow \\
\text{NHS}(x, x_i) \geq \tau > \tfrac{1+\text{MSNHS}}{2} \\
\text{and} \\
\text{NHS}(x, x_j) \geq \tau > \tfrac{1+\text{MSNHS}}{2} \quad \Rightarrow \\
\text{NHS}(x, x_i) + \text{NHS}(x, x_j) > 1 + \text{MSNHS} \Rightarrow \\
\text{NHS}(x, x_i) + \text{NHS}(x, x_j) > 1 + \text{NHS}(x_i, x_j) \Rightarrow
\end{gathered}$$

a contradiction by a fundamental property of NHS (6.3).

case(ii):

$$\begin{gathered}
\text{NHS}(x, x_i) \ \leq 1 - \tau \text{ and } \text{NHS}(x, x_j) \leq 1 - \tau \Rightarrow \\
\text{NHS}(x, x_i) \leq 1 - \tau < \tfrac{1-\text{MSNHS}}{2} \\
\text{and} \\
\text{NHS}(x, x_j) \leq 1 - \tau < \tfrac{1-\text{MSNHS}}{2} \quad \Rightarrow \\
\text{NHS}(x, x_i) + \text{NHS}(x, x_j) < 1 - \text{MSNHS} \Rightarrow \\
\text{NHS}(x, x_i) + \text{NHS}(x, x_j) < 1 - \text{NHS}(x_i, x_j) \Rightarrow
\end{gathered}$$

a contradiction by a fundamental property of NHS (6.4).

case(iii):

$$\mathrm{NHS}(x, x_i) \geq \tau \text{ and } \mathrm{NHS}(x, x_j) \leq 1 - \tau \Rightarrow$$

$$\mathrm{NHS}(x, x_i) \geq \tau > \tfrac{1+\mathrm{MSNHS}}{2}$$

and

$$\mathrm{NHS}(x, x_j) \leq 1 - \tau < \tfrac{1-\mathrm{MSNHS}}{2} \quad \Rightarrow$$

$$\mathrm{NHS}(x, x_i) - \mathrm{NHS}(x, x_j) > \mathrm{MSNHS} \Rightarrow$$

$$\mathrm{NHS}(x, x_i) - \mathrm{NHS}(x, x_j) > 1 - \mathrm{NHS}(x_i, x_j) \Rightarrow$$

$$\mathrm{NHS}(x, x_i) + \mathrm{NHS}(x_i, x_j) > 1 + \mathrm{NHS}(x, x_j) \Rightarrow$$

a contradiction by a fundamental property of NHS (6.3).

case(iv): This proof is similar to the proof for *case (iii)*.

Thus we have proved that if (6.16) holds, then threshold satisfies the formula (6.17) provides unique matching of each extracted watermark.

Table 6.2: Explanation of data-sets used in experiments

Data set	set of original images	number of original images	size of original images (pixels)	set of watermarks	number of watermarks	size of watermarks (pixels)
D_1	H_1	6	256×256	X_1	10	128×128
D_2	H_2	10	256×256	X_2	10	128×128
D_3	$H_3 = H_2$	10	256×256	X_3	20	128×128
D_4	H_4	20	256×256	X_4	10	128×128
D_5	H_5	30	256×256	X_5	5	128×128
D'_1	H'_1	6	512×512	X'_1	10	64×64
D'_2	H'_2	10	512×512	X'_2	10	64×64
D'_3	$H'_3 = H'_2$	10	512×512	X'_3	20	64×64
D'_4	H'_4	20	512×512	X'_4	10	64×64
D'_5	H'_5	30	512×512	X'_5	5	64×64

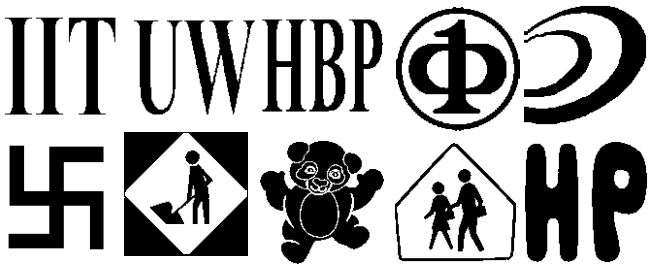


Figure 6.2: Explanation of sets of watermarks X_1 and X'_1.

6.4 Experiments, Results and Analysis

We have done two experiments namely Experiment 1 and Experiment 2. The main objective of the first experiment (Experiment 1) is to compare the performance of watermarking systems with respect to different comparators. The objective of the second experiment (Experiment 2) is to validate the derived analytical formula for threshold interval determination corresponds to (FPR, FNR)=(0,0). The derived analytic formula is verified with respect to algorithm 1.

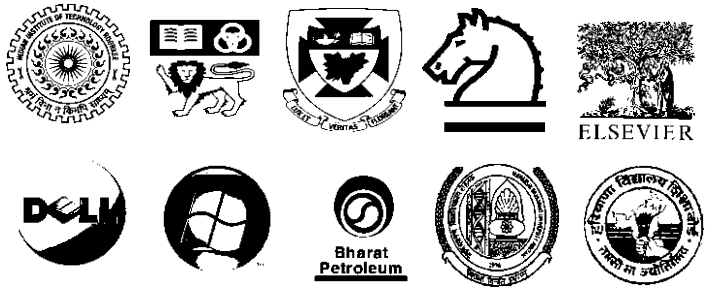


Figure 6.3: Explanation of sets of watermarks X_2 and X'_2.

Figure 6.4: Explanation of sets of watermarks X_3 and X'_3.

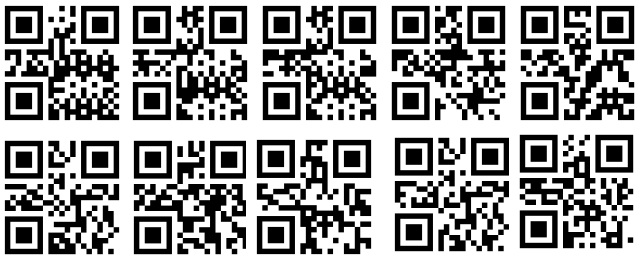


Figure 6.5: Explanation of sets of watermarks X_4 and X'_4.

Figure 6.6: Explanation of sets of watermarks X_5 and X'_5.

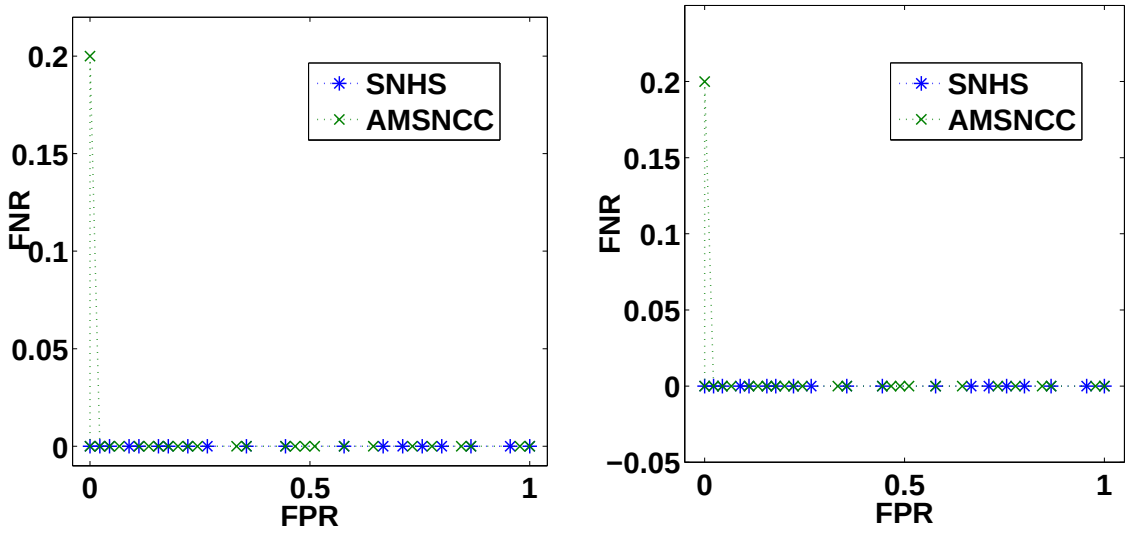
Figure 6.7: Explanation of sets of original images H_1 and H'_1.

Figure 6.8: Explanation of sets of original images H_2 and H'_2. Note that $H_3 = H_2$ and $H'_3 = H'_2$

Figure 6.9: Explanation of sets of original images H_4 and H'_4.

Figure 6.10: Explanation of sets of original images H_5 and H_5'.

In experiments, we have used several watermarking systems. Watermarking systems are corresponding to two watermarking schemes and ten data-sets. One watermarking scheme is of Wong et al. [235] and second watermarking scheme is of Bhatnagar et al. [15]. Each data-set consists of set of host images and set of watermarks. The data-sets are named as D_1, D_2, $\cdots$, D_5, D'_1, D'_2, $\cdots$, D'_5. These are briefly explained in table 6.2. D_1 is similar to D'_1, D_2 is similar to D'_2 and so on. The meaning of similar is that one data-set of pair of similar data-sets consists of scaled versions of original images and watermarks of other data-set. Figs. 6.2 – 6.6 show watermarks of the data sets and Figs. 6.7 – 6.10 show original images of the data sets. Data-sets D_1, D_2, $\cdots$, D_5 are combined with watermarking scheme of [235] and data-sets D'_1, D'_2, $\cdots$, D'_5 are combined with watermarking scheme of [15] to generate watermarking systems in the experiments.



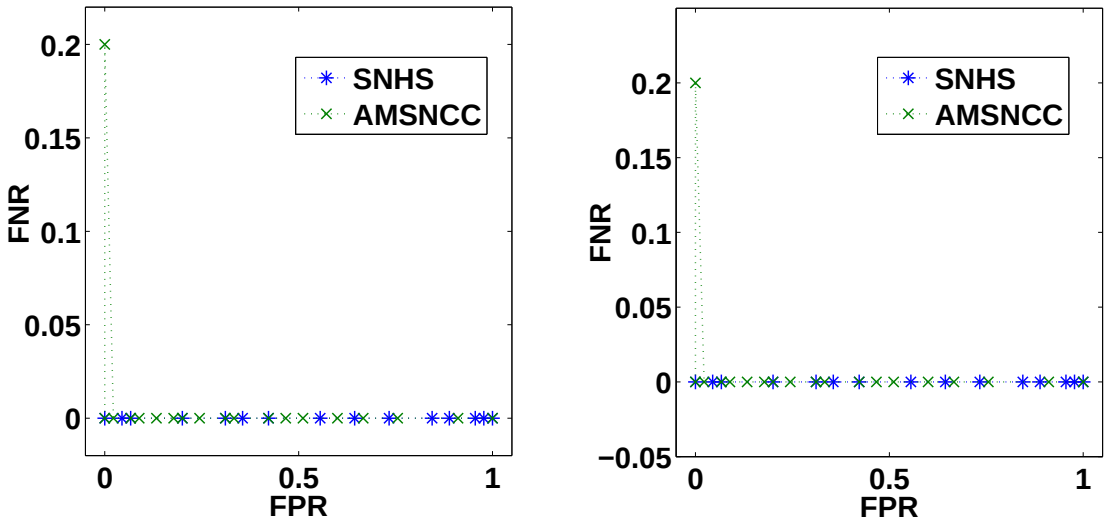
(a) (b)

Figure 6.11: ROC curves of watermarking systems. Data set is D_1, watermarking scheme is of Wong et al. [235]. (a) no attack (b) negative attack.

6.4.1 Experiment 1: Comparison of Comparators

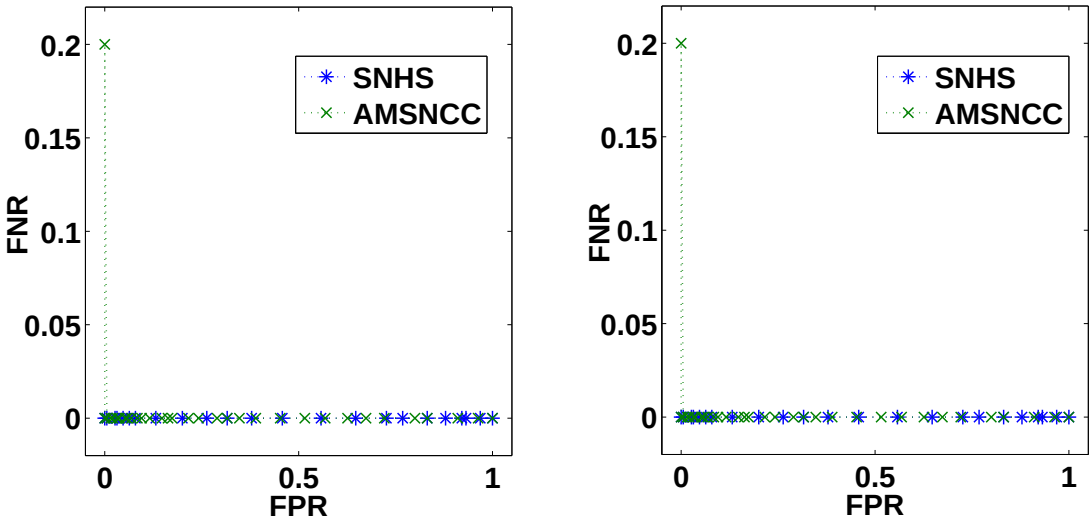
This experiment compares the performance of watermarking systems with respect to different comparators. The performance is evaluated using ROC curves. We have plotted the ROC curves of watermarking systems based on SNHS and AMSNCC based comparators. To evaluate the robustness of watermarking systems, we have applied several attacks such as negative operation followed by average filtering, Gaussian filtering, Gaussian noise, JPEG compression, and rotation on watermarked images. We have computed the threshold intervals for ideal point (FPR, FNR)=(0,0) on ROC curves using the algorithm 1 for several watermarking systems.

Figs. 6.11 – 6.15 show ROC curves of watermarking systems generated using data-sets D_1, D_2, $\cdots$, D_5 and watermarking scheme of [235]. The channel condition is either no attack or negative attack on the watermarked images. Table 6.3 provides threshold interval for ideal point of the ROC curves shown in Figs. 6.11 – 6.15.



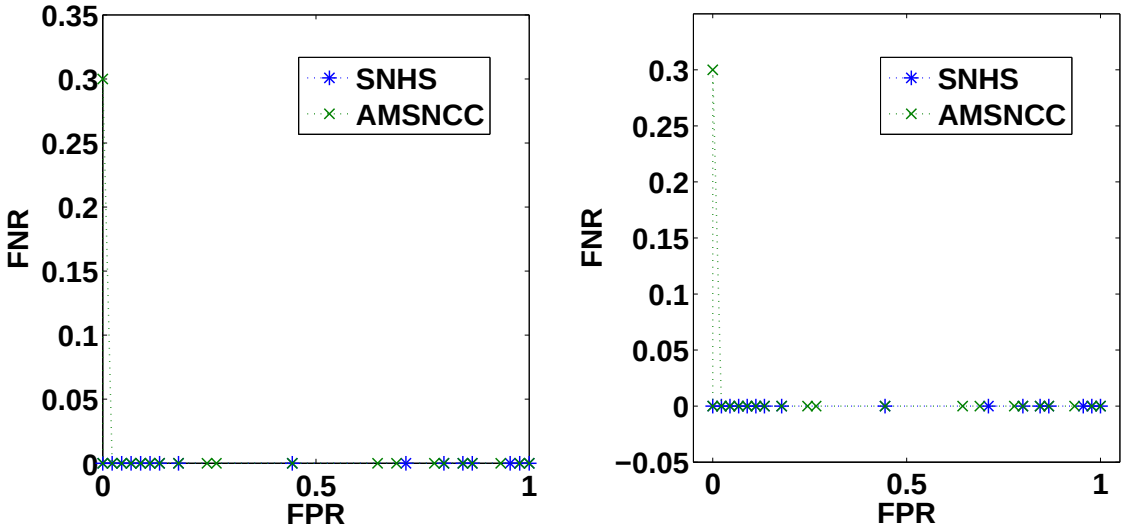
(a) (b)

Figure 6.12: ROC curves of watermarking systems. Data set is D_2, watermarking scheme is of [235]. (a) no attack (b) negative attack.



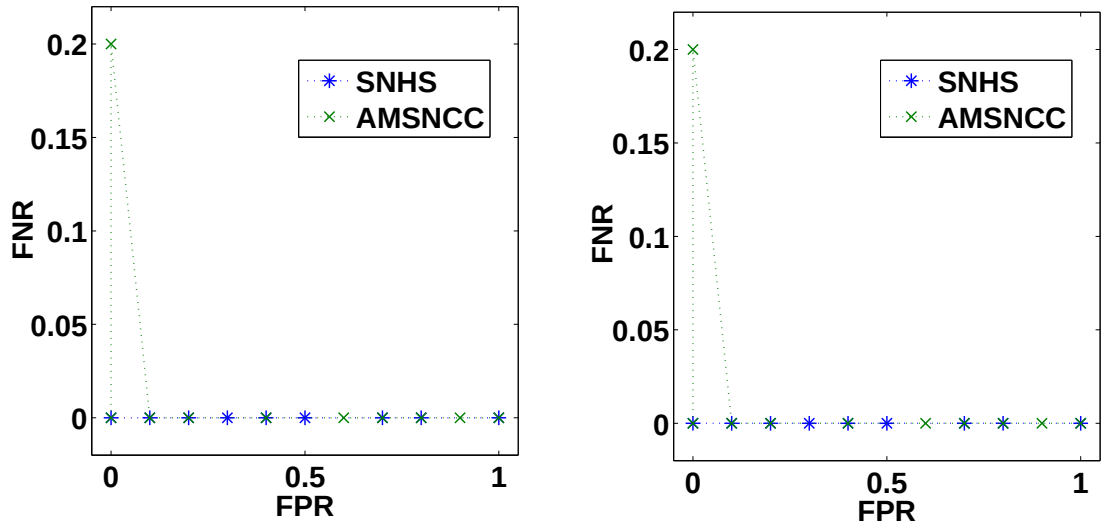
(a) (b)

Figure 6.13: ROC curves of watermarking systems. Data set is D_3, watermarking scheme is of [235]. (a) no attack (b) negative attack.



(a) (b)

Figure 6.14: ROC curves of watermarking systems. Data set is D_4, watermarking scheme is of [235]. (a) no attack (b) negative attack.

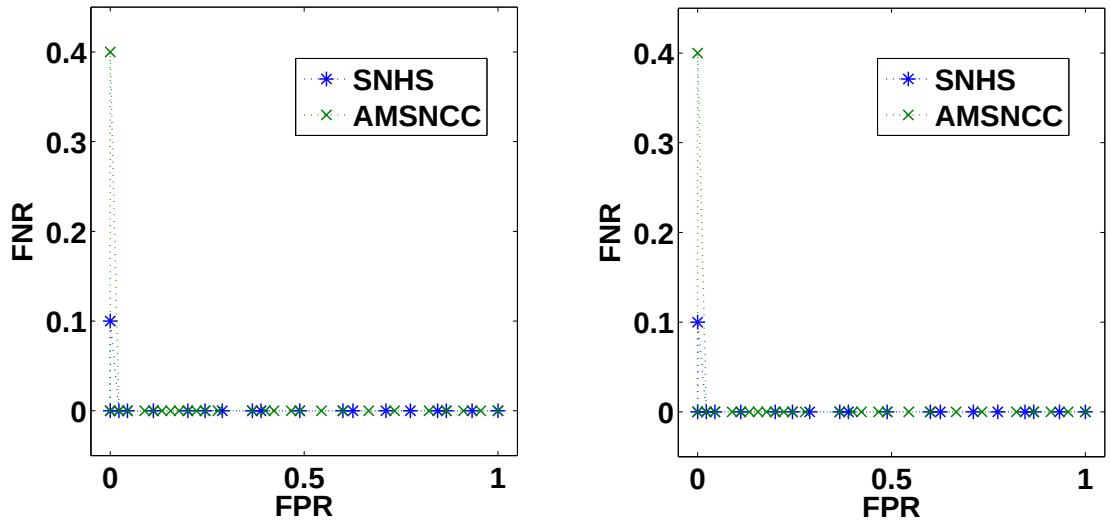


(a) (b)

Figure 6.15: ROC curves of watermarking systems. Data set is D_5, watermarking scheme is of [235]. (a) no attack (b) negative attack.

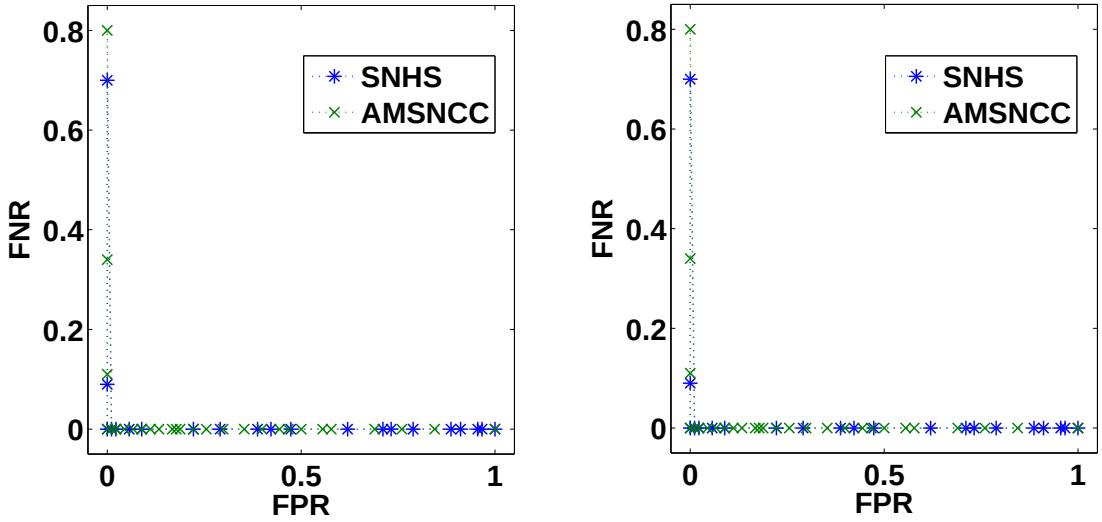
Table 6.3: Threshold interval that corresponds to (FPR, FNR)=(0,0) of various watermarking systems. Watermarking scheme is of Wong et al. [235], comparators are based on SNHS and AMSNCC.

Data-Set	Channel condition	Threshold interval for	
		AMSNCC	SNHS
D_1	no attack	[0.39,1.00]	[0.74, 1.00]
D_1	negative attack	[0.39,1.00]	[0.74, 1.00]
D_2	no attack	[0.23,1.00]	[0.68,1.00]
D_2	negative attack	[0.23,1.00]	[0.68,1.00]
D_3	no attack	[0.39, 1.00]	[0.74, 1.00]
D_3	negative attack	[0.39, 1.00]	[0.74, 1.00]
D_4	no attack	[0.90,1.00]	[0.96,1.00]
D_4	negative attack	[0.90,1.00]	[0.96,1.00]
D_5	no attack	[0.38,1.00]	[0.74, 1.00]
D_5	negative attack	[0.38,1.00]	[0.74, 1.00]



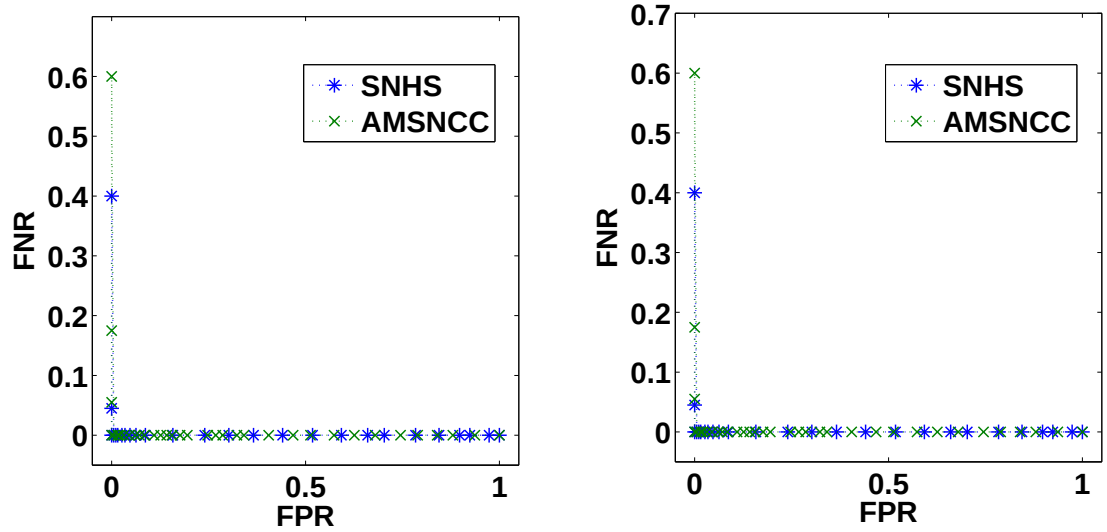
(a) (b)

Figure 6.16: ROC curves of watermarking systems. Data set is D_1', watermarking scheme is of Bhatnagar et al. [15]. (a) no attack (b) negative attack.



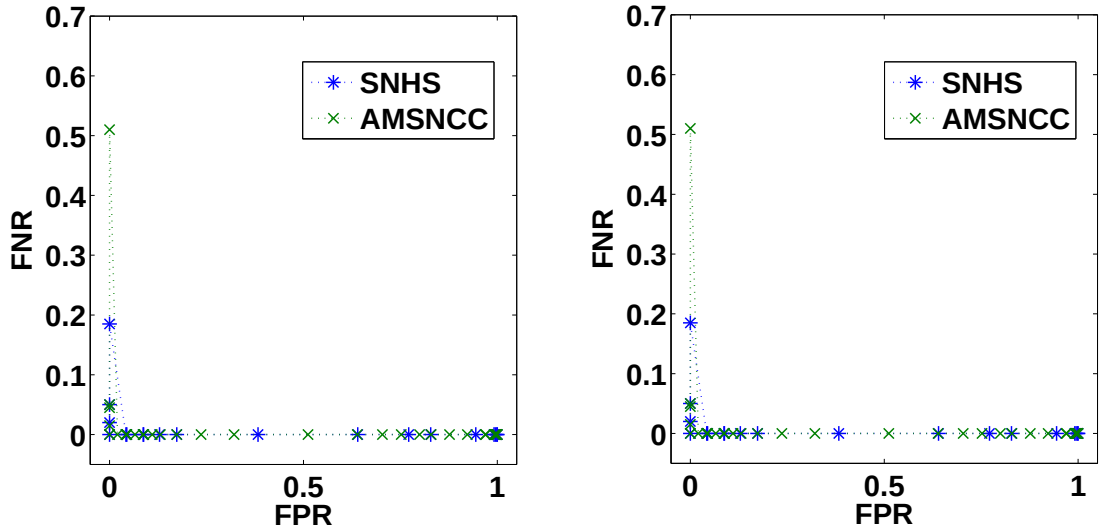
(a) (b)

Figure 6.17: ROC curves of watermarking systems. Data set is D'_2, watermarking scheme is of [15]. (a) no attack (b) negative attack.



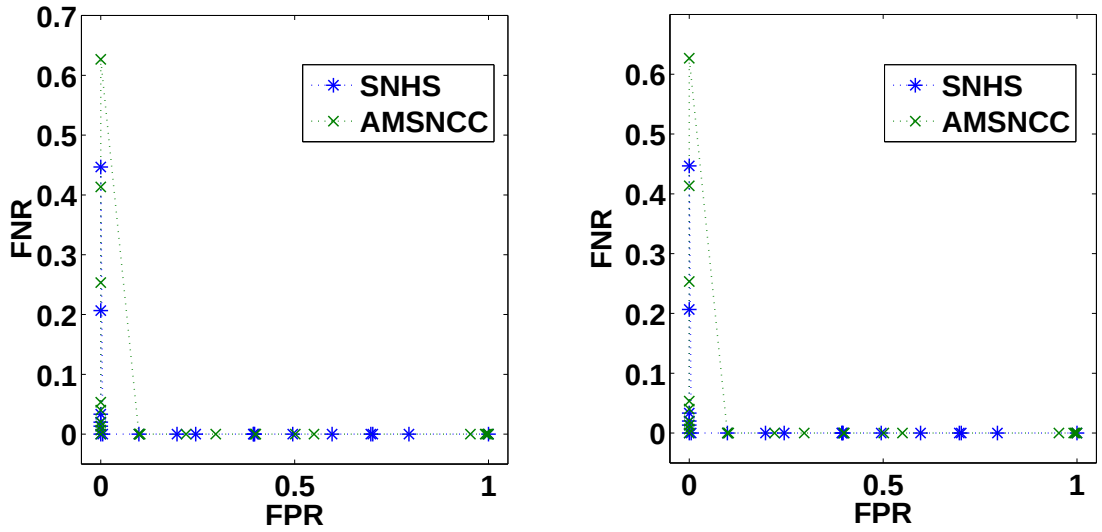
(a) (b)

Figure 6.18: ROC curves of watermarking systems. Data set is D'_3, watermarking scheme is of [15]. (a) no attack (b) negative attack.



(a) (b)

Figure 6.19: ROC curves of watermarking systems. Data set is D'_4, watermarking scheme is of [15]. (a) no attack (b) negative attack.



(a) (b)

Figure 6.20: ROC curves of watermarking systems. Data set is D'_5, watermarking scheme is of [15]. (a) no attack (b) negative attack.

Table 6.4: Threshold interval that corresponds to (FPR, FNR)=(0,0) of various watermarking systems. Watermarking scheme is of Bhatnagar et al. [15], comparators are based on SNHS and AMSNCC.

Data-Set	Channel condition	Threshold interval for	
		AMSNCC	SNHS
D_1'	no attack	[0.43, 1.00]	[0.73, 0.99]
D_1'	negative attack	[0.43, 1.00]	[0.73, 0.99]
D_2'	no attack	[0.27, 0.97]	[0.69, 0.98]
D_2'	negative attack	[0.27, 0.97]	[0.69, 0.98]
D_3'	no attack	[0.43, 0.97]	[0.73, 0.98]
D_3'	negative attack	[0.43, 0.97]	[0.73, 0.98]
D_4'	no attack	[0.91, 0.93]	{0.96}
D_4'	negative attack	[0.91, 0.93]	{0.96}
D_5'	no attack	[0.43, 0.82]	[0.65, 0.91]
D_5'	negative attack	[0.43, 0.82]	[0.65, 0.91]

Table 6.5: Threshold interval that corresponds to (FPR, FNR)=(0,0) of various watermarking systems. Watermarking scheme is of Wong et al. [235], comparators are based on SNHS and AMSNCC, data set is D_1.

Channel condition	Threshold interval for	
	AMSNCC	SNHS
Negative+Gaussian Filter, var=0.3	[0.39, 0.97]	[0.74, 0.99]
Negative+Gaussian Filter, var=0.7	does not exist	does not exist
Negative+Gaussian noise, var=10^{-5}	[0.28, 0.62]	[0.68, 0.84]
Negative+Gaussian noise, var=10^{-4}	does not exist	{0.54}
Negative+Gaussian noise, var=10^{-3}	does not exist	does not exist
Negative+JPEG 95	[0.15, 0.28]	[.60, .66]
Negative+JPEG 90	[0.09, 0.13]	[.57, .58]
Negative+JPEG 80	does not exist	doest not exist
Negative+Rotation 0.2	[0.39, 0.99]	[0.74, 1.00]
Negative+Rotation 0.5	[0.09, 0.16]	{0.59}
Negative+Rotation 1	does not exist	doest not exist

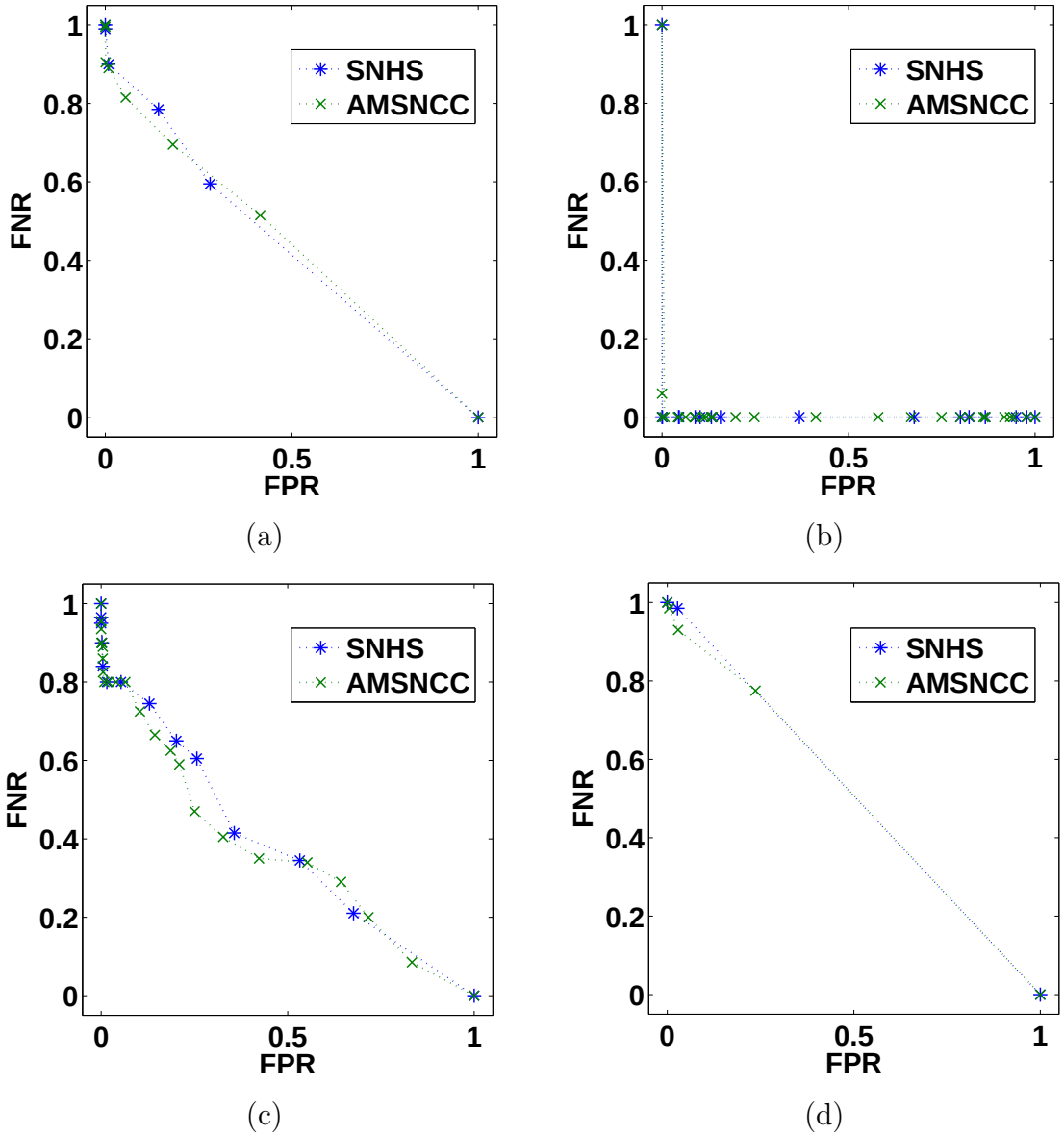
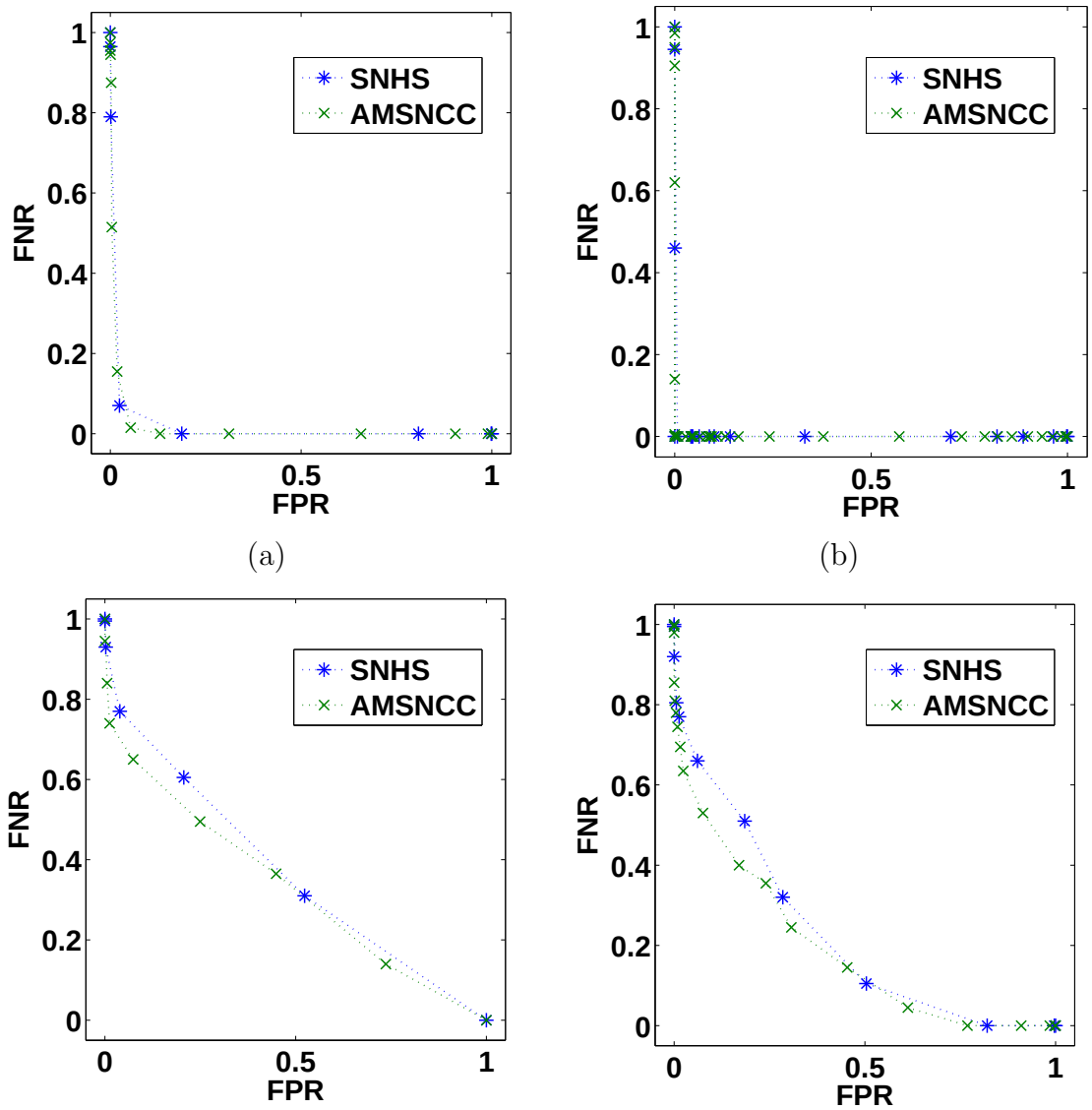


Figure 6.21: ROC curves of watermarking systems. Data set is D_4, watermarking scheme is of [235]. (a) Negative+ average filtering, filter size 3×3 (b) Negative+ Gaussian filtering, variance 0.3 (c) Negative+ Gaussian filtering, variance 0.7 (d) Negative+ Gaussian noise, variance=10^{-3}



(a) (b)

(a) (b)

Figure 6.22: ROC curves of watermarking systems. Data set is D_4, watermarking scheme is of [235]. (a) Negative+ Gaussian noise, variance=10^{-4} (b) Negative+ Gaussian noise, variance=10^{-5} (c) Negative+ JPEG compression, quality factor=80 (d) Negative+ JPEG compression, quality factor=90

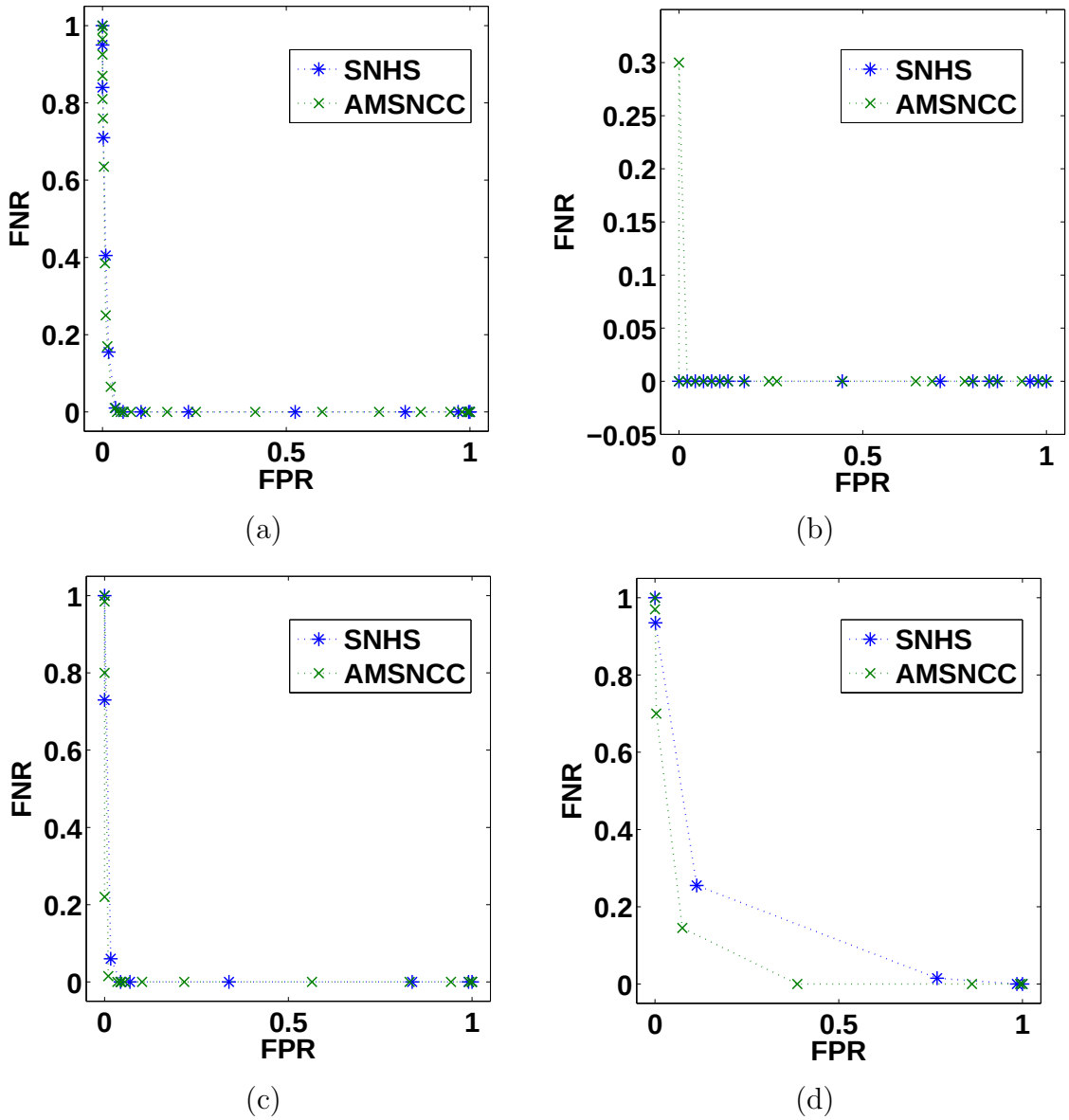
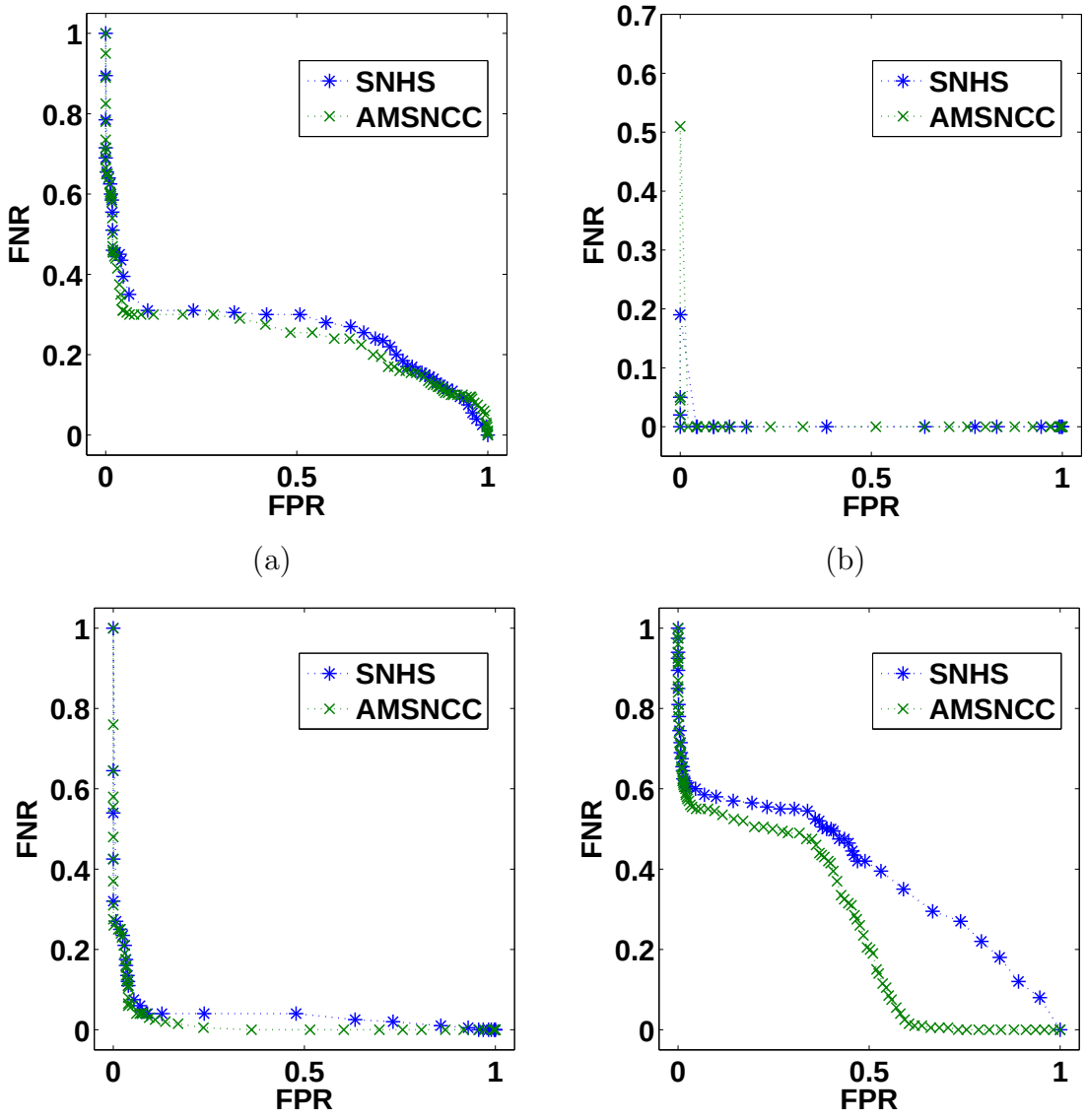


Figure 6.23: ROC curves of watermarking systems. Data set is D_4, watermarking scheme is of [235]. (a) Negative+ JPEG compression, quality factor=95 (b) Negative+ rotation, rotation degree=0.2 (c) Negative+ rotation, rotation degree=0.5 (d) Negative+ rotation, rotation degree=1



(a) (b)

(a) (b)

Figure 6.24: ROC curves of watermarking systems. Data set is D_4', watermarking scheme is of [15]. (a) Negative+ average filtering, filter size 3×3 (b) Negative+ Gaussian filtering, variance 0.3 (c) Negative+ Gaussian filtering, variance 0.7 (d) Negative+ Gaussian noise, variance=10^{-3}

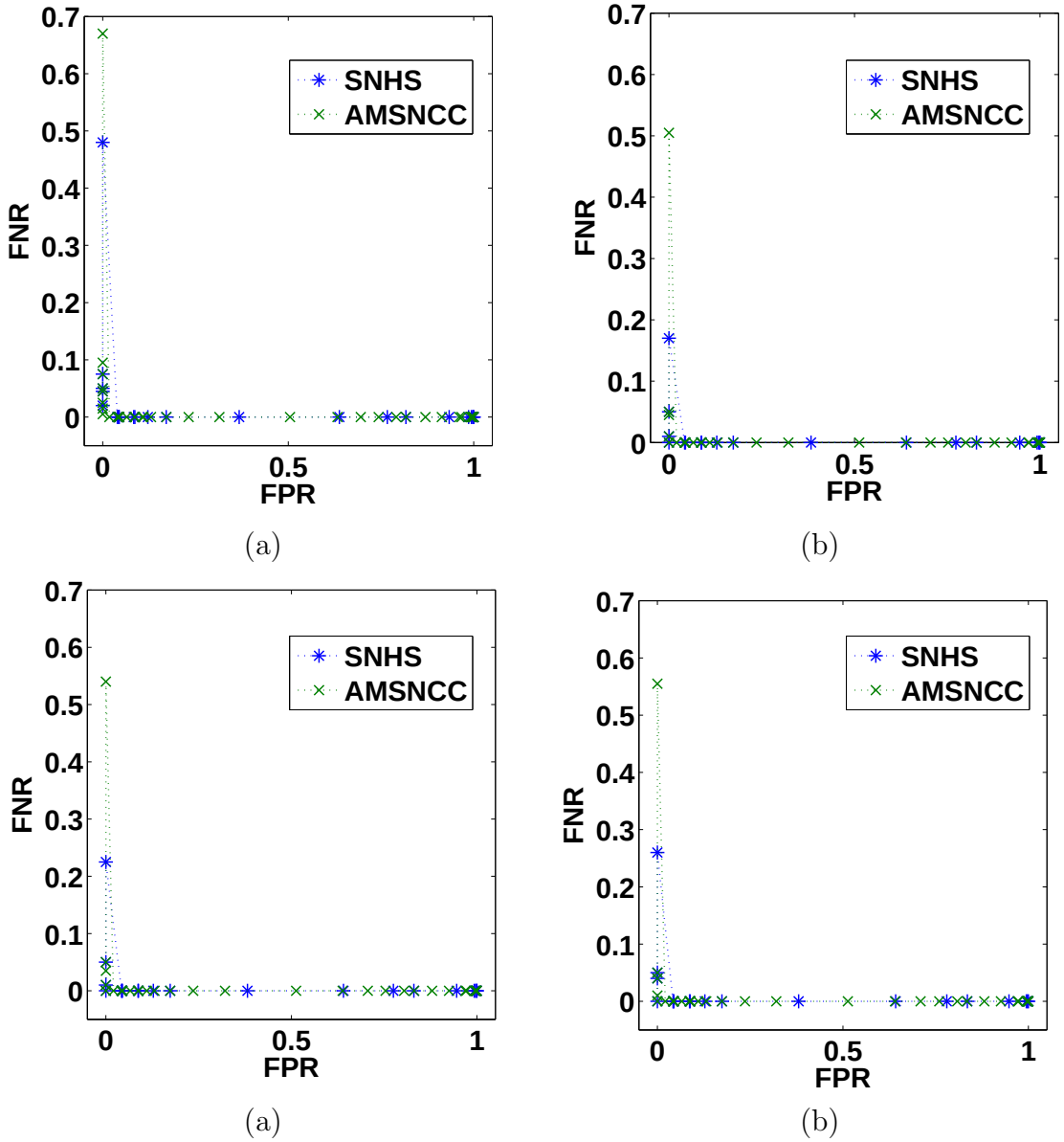


Figure 6.25: ROC curves of watermarking systems. Data set is D'_4, watermarking scheme is of [15]. (a) Negative+ Gaussian noise, variance=10^{-4} (b) Negative+ Gaussian noise, variance=10^{-5} (c) Negative+ JPEG compression, quality factor=95 (d) Negative+ JPEG compression, quality factor=90

Table 6.6: Threshold interval that corresponds to (FPR, FNR)=(0,0) of various watermarking systems. Watermarking scheme is of Bhatnagar et al. [15], comparators are based on SNHS and AMSNCC, data set is D_1'.

Channel condition	Threshold interval for	
	AMSNCC	SNHS
Negative+Gaussian Filter, var=0.3	[0.42, 0.99]	[0.73, 0.99]
Negative+Gaussian Filter, var=0.7	does not exist	does not exist
Negative+Gaussian noise, var=10^{-5}	[0.43, 0.99]	[0.73, 0.99]
Negative+Gaussian noise, var=10^{-4}	[0.43, 0.99]	[0.73, 0.99]
Negative+Gaussian noise, var=10^{-3}	does not exist	does not exist
Negative+JPEG 95	[0.43, 0.99]	[0.73, 0.99]
Negative+JPEG 90	[0.43, 0.99]	[0.73, 0.99]
Negative+JPEG 80	[0.43, 0.98]	[0.73, 0.99]
Negative+Rotation 0.2	does not exist	does not exist
Negative+Rotation 0.5	does not exist	does not exist

Figs. 6.16 – 6.20 show ROC curves of watermarking systems generated using data-sets D_1', D_2', $\cdots$, D_5' and watermarking scheme of [15]. The channel condition is either no attack or negative attack on the watermarked images. Table 6.4 provides threshold interval for ideal point of the ROC curves shown in Figs. 6.16 – 6.20.

Figs. 6.21 – 6.23 show ROC curves of watermarking systems under various attacks on watermarked images. The watermarking systems are generated using the data-set D_4 and the watermarking scheme of [235].

Table 6.5 provides threshold interval for ideal point of the ROC curves of watermarking systems under various channel conditions. The watermarking systems are generated using the data-set D_1 and the watermarking scheme of [235].

Figs. 6.24 – 6.25 show ROC curves of watermarking systems under various attacks on watermarked images. The watermarking systems are generated using the data-set D_4' and the watermarking scheme of [15].

Table 6.6 provides threshold interval for ideal point of the ROC curves of watermarking systems under various channel conditions. The watermarking systems are generated using the data-set D_1' and the watermarking scheme of [15].

The highlights of the experiment are as follows:

- Choice of comparator is useful to determine the performance of watermarking systems. For watermarking systems generated using watermarking scheme of Wong et al. [235], AMSNCC and SNHS based comparators have better performance than NHS, NCC and MSNCC based comparators against negative attack on watermarked images. The reason for better performance of AMSNCC and SNHS based comparators is that the extracted watermarks were negative of original embedded watermarks.

- For watermarking systems generated using watermarking scheme of [15], the performance of all the comparators (NHS, NCC, MSNCC, AMSNCC and SNHS based comparators) is same for all the studied cases. The reason for same performance of all the comparators is that the extracted watermarks were not negative of original embedded watermarks.

- The performance of AMSNCC and SNHS based comparators is very close.

- The length of threshold interval that corresponds to the point (FPR,FNR)=(0,0) decrease with increase in attack level and finally the threshold interval vanishes.

- The performance of the watermarking systems degrades with attack level.

Table 6.7: Verification of analytic formula for threshold interval determination that corresponds to (FPR, FNR)=(0,0). Watermarking scheme is of Wong et al. [235].

Data-Set	Channel condition	P	MSNHS	Threshold interval for SNHS using		Verified
				Generic algorithm	Derived formula	
D_1	no attack	1	0.7347	[0.74, 1.00]	(.86,1.00]	Yes
D_1	negative attack	1	0.7347	[0.74, 1.00]	(.86,1.00]	Yes
D_2	no attack	1	0.6799	[0.68,1.00]	(.83,1.00]	Yes
D_2	negative attack	1	0.6799	[0.68,1.00]	(.83,1.00]	Yes
D_3	no attack	1	0.7347	[0.74, 1.00]	(.86,1.00]	Yes
D_3	negative attack	1	0.7347	[0.74, 1.00]	(.86,1.00]	Yes
D_4	no attack	1	0.9501	[0.96,1.00]	(.97,1.00]	Yes
D_4	negative attack	1	0.9501	[0.96,1.00]	(.97,1.00]	Yes
D_5	no attack	1	0.6371	[0.64, 1.00]	(.81,1.00]	Yes
D_5	negative attack	1	0.6371	[0.64, 1.00]	(.81,1.00]	Yes

6.4.2 Experiment 2: Verification of Analytic Formula of Threshold Interval Determination that Corresponds to (FPR, FNR)=(0,0)

This experiment verifies the analytical formula (6.17) of threshold interval determination that corresponds to (FPR, FNR)=(0,0). In the analytical formula, two terms MSNHS and P are required. The term MSNHS is computed using the algorithm 16 and the term P is computed using the algorithm 17. The verification of the analytical formula has been done with respect to algorithm 15 for several watermarking systems.

Table 6.7 verifies the analytical formula for watermarking systems generated using data-sets D_1, D_2, $\cdots$, D_5 and watermarking scheme of Wong et al. [235]. The channel condition is either no attack or negative attack on the watermarked images.

Table 6.8: Verification of analytic formula for threshold interval determination that corresponds to (FPR, FNR)=(0,0). Watermarking scheme is of Bhatnagar et al. [15].

Data-Set	Channel condition	P	MSNHS	Threshold interval for SNHS using		Verified
				Generic algorithm	Derived formula	
D'_1	no attack	0.9963	0.7212	[0.73, 0.99]	(.86, .99]	Yes
D'_1	negative attack	0.9963	0.7212	[0.73, 0.99]	(.86, .99]	Yes
D'_2	no attack	0.9880	0.6819	[0.69, 0.98]	(.84, .98]	Yes
D'_2	negative attack	0.9880	0.6819	[0.69, 0.98]	(.84, .98]	Yes
D'_3	no attack	0.9880	0.7212	[0.73, 0.98]	(.86, .98]	Yes
D'_3	negative attack	0.9880	0.7212	[0.73, 0.98]	(.86, .98]	Yes
D'_4	no attack	0.9673	0.9526	{0.96}	does not reply	Yes
D'_4	negative attack	0.9673	0.9526	{0.96}	does not reply	Yes
D'_5	no attack	0.9133	0.6399	[0.65, 0.91]	(.81, .91]	Yes
D'_5	negative attack	0.9133	0.6399	[0.65, 0.91]	(.81, .91]	Yes

Table 6.8 verifies the analytical formula for watermarking systems generated using data-sets D'_1, D'_2, $\cdots$, D'_5 and watermarking scheme of Bhatnagar et al. [15]. The channel condition is either no attack or negative attack on the watermarked images.

Table 6.9 verifies the analytical formula for watermarking systems under various attacks on watermarked images. The watermarking systems are generated using the data-set D_1 and the watermarking scheme of [235].

Table 6.10 verifies the analytical formula for watermarking systems under various attacks on watermarked images. The watermarking systems are generated using the data-set D'_1 and the watermarking scheme of [15].

Table 6.9: Verification of analytic formula for threshold interval determination that corresponds to (FPR, FNR)=(0,0). Watermarking scheme is of Wong et al. [235], data-set is D_1 and MSNHS=0.7347.

Channel condition	P	Threshold interval for SNHS using		Verified
		Generic algorithm	Derived formula	
Negative+Gaussian Filter, var=0.3	0.9904	[0.74, 0.99]	(0.86,0.99]	Yes
Negative+Gaussian Filter, var=0.7	0.5165	does not exist	does not reply	Yes
Negative+Gaussian noise, var=10^{-5}	0.8438	[0.68, 0.84]	does not reply	Yes
Negative+Gaussian noise, var=10^{-4}	0.5483	{0.54}	does not reply	Yes
Negative+Gaussian noise, var=10^{-3}	0.5	does not exist	does not reply	Yes
Negative+JPEG 95	0.6664	[.60, .66]	does not reply	Yes
Negative+JPEG 90	0.5836	[.57, .58]	does not reply	Yes
Negative+JPEG 80	0.5238	does not exist	does not reply	Yes
Negative+Rotation 0.2	1	[0.74, 1.00]	(.86,1.00]	Yes
Negative+Rotation 0.5	0.5955	{0.59}	does not reply	Yes
Negative+Rotation 1	0.5224	does not exist	does not reply	Yes

Table 6.10: Verification of analytic formula for threshold interval determination that corresponds to (FPR, FNR)=(0,0). Watermarking scheme is Bhatnagar of et al. [15], data-set is D_1' and MSNHS=0.7212.

Channel condition	P	Threshold interval for SNHS using		Verified
		Generic algorithm	Derived formula	
Negative+Gaussian Filter, var=0.3	0.9963	[0.73, 0.99]	(.86,.99]	Yes
Negative+Gaussian Filter, var=0.7	0.5073	does not exist	does not reply	Yes
Negative+Gaussian noise, var=10^{-5}	0.9958	[0.73, 0.99]	(.86,.99]	Yes
Negative+Gaussian noise, var=10^{-4}	0.9963	[0.73, 0.99]	(.86,.99]	Yes
Negative+Gaussian noise, var=10^{-3}	0.5261	does not exist	does not reply	Yes
Negative+JPEG 95	0.9954	[0.73, 0.99]	(.86,.99]	Yes
Negative+JPEG 90	0.9954	[0.73, 0.99]	(.86,.99]	Yes
Negative+JPEG 80	0.9954	[0.73, 0.99]	(.86,.99]	Yes
Negative+Rotation 0.2	0.5039	does not exist	does not reply	Yes
Negative+Rotation 0.5	0.5039	does not exist	does not reply	Yes

The highlights of the experiment for SNHS based comparator are as follows:

- The threshold interval that corresponds to the point (FPR, FNR)=(0,0) found using the formula (6.17) is subinterval of the actual threshold interval found using the algorithm 15.
- If the formula (6.17) does not find the threshold interval corresponds to the point (FPR, FNR)=(0,0), then the actual threshold interval may exist or may not exist.
- In all the studied cases (tables 6.7- 6.10), the formula (6.17) obeys algorithm 15.
- We have made two empirical observations for a given watermarking system. First is that if P is greater than $\frac{1+\text{MSNHS}}{2}$ then the actual threshold interval for the point (FPR, FNR)=(0,0) is [MSNHS,P]. Second is that that if P is less than $\frac{1+\text{MSNHS}}{2}$ then the upper bound on actual threshold interval for the point (FPR, FNR)=(0,0) is P.

6.5 Conclusions

We have studied five different comparators for watermarking systems of binary watermarks under the assumption that negative pair of binary watermark is treated same as itself. We have observed that if the extracted watermarks are negative of embedded watermarks then NHS, NCC and MSNCC based comparators give high false negative rate, while SNHS and AMCNCC based comparators give very low false negative rate. We have proposed a generic algorithm to plot ROC curve of a watermarking system with respect to threshold of a given comparator. We have provided an analytic formula to compute threshold interval for the ideal point ((FPR, FNR)=(0,0)) of ROC curve of a watermarking system of SNHS based comparator. We have computed the ideal threshold interval for several watermarking systems using the proposed algorithm 15 and derived formula (6.17). The terms MSNHS and P of the formula (6.17) are computed using the algorithms 16 and 17 respectively. We have verified that the formula (6.17) obeys the algorithm 15 and ideal threshold interval found using the formula (6.17) is a sub-interval of ideal threshold interval found using the algorithm 15.

Chapter 7

Conclusions and Future Scope

7.1 Conclusions

In this thesis, we have designed nine different watermarking schemes.

Four blind invisible watermarking schemes embed a face image in a gray scale image. Among these four schemes, two operate on the DWT domain and another two operate on the RDWT domain. One watermarking scheme of each domain incorporate a novel weighted binary coding. We have performed several experiments to evaluate the performance of these watermarking schemes. We have observed that the DWT based watermarking scheme has coupled with the weighted binary coding is the best choice for applications scenario such as owner identification, proof of ownership, and fingerprinting/transaction tracking.

Two invisible watermarking schemes embed a binary logo in a gray scale image. Watermark embedding has been done in the ROWT domain. Among these two, one is non-blind and other is blind. We have compared the proposed watermarking schemes with related state of the art and have also observed that the proposed watermarking schemes are more robust. Further, we have observed that the robustness of the proposed non-blind watermarking scheme is better than the proposed blind watermarking scheme.

Two blind invisible watermarking schemes verify the integrity of a face image based biometric system. One watermarking scheme operates in the spatial domain and other in the DCT domain. Spatial domain based watermarking scheme is reversible and fragile which detects tampering of the training face database. The DCT domain based watermarking scheme is robust against channel noise and detects unauthorized test images.

One spatial domain based visible watermarking scheme embeds a binary logo watermark at N non-overlapping positions in an image such that important portions of the image are not occluded. The image areas for embedding the watermark (watermarking positions) are found through visual saliency computation or available human eye fixation density maps. This is an automated watermarking scheme in which watermarking positions and optimal embedding strength are automatically determined. Several experiments have been performed to evaluate the performance of the proposed watermarking scheme. We observed that the proposed watermarking scheme obeys all the rules of 'good' visible watermarking scheme. Further, proposed watermarking scheme has better performance than related state of the art.

Apart from developing watermarking schemes, we have explored an opportunity to study the effect of comparators on the performance of watermarking system. We have studied the performance of binary watermark based watermarking system under the assumption that negative of binary watermark is treated same as itself, since negative pair of binary watermarks provides same information. We have used ROC curve to evaluate the performance of watermarking system. We have observed that SNHS and AMSNCC based comparators successfully identify extracted watermarks, if an extracted watermark is negative or same as of original embedded watermark. Further, we have derived a formula to find the threshold interval that corresponds to (FPR, FNR)=(0,0) for SNHS based comparator for a given watermarking system. We have verified the derived formula with respect to ROC curve for several watermarking systems.

7.2 Further Scope

7.2.1 Real Time Watermarking

Nine different watermarking schemes have been designed in this thesis. Algorithms of each watermarking scheme are compatible with high level language/productivity software such as MATLAB, C++, JAVA etc. For real time watermarking, hardware implementation of these watermarking schemes will be a scope. In hardware implementation, various characteristics such as silicon area, memory requirements, power consumptions and performance should be evaluated [108].

7.2.2 Video Watermarking

In this thesis, we have proposed a visible watermarking scheme, which embeds a binary logo in an image at optimal position instead of fixed position. This work has a great opportunity to extend for videos. In the extended work, video will be used instead of images. The watermark will be embedded at optimal position of each frame of the video. Optimal position, hence watermarking position will change with respect to frame. This change in watermarking position with respect to frame will be a new issue in video watermarking. Therefore, one more requirement in the extended work for video will be that change in watermarking position with respect to change in frames should not produce any unpleasant effect for viewers, for example, sudden change in watermarking position may disturb concentration of the viewers.

7.2.3 Cloud Computing

Cloud computing refers to both the applications delivered as services over the internet and the hardware and systems software in the data centers that provide those services. Cloud computing is the long dreamed vision of computing as a utility where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in cloud computing a very challenging and unavoidable task, especially for users with constrained computing resources and capabilities [226, 8].

In further scope, we can explore the watermarking techniques to find solution of problems related with data integrity protection in cloud computing.

Appendix A

PSNR and Capacity

A.1 PSNR

In this thesis, PSNR is used to analyze the visual quality of watermarked image with original image and visual quality of extracted watermark with original watermark. It has inverse relation with mean square difference (mean square error) between the two images. Mathematically, PSNR between two images, say $\mathbf{I}_1$ and $\mathbf{I}_2$ is defined as

$$PSNR(\mathbf{I}_1, \mathbf{I}_2) = \ 10 \times \log_{10} \frac{l_{peak}^2}{MSE(\mathbf{I}_1, \mathbf{I}_2)} \ ; \tag{A.1}$$

where, l_{peak} is the maximum gray level value in the images, $MSE(\mathbf{I}_1, \mathbf{I}_2)$ (mean square error) is

$$MSE(\mathbf{I}_1, \mathbf{I}_2) = \frac{1}{M_1 \times N_1} \sum_{i=1}^{M_1} \sum_{j=1}^{N_1} \left(I_1(i,j) - I_2(i,i)\right)^2, \tag{A.2}$$

and $M_1 \times N_1$ is size of the images. The unit of PSNR is decibel (dB).

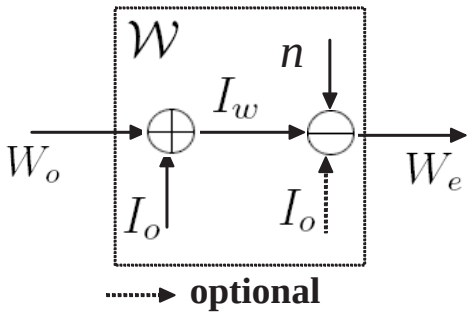


Figure A.1: Watermarking as a communication channel.

A.2 Capacity of Watermarking Scheme

Ramkumar et al. [176] have modeled watermarking process as a communication channel and defined the capacity. Fig. A.1 explains watermarking as a communication channel. In Fig. A.1, W_o is an original watermark, W_e is an extracted watermark and $\mathcal{W}$ is the watermarking channel. $\mathcal{W}$ consists of four components: a host image I_o, a watermark embedding algorithm $\oplus$ that embeds W_o in I_o and outputs I_w, a watermark extraction algorithm $\ominus$ that extracts W_e from I_w, and watermarking extraction algorithm noise $n = W_e - W_o$. The capacity of a watermarking scheme for a given host image is defined as follows:

$$C = M_2 \times N_2 \times \max\{h(W_e) - h(n)\}, \tag{A.3}$$

where, $M_2 \times N_2$ is the size/length of W_e/n; h is entropy which is defined as follows:

$$h(W) = \begin{cases} -\mathrm{P}_W(0)\log_2(\mathrm{P}_W(0)) - \mathrm{P}_W(1)\log_2(\mathrm{P}_W(1)) \\ \quad \text{if} \qquad \mathrm{P}_W(0) \text{ and } \mathrm{P}_W(1) \neq 0, \\ 0 \quad \text{if} \qquad \mathrm{P}_W(0) \text{ or } \mathrm{P}_W(1) = 0, \end{cases} \tag{A.4}$$

W is a binary image (watermark), and $\mathrm{P}_W(0)$ and $\mathrm{P}_W(1)$ are fractions of symbols 0 and 1, respectively, in W. The unit of capacity is bits.

Appendix B

Mathematical Preliminary

B.1 Convolution

Convolution of two real valued functions x and y defined on the set of real numbers is a real valued function of real variable defined as follows:

$$x(t) * y(t) = \int_{-\infty}^{\infty} x(\tau)y(t-\tau)d\tau, \quad t \in \mathbb{R} \text{ (set of real numbers)} \tag{B.1}$$

The symbol * denotes convolution operator.

B.2 Discrete Convolution

Convolution of two real valued functions x and y defined on the set of integers is a real valued function on the set of integers defined as follows:

$$x[n] * y[n] = \sum_{m=-\infty}^{\infty} x(m)y(n-m) \quad n \in \mathbb{Z} \text{ (set of integers)} \tag{B.2}$$

B.2.1 Discrete Cosine Transformation (DCT)

Discrete cosine transformation (DCT), $C_x(k)$, of a single variable, uniformly discretized signal, $x(n)$, of length N, is defined as follows [24]:

$$C_x(k) = \alpha(k) \sum_{n=0}^{N-1} x(n) \cos \frac{(2n+1)\pi k}{2N}, \tag{B.3}$$

where

$$\alpha(0) = \frac{1}{\sqrt{N}}, \quad \alpha(k) = \sqrt{\frac{2}{N}}, \quad 1 \leq k \leq N-1. \tag{B.4}$$

Conversely, given $C_x(k)$, we can obtain $x(n)$ using the inverse discrete cosine transformation (IDCT) as follows:

$$x(n) = \sum_{k=0}^{N-1} \alpha(k) C_x(k) \cos \frac{(2n+1)\pi k}{2N} \tag{B.5}$$

The DCT and IDCT pair of, two variable, uniformly discretized signal, $x(n_1, n_2)$, of size $N_1 \times N_2$, is defined by the equations (B.6) and((B.7)) respectively as follows:

$$C_x(k_1, k_2) = \alpha_1(k_1)\alpha_2(k_2) \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} x(n_1, n_2) \cos \frac{(2n_1+1)\pi k_1}{2N_1} \cos \frac{(2n_2+1)\pi k_2}{2N_2}. \tag{B.6}$$

$$x(n_1, n_2) = \sum_{k_1=0}^{N_1-1} \sum_{k_2=0}^{N_2-1} \alpha_1(k_1)\alpha_2(k_2) C_x(k_1, k_2) \cos \frac{(2n_1+1)\pi k_1}{2N_1} \cos \frac{(2n_2+1)\pi k_2}{2N_2}. \tag{B.7}$$

DCT has several important properties [75], like, the DCT coefficients are purely real; the DCT has near-optimal property for energy compaction; and the DCT of a signal of length N can be computed in $O(N \log N)$ operations. These properties prove DCT as an excellent tool in image processing applications. Energy compaction property of DCT makes it as the most promising domain for texture classification.

B.3 Wavelet

In the past two decades, wavelets have been widely used in different fields such as signal and image processing, data compression, human vision, pattern recognition, image classification, image retrieval, image fusion, digital watermarking, etc. [138, 255, 168, 23, 172, 9, 201, 194, 4]. Some prominent properties of wavelets are:

1. Wavelet gives time frequency representation of a function.

2. The wavelets have the ability to provide different time and frequency resolutions at different frequencies. For low frequencies, wavelets provide good frequency resolution, but bad time resolution. For high frequencies, it is the other way around.

A wavelet is a wave-like oscillation with an amplitude that starts out at zero, increases, and then decreases back to zero. From mathematical point of view, we can define wavelets in term of scaling and shifted version of fundamental function known as mother wavelet. The wavelet corresponding to scale a and time location b is defined as follows [185]:

$$\psi_{a,b}(t) = \frac{1}{\sqrt{a}}\psi\left(\frac{t-b}{a}\right) \tag{B.8}$$

where $\psi(t)$ is the wavelet prototype, also known as mother wavelet. Mother wavelet is a band pass function. A mother wavelet must satisfy the following admissibility condition:

$$\int_{-\infty}^{\infty} \frac{|\Im(\psi(t))|^2}{|\omega|} d\omega < \infty \tag{B.9}$$

where $\Im(.)$ denotes the Fourier transform defined as follows:

$$\Im(\psi(t)) = \int_{-\infty}^{\infty} \psi(t) e^{-2\pi\iota t\omega} dt \tag{B.10}$$

where, ω is a real the Fourier domain variable, and $\iota = \sqrt{-1}$.

The inequality (B.9) describes that

1. the mother wavelet function must oscillate and have an average value of zero,

2. the mother wavelet must have exponential decay and exhibits compact support.

The factor $|a|^{-1/2}$ in equation (B.8) is used to ensure energy preservation [65, 110, 36].

B.3.1 Wavelet Transform

Goupillaud et al. [65] defined the continuous wavelet transform (CWT) of a finite energy analog signal $x(t)$ as follows:

$$CWT\left\{x(t); a, b\right\} = \int_{-\infty}^{\infty} x(t)\psi_{a,b}(t)\, dt \tag{B.11}$$

B.3.2 Wavelet Series

The wavelet transform can decompose a signal into two parts:

1. approximation part which describes large-scale (approximation) behavior of the signal,

2. detail part which describes small-scale (detail) behavior of the signal.

The approximation part is obtained using the scaling functions as basis, and the detail part is obtained using the wavelet functions as basis. A wavelet series representation of a finite energy analog signal $x(t)$ in terms of scaling and wavelets functions is as follows [64]:

$$x(t) = \sum_{k} a_{j_0,k}\phi_{j_0,k}(t) + \sum_{j=j_0}^{\infty}\sum_{k} d_{j,k}\psi_{j,k}(t) \tag{B.12}$$

where $\phi_{j,k}$, $\psi_{j,k}$, are stretched and shifted versions of a fundamental real valued scaling function ϕ and wavelet function ψ at scale j and position k defined as follows:

$$\phi_{j,k}(t) = 2^{-j/2}\phi\left(2^{-j}t - k\right) \tag{B.13}$$

$$\psi_{j,k}(t) = 2^{-j/2}\psi\left(2^{-j}t - k\right) \tag{B.14}$$

Note that in equations (B.13) and (B.14), $a = 2^j$, $b = 2^j k$ and $\phi_{j,k}$ and $\psi_{j,k}$ are orthonormal functions. In equation (B.12),

- coefficients $a_{j_0,k}$s (scaling/approximate coefficients) provide approximate part of the signal and are computed as follows:

$$a_{j_0,k} = \int_{-\infty}^{\infty} x(t)\phi_{j_0,k}(t)dt \tag{B.15}$$

- coefficients $d_{j,k}$s (wavelet/detail coefficients) provide detail part of the signal and are computed as follows:

$$d_{j,k} = \int_{-\infty}^{\infty} x(t)\psi_{j,k}(t)dt \tag{B.16}$$

B.3.3 Discrete Wavelet Transformation (DWT)

Discrete wavelet transform (DWT) is defined for a 1-D real discrete signal, $x[n]$, of length N , $n \in \mathbb{Z}$. Like an analog signal, a discrete signal can also be represented in terms of scaling and wavelets functions according to equation (B.12). For a discrete signal, scaling coefficients, and wavelet coefficients are computed as:

$$a_{j_0,k} = \sum_{n=0}^{N-1} x(n)\phi_{j_0,k}(n) \tag{B.17}$$

$$d_{j,k} = \sum_{n=0}^{N-1} x(n)\psi_{j,k}(n) \tag{B.18}$$

The equations (B.17) and (B.18) provide DWT of the discrete signal.

B.3.4 Fast Wavelet Transform (FWT)

The fast wavelet transform (FWT) is a computationally efficient implementation of the DWT using the dyadic filter tree algorithm [48] that exploits a fortunate relationship between the coefficients of the DWT at adjacent scales. FWT is also called Mallat's herringbone algorithm [138].

Let g and h be the scaling and wavelet filters respectively. The DWT coefficients of a discrete signal x using the FWT are computed by the following analysis equations:

$$a_{j+1}[k] = (a_j[k] * g[-k]) \downarrow 2 \tag{B.19}$$

$$d_{j+1}[k] = (a_j[k] * h[-k]) \downarrow 2 \tag{B.20}$$

where $a_0 = x$ and $\downarrow 2$ denotes down-sampling by a factor of two.

The reconstruction of x as x' from a_js and d_js is given by the following synthesis equation.

$$a'_j[k] = (a_{j+1}[k] \uparrow 2) * g[k] + (d_{j+1}[k] \uparrow 2) * h[k], \tag{B.21}$$

where $\uparrow 2$ denotes up-sampling by a factor of two. In this thesis, we have used Haar wavelet as mother wavelet, which is defined as follows:

$$\psi(t) = \begin{cases} 1 & 0 \leq t < 1/2 \\ -1 & 1/2 \leq t < 1 \\ 0 & \text{otherwise} \end{cases} \tag{B.22}$$

The scaling function $\phi(t)$ corresponds to haar wavelet is unit step function. For these mother wavelet and scaling function, the high pass finite impulse response (FIR) is $h[k] = [-1/\sqrt{2},\ 1/\sqrt{2}]$ and low pass FIR is $g[k] = [1/\sqrt{2},\ 1/\sqrt{2}]$.

B.3.5 Redundant Discrete Wavelet Transform (RDWT)

The Redundant discrete wavelet transform (RDWT) can be considered as an approximation to the continuous wavelet transform that removes the down-sampling operation from the traditional critically sampled DWT to produce an over-complete representation. The shift-variance characteristic of the DWT arises from its use of down-sampling, while the RDWT is shift invariant since the spatial sampling rate is fixed across scale. The filter tree approach in case of orthogonal wavelet can be implemented for the decomposition and reconstruction of the signal using the

following pseudo algorithm:

$$h_{j+1}[k] = h_j[k] \uparrow 2, \tag{B.23}$$

$$g_{j+1}[k] = g_j[k] \uparrow 2. \tag{B.24}$$

$$a_{j+1}[k] = (a_j[k] * g_{j+1}[-k]), \tag{B.25}$$

$$d_{j+1}[k] = (c_j[k] * h_{j+1}[-k]), \tag{B.26}$$

while RDWT synthesis is

$$a'_j[k] = \frac{1}{2}(a_{j+1}[k] * g_{j+1}[k] + d_{j+1}[k] * h_{j+1}[k]). \tag{B.27}$$

Equations (B.24) to (B.27) are known as the 'algorithme a trous' [48], since the filter-up-sampling procedure inserts holes (trous in French) between the filter taps.

B.3.6 2D-DWT

1-D DWT can easily be extended to two dimensional signal, like images. In two dimension, a two dimensional scaling function, $\phi(m, n)$, and three two-dimensional wavelets, $\psi^H(m, n)$, $\psi^V(m, n)$, $\psi^D(m, n)$, are required. The separable scaling function, and wavelets are defined as follows:

$$\phi(m, n) = \phi(m)\phi(n) \tag{B.28}$$

$$\psi^H(m, n) = \psi(m)\phi(n) \tag{B.29}$$

$$\psi^V(m, n) = \phi(m)\psi(n) \tag{B.30}$$

$$\psi^D(m, n) = \psi(m)\psi(n) \tag{B.31}$$

Here, ψ^H measures variations along columns (like horizontal edge), ψ^V measures variations along columns (like vertical edge), and ψ^D measures variations along diagonals (like diagonal edges).

2D-DWT analysis equations to decompose an image

$$
\begin{aligned}
a_{j+1}[k1,k2] &= (g[-k1] * (g[-k2] * c_j[k1,k2] \downarrow 2)) \downarrow 2 && \text{(B.32)}\\
d^H_{j+1}[k1,k2] &= (h[-k1] * (g[-k2] * c_j[k1,k2] \downarrow 2)) \downarrow 2 && \text{(B.33)}\\
d^V_{j+1}[k1,k2] &= (g[-k1] * (h[-k2] * c_j[k1,k2] \downarrow 2)) \downarrow 2 && \text{(B.34)}\\
d^D_{j+1}[k1,k2] &= (h[-k1] * (h[-k2] * c_j[k1,k2] \downarrow 2)) \downarrow 2 && \text{(B.35)}
\end{aligned}
$$

where, $a_0 = I$ is a gray scale image. Fig. B.1 shows the implementation result of 1-level 2D-DWT.

2D-DWT synthesis equation to reconstruct an image

$$
\begin{aligned}
a'_j[k1,k2] = \; & (g[k1] * ((g[k2] * (a_{j+1}[k1,k2] \uparrow 2)) \uparrow 2)) + \\
& (h[k1] * ((g[k2] * (d^H_{j+1}[k1,k2] \uparrow 2)) \uparrow 2)) + \\
& (g[k1] * ((h[k2] * (d^V_{j+1}[k1,k2] \uparrow 2)) \uparrow 2)) + \\
& (h[k1] * ((h[k2] * (d^D_{j+1}[k1,k2] \uparrow 2)) \uparrow 2))
\end{aligned}
\qquad \text{(B.36)}
$$

B.3.7 2D-RDWT

2D-RDWT analysis equations to decompose an image

$$
\begin{aligned}
a_{j+1}[k1,k2] &= g_{j+1}[-k1] * (g_{j+1}[-k2] * c_j[k1,k2]) && \text{(B.37)}\\
a^H_{j+1}[k1,k2] &= h_{j+1}[-k1] * (g_{j+1}[-k2] * c_j[k1,k2]) && \text{(B.38)}\\
a^V_{j+1}[k1,k2] &= g_{j+1}[-k1] * (h_{j+1}[-k2] * c_j[k1,k2]) && \text{(B.39)}\\
d^D_{j+1}[k1,k2] &= h_{j+1}[-k1] * (h_{j+1}[-k2] * c_j[k1,k2]) && \text{(B.40)}
\end{aligned}
$$

where, $a_0 = I$ is a gray scale image.

2D-RDWT synthesis equation to reconstruct image

$$a'_j[k1,k2] = \frac{1}{4}\begin{pmatrix} (g_{j+1}[k1] * (g_{j+1}[k2] * a_{j+1}[k1,k2]) + \\ (h_{j+1}[k1] * (g_{j+1}[k2] * d^H_{j+1}[k1,k2]) + \\ (g_{j+1}[k1] * (h_{j+1}[k2] * d^V_{j+1}[k1,k2]) + \\ (h_{j+1}[k1] * (h_{j+1}[k2] * d^D_{j+1}[k1,k2]) \end{pmatrix} \tag{B.41}$$

Fig. B.1 shows the implementation result of 1-level 2D-RDWT.

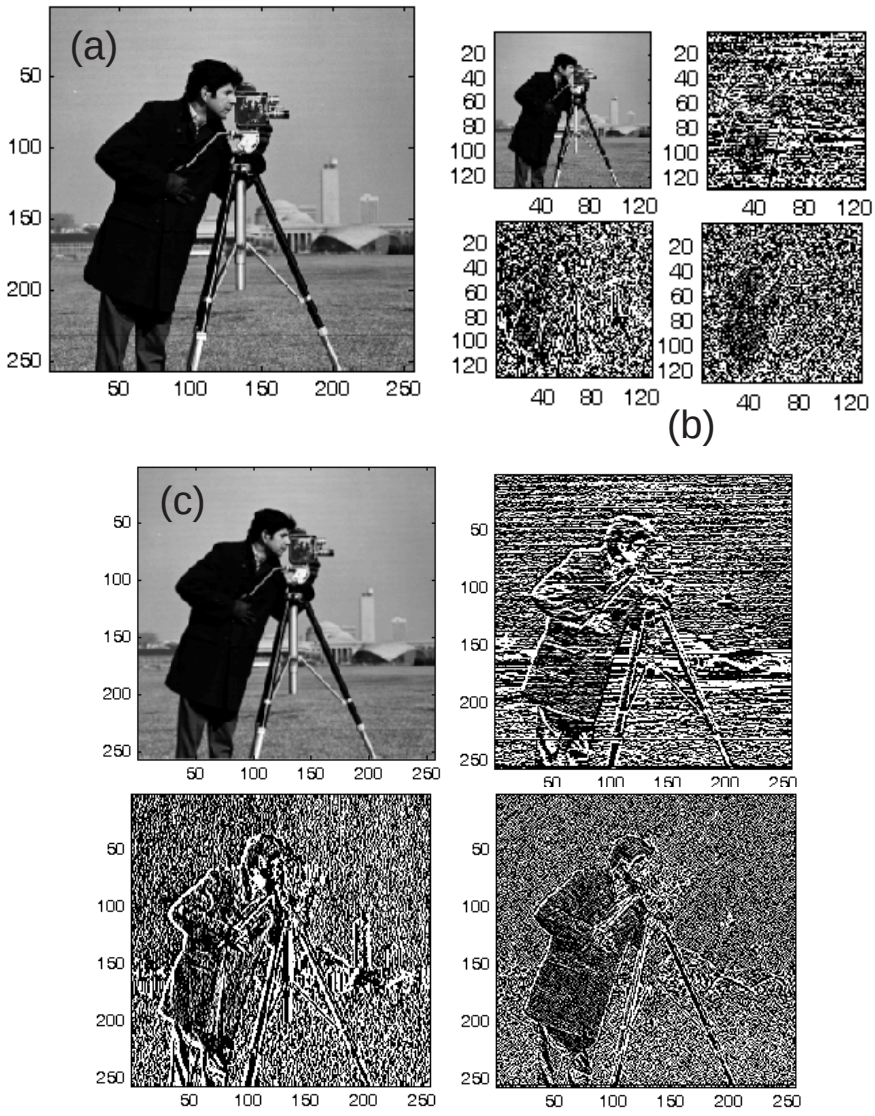


Figure B.1: Comparison between DWT and RDWT (a) original image (b) 1-level DWT decomposition of image (c) 1-level RDWT decomposition of image. Note that in DWT size of each sub band is half of original image, but in RDWT size of each sub band is equal to size of original image.

Bibliography

[1] International biometrics & identification association, immigration. http://www.ibia.org/biometrics/app/immigration, last accessed on July, 2014.

[2] Abdallah, H. A. and Hadhoud, M. M. Blind wavelet-based image watermarking. *International Journal of Signal Processing, Image Processing and Pattern Recognition*, **4**(1):15–28, 2011.

[3] Agarwal, H., Raman, B. and Atrey, P. K. Watermarking schemes to secure the face database and test images in a biometric system. In *IEEE International Conference on Signal and Image Processing Applications*, pages 128–133, Melaka, Malaysia, 2013.

[4] Agarwal, H., Raman, B. and Venkat, I. Blind reliable invisible watermarking method in wavelet domain for face image watermark. *Multimedia Tools and Applications*, pages 1–39, 2014. DOI: 10.1007/s11042-014-1934-1.

[5] Al-Otum, H. M. and Samara, N. A. A robust blind color image watermarking based on wavelet-tree bit host difference selection. *Signal Processing*, **90**(8):2498–2512, 2010.

[6] Alattar, O.M. and Alattar, A. M. A fast hierarchical watermark detector for real-time software or low-cost hardware implementation. In *IEEE International Conference on Image Processing*, volume 1, pages 973–976, Genova, Italy, 2005.

[7] Ali, M. and Ahn, C. W. An optimized watermarking technique based on self-adaptive DE in DWT–SVD transform domain. *Signal Processing*, **94**:545–556, 2014.

[8] Armbrust, M., Fox, A., Griffith, R., et al. A view of cloud computing. *Communications of the ACM*, **53**(4):50–58, 2010.

[9] Audícana, M. G., Saleta, J. L., Catalán, R. G. and García, R. Fusion of multispectral and panchromatic images using improved IHS and PCA mergers based on wavelet decomposition. *IEEE Transactions on Geoscience and Remote Sensing*, 42(6):1291–1299, 2004.

[10] Bao, P. and Ma, X. Image adaptive watermarking using wavelet domain singular value decomposition. *IEEE Transactions on Circuits and Systems for Video Technology*, **15**(1):96–102, 2005.

[11] Barni, M., Bartolini, F. and Piva, A. Improved wavelet-based watermarking through pixel-wise masking. *IEEE Transactions on Image Processing*, **10**(5):783–791, 2001.

[12] Barni, M., Bartolini, F., Cappellini, V. and Piva, A. A DCT-domain system for robust image watermarking. *Signal processing*, **66**(3):357–372, 1998.

[13] Bender, W., Butera, W., Gruhl, D., et al. Applications for data hiding. *IBM Systems Journal*, **39**(3.4):547–568, 2000.

[14] Bhatnagar, G. A new facet in robust digital watermarking framework. *International Journal of Electronics and Communications*, **66**(4):275–285, 2012.

[15] Bhatnagar, G. and Raman, B. A new robust reference watermarking scheme based on DWT-SVD. *Computer Standards & Interfaces*, **31**(5):1002–1013, 2009.

[16] Bhatnagar, G. and Raman, B. Robust reference-watermarking scheme using wavelet packet transform and bidiagonal-singular value decomposition. *International Journal of Image and Graphics*, **9**(3):449–477, 2009.

[17] Bhatnagar, G. and Raman, B. Distributed multiresolution discrete Fourier transform and its application to watermarking. *International Journal of Wavelets, Multiresolution and Information Processing*, **8**(2):225–241, 2010.

[18] Bhatnagar, G. and Raman, B. A new SVD based watermarking framework in fractional Fourier domain. In *International Conference on Contemporary Computing*, pages 107–118. Springer, Noida, India, 2010.

[19] Bhatnagar, G. and Raman, B. A new robust reference logo watermarking scheme. *Multimedia Tools and Applications*, **52**(2-3):621–640, 2011.

[20] Bhatnagar, G. and Wu, Q. J. Biometrics inspired watermarking based on a fractional dual tree complex wavelet transform. *Future Generation Computer Systems*, **29**(1):182–195, 2013.

[21] Bhatnagar, G., Raman, B. and Wu, Q. J. Robust watermarking using fractional wavelet packet transform. *IET image processing*, **6**(4):386–397, 2012.

[22] Bhatnagar, G., Wu, Q. J. and Raman, B. Biometric template security based on watermarking. In *Procedia Computer Science Elsevier*, volume **2**, pages 227–235, 2010.

[23] Bian, L. Retrieving urban objects using a wavelet transform approach. *Photogrammetric Engineering & Remote Sensing*, **69**(2):133–141, 2003.

[24] Bose, T., Meyer, F. G. and Chen, M. Q. *Digital signal and image processing*. Wiley New York, 2004.

[25] Bruce, N. D., Tsotsos, J. K. Saliency, attention, and visual search: An information theoretic approach. *Journal of vision*, **9**(3):1–24, 2009.

[26] Brunton, A. and Zhao, J. Real-time video watermarking on programmable graphics hardware. In *IEEE Canadian Conference on Electrical and Computer Engineering*, pages 1312–1315, SK, Canada, 2005.

[27] Cao, J. G., Fowler, J. E. and Younan, N. H. An image-adaptive watermark based on a redundant wavelet transform. In *IEEE International Conference on Image Processing*, volume 2, pages 277–280, Thessaloniki, Greece, 2001.

[28] Celik, M. U., Sharma, G., Tekalp, A. M. and Saber, E. Lossless generalized-LSB data embedding. *IEEE Transactions on Image Processing*, **14**(2):253–266, 2005.

[29] Chandler, D. M. Seven challenges in image quality assessment: past, present, and future research. *ISRN Signal Processing*, **2013**:1–53, 2013.

[30] Chandra, D. V. S. Digital image watermarking using singular value decomposition. In *IEEE 45th Midwest Symposium on Circuits and Systems*, volume 3, pages 264–267, Tulsa, Oklahoma, 2002.

[31] Chandran, R. and Yan, W. Q. A comprehensive survey of antiforensics for network security. *Managing Trust in Cyberspace*, pages 419–447, 2013.

[32] Chang, C. C., Tsai, P. and Lin, C. C. SVD-based digital image watermarking scheme. *Pattern Recognition Letters*, **26**(10):1577–1586, 2005.

[33] Cheddad, A., Condell, J., Curran, K. and McKevitt, P. Biometric inspired digital image steganography. In *15th Annual IEEE International Conference and Workshop on the Engineering of Computer Based Systems*, pages 159–168, Belfast, Northern Ireland, 2008.

[34] Chou, C. H. and Li, Y. C. A perceptually tuned subband image coder based on the measure of just-noticeable-distortion profile. *IEEE Transactions on Circuits and Systems for Video Technology*, **5**(6):467–476, 1995.

[35] Chung, Y., Moon, D., Moon, K. and Pan, S. Hiding biometric data for secure transmission. *Knowledge-Based Intelligent Information and Engineering Systems Lecture Notes in Computer Science*, **3683**:1049–1057, 2005.

[36] Combes, J. M., Grossmann, A. and Tchamitchian, P. Wavelets. time-frequency methods and phase space. In *Wavelets. Time-Frequency Methods and Phase Space*, volume 1, 1989.

[37] Coria, L. E., Pickering, M. R., Nasiopoulos, P. and Ward, R. K. A video watermarking scheme based on the dual-tree complex wavelet transform. *IEEE Transactions on Information Forensics and Security*, **3**(3):466–474, 2008.

[38] Cox, I. J. and Miller, M. L. Electronic watermarking: the first 50 years. In *IEEE Fourth Workshop on Multimedia Signal Processing*, pages 225–230, Cannes, 2001.

[39] Cox, I. J., Kilian, J., Leighton, F. T. and Shamoon, T. Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing*, **6**(12):1673–1687, 1997.

[40] Cox, I., Miller, M., Bloom, J. et al. *Digital Watermarking and Steganography*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, second edition, 2007.

[41] Craver, S. A., Memon, N. D., Yeo, B. L. and Yeung, M. M. Can invisible watermarks resolve rightful ownerships? In *SPIE Storage and Retrieval for Image and Video Databases V*, pages 310–321, San Jose, CA, 1997.

[42] Craver, S., Memon, N., Yeo, B. L. and Yeung, M. M. Resolving rightful ownerships with invisible watermarking techniques: Limitations, attacks, and implications. *IEEE Journal on Selected Areas in Communications*, **16**(4):573–586, 1998.

[43] Cui, D. Dual digital watermarking algorithm for image based on fractional Fourier transform. In *Second IEEE Pacific-Asia Conference on Web Mining and Web-based Application*, pages 51–54, Wuhan, China, 2009.

[44] Dawei, Z., Guanrong, C. and Wenbo, L. A chaos-based robust wavelet-domain watermarking algorithm. *Chaos, Solitons & Fractals*, **22**(1):47–54, 2004.

[45] Ding, S., Li, C. and Liu, Z. Protecting hidden transmission of biometrics using authentication watermarking. In *WASE International Conference on Information Engineering*, volume 2, pages 105–108, Hebei, China, 2010.

[46] Djurovic, I., Stankovic, S. and Pitas, I. Digital watermarking in the fractional Fourier transformation domain. *Journal of Network and Computer Applications*, **24**(2):167–173, 2001.

[47] Dugad, R., Ratakonda, K. and Ahuja, N. A new wavelet-based scheme for watermarking images. In *IEEE International Conference on Image Processing*, volume 2, pages 419–423, Chicago, Illinois, USA, 1998.

[48] Duhamel, P. Implementation of "split-radix" FFT algorithms for complex, real, and real-symmetric data. *IEEE Transactions on Acoustics, Speech and Signal Processing*, **34**(2):285–295, 1986.

[49] Eggers, J. J. and Girod, B. Blind watermarking applied to image authentication. In *IEEE International Conference on Acoustics, Speech, and Signal Processing*, volume 3, pages 1977–1980, Salt Lake City, UT, 2001.

[50] Eggers, J. J., Su, J., Girod, B. A blind watermarking scheme based on structured codebooks. In *IEE Seminar on Secure Images and Image Authentication (Ref. No. 2000/039)*, pages 1–21. IET, 2000.

[51] Eggers, J. J., Su, J. K. and Girod, B. Robustness of a blind image watermarking scheme. In *IEEE International Conference on Image Processing*, volume 3, pages 17–20, Vancouver, British Columbia, Canada, 2000.

[52] Eggers, J. J., Su, J. K. and Girod, B. Performance of a practical blind watermarking scheme. In *SPIE Security and Watermarking of Multimedia Contents III*, pages 594–605, San Jose, CA, 2001.

[53] Emmanuel, S., Kiang, H. C. and Das, A. A reversible watermarking scheme for JPEG-2000 compressed images. In *IEEE International Conference on Multimedia and Expo*, pages 69–72, Amsterdam, Netherlands, 2005.

[54] Fallahpour, M. and Megías, D. High capacity audio watermarking using the high frequency band of the wavelet domain. *Multimedia tools and Applications*, **52**(2-3):485–498, 2011.

[55] Faragallah, O. S. Efficient video watermarking based on singular value decomposition in the discrete wavelet transform domain. *AEU-International Journal of Electronics and Communications*, **67**(3):189–196, 2013.

[56] Fei, C., Kwong, R. and Kundur, D. Secure semi-fragile watermarking for image authentication. In *First IEEE International Workshop on Information Forensics and Security*, pages 141–145, London, UK, 2009.

[57] Feng, Z., Xiaomin, M. and Shouyi, Y. Multiple-chirp typed blind watermarking algorithm based on fractional Fourier transform. In *IEEE International Symposium on Intelligent Signal Processing and Communication Systems*, pages 141–144, Hong Kong, China, 2005.

[58] Fouad, M., Abdulmotaleb, E. S. and Petriu, E. Combining DWT and LSB watermarking to secure revocable iris templates. In *IEEE 10th International Conference on Information Sciences Signal Processing and their Applications*, pages 25–28, Kuala Lumpur, Malaysia, 2010.

[59] Fridrich, J. Visual hash for oblivious watermarking. In *SPIE Security and Watermarking of Multimedia Contents II*, volume 3971, pages 286–294, San Jose, CA, 2000.

[60] Ganic, E. and Eskicioglu, A. M. Robust DWT-SVD domain image watermarking: embedding data in all frequencies. In *ACM Workshop on Multimedia and Security*, pages 166–174, Magdeburg, Germany, 2004.

[61] Ganic, E. and Eskicioglu, A. M. Robust embedding of visual watermarks using discrete wavelet transform and singular value decomposition. *Journal of Electronic Imaging*, **14**(4):043004, 2005.

[62] Ghouti, L., Bouridane, A., Ibrahim, M. K. and Boussakta, S. Digital image watermarking using balanced multiwavelets. *IEEE Transactions on Signal Processing*, **54**(4):1519–1536, 2006.

[63] Gonde, A.B., Maheshwari, R. P. and Raman, B. Complex wavelet transform with vocabulary tree for content based image retrieval. In *ACM Seventh Indian Conference on Computer Vision, Graphics and Image Processing*, pages 359–366, Chennai, India, 2010.

[64] Gonzalez, R.C. and Woods, R. E. *Digital Image Processing*. Prentice Hall, 2008.

[65] Goupillaud, P., Grossmann, A. and Morlet, J. Cycle-octave and related transforms in seismic signal analysis. *Geoexploration*, **23**(1):85–102, 1984.

[66] Gunsel, B., Uludag, U. and Tekalp, A.M. Robust watermarking of fingerprint images. *Pattern Recognition*, **35**(12):2739–2747, 2002.

[67] Harel, J., Koch, C. and Perona, Pietro. Graph-based visual saliency. *Advances in neural information processing systems*, **19**:545–552, 2007.

[68] Hartung, F. H., Su, J. K. and Girod, B. Spread spectrum watermarking: Malicious attacks and counterattacks. In *SPIE Security and Watermarking of Multimedia Contents*, volume 3657, pages 147–158, San Jose, CA, 1999.

[69] Hassanien, A. E. Hiding iris data for authentication of digital images using wavelet theory. *Pattern Recognition and Image Analysis*, **16**(4):637–643, 2006.

[70] Hernández, J. R., Amado, M. and Pérez-González, F. DCT-domain watermarking techniques for still images: Detector performance analysis and a new structure. *IEEE Transactions on Image Processing*, **9**(1):55–68, 2000.

[71] Holliman, M. and Memon, N. Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes. *IEEE Transactions on Image Processing*, **9**(3):432–441, 2000.

[72] Hong, I., Kim, I. and Han, S. A blind watermarking technique using wavelet transform. In *IEEE International Symposium on Industrial Electronics*, volume 3, pages 1946–1950, Pusan, Korea, 2001.

[73] Hou, X. and Zhang, L. Saliency detection: A spectral residual approach. In *IEEE Conference on Computer Vision and Pattern Recognition*, pages 1–8, Minneapolis, MN, 2007.

[74] Hsieh, M. S., Tseng, D. C. and Huang, Y. H. Hiding digital watermarks using multiresolution wavelet transform. *IEEE Transactions on Industrial Electronics*, **48**(5):875–882, 2001.

[75] Hsu, C. T. and Wu, J. L. Energy compaction capability of DCT and DHT with CT image constraints. In *IEEE 13th International Conference on Digital Signal Processing*, volume 1, pages 345–348, Santorini, 1997.

[76] Hsu, C. T. and Wu, J. L. Multiresolution watermarking for digital images. *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, **45**(8):1097–1101, 1998.

[77] Hu, Y. and Jeon, B. Reversible visible watermarking and lossless recovery of original images. *IEEE Transactions on Circuits and Systems for Video Technology*, **16**(11):1423–1429, 2006.

[78] Hu, Y. and Kwong, S. Wavelet domain adaptive visible watermarking. *Electronics Letters*, **37**(20):1219–1220, 2001.

[79] Hu, Y., Kwong, S. and Huang, J. Using invisible watermarks to protect visibly watermarked images. In *IEEE International Symposium on Circuits and Systems*, volume 5, pages 584–587, Vancouver, Canada, 2004.

[80] Huang, B. B. and Tang, S. X. A contrast-sensitive visible watermarking scheme. *IEEE MultiMedia*, **13**(2):60–66, 2006.

[81] Hwang, M. S. and Chang, C. C. and Hwang, K. F. A watermarking technique based on one-way hash functions. *IEEE Transactions on Consumer Electronics*, **45**(2):286–294, 1999.

[82] Irany, B. M., Guo, X. C. and Hatzinakos, D. A high capacity reversible multiple watermarking scheme for medical images. In *IEEE 17th International Conference on Digital Signal Processing*, pages 1–6, Corfu, Greece, 2011.

[83] Itti, L., Koch, C., Niebur, E., et al. A model of saliency-based visual attention for rapid scene analysis. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, **20**(11):1254–1259, 1998.

[84] Jain, A. K. and Nandakumar, K. Biometric authentication: System security and user privacy. *IEEE Computer*, **45**(11):87–92, 2012.

[85] Jain, A. K. and Uludag, U. Hiding biometric data. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, **25**(11):1494–1498, 2003.

[86] Jain, A. K., Bolle R. and S. Pankanti. *Biometrics: personal identification in networked society*. Springer, 1999.

[87] Jain, A. K., Ross, A. and Prabhakar, S. An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, **14**(1):4–20, 2004.

[88] Jain, V. and Mukherjee, A. The indian face database, 2002. http://vis-www.cs.umass.edu/ vidit/IndianFaceDatabase/ (last accessed on July, 2014).

[89] Jha, R. K., Biswas, P. K. and Chatterji, B. N. Logo extraction using combined discrete wavelet transform and dynamic stochastic resonance. *International Journal of Image and Graphics*, **13**(1):1–21, 2013.

[90] Jha, R. K., Biswas, P. K. and Shrivastava, S. Logo extraction using dynamic stochastic resonance. *Signal, Image and Video Processing*, **7**(1):119–128, 2013.

[91] Joshi, A. M., Darji, A. and Mishra, V. Design and implementation of real-time image watermarking. In *IEEE International Conference on Signal Processing, Communications and Computing*, pages 1–5, Xi'an, 2011.

[92] Kamble, S., Maheshkar, V., Agarwal, S. and Shrivastava, V. Robust multiple watermarking using entropy based spread spectrum. In *Contemporary Computing*, pages 497–507. 2010.

[93] Kamble, S., Maheshkar, V., Agarwal, S. and Srivastava, V. K. DWT-based multiple watermarking for privacy and security of digital images in E-commerce. In *IEEE International Conference on Multimedia, Signal Processing and Communication Technologies*, pages 224–227, Aligarh, India, 2011.

[94] Kamble, S., Maheshkar, V., Agarwal, S. and Srivastava, V. K. DWT-SVD based robust image watermarking using Arnold map. *International Journal of Information Technology and Knowledge Management*, **5**(1):101–105, 2012.

[95] Kankanhalli, M. S., Rajmohan and Ramakrishnan, K. R. Content based watermarking of images. In *sixth ACM international conference on Multimedia*, pages 61–70, Bristol, UK, 1998.

[96] Kankanhalli, M. S., Rajmohan and Ramakrishnan, K. R. Adaptive visible watermarking of images. In *IEEE International Conference on Multimedia Computing and Systems*, volume 1, pages 568–573, Florence, 1999.

[97] Keyvanpour, M. R. and Merrikh-Bayat, F. Robust dynamic block-based image watermarking in DWT domain. *Procedia Computer Science*, **3**:238–242, 2011.

[98] Khan, M. K., Xie, L. and Zhang, J. Robust hiding of fingerprint-biometric data into audio signals. *Advances in Biometrics Lecture Notes in Computer Science, Springer*, **4642**:702–712, 2007.

[99] Khan, M. K., Zhang, J. and Tian, L. Chaotic secure content-based hidden transmission of biometric templates. *Chaos, Solitons &Fractals*, **32**(5):1749–1759, 2007.

[100] Khana, A., Malika S. A., Alib A., et al. Intelligent reversible watermarking and authentication: Hiding depth map information for 3D cameras. *Information Sciences*, **216**:155–175, 2012.

[101] Kim, B. S., Choi, J. G., Park, C. H. et al. Robust digital image watermarking method against geometrical attacks. *Real-Time Imaging*, **9**(2):139–149, 2003.

[102] Kim, J. R. and Moon, Y. S. A robust wavelet-based digital watermarking using level-adaptive thresholding. In *International Conference on Image Processing*, volume 2, pages 226–230, Kobe, Japan, 1999.

[103] Kim, T., Chung, Y., Jung, S. and Moon, D. Secure remote fingerprint verification using dual watermarks. *Digital Rights Management Technologies, Issues, Challenges and Systems Lecture Notes in Computer Science, Springer*, **3919**:217–227, 2006.

[104] Kim, W. G. and Lee, H. K. Multimodal biometric image watermarking using two-stage integrity verification. *Signal Processing*, **89**(12):2385–2399, December 2009.

[105] Kokare, M., Biswas, P. K. and Chatterji, B. N. Texture image retrieval using new rotated complex wavelet filters. *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, **35**(6):1168–1178, 2005.

[106] Kokare, M., Biswas, P. K. and Chatterji, B. N. Rotation-invariant texture image retrieval using rotated complex wavelet filters. *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, **36**(6):1273–1282, 2006.

[107] Korus, P., Białas, J. and Dziech, A. A new approach to high-capacity annotation watermarking based on digital fountain codes. *Multimedia Tools and Applications*, **68**(1):59–77, 2014.

[108] Kougianos, E., Mohanty, S. P. and Mahapatra, R. N. Hardware assisted watermarking for multimedia. *Computers & Electrical Engineering*, **35**(2):339–358, 2009.

[109] Kovesi, P. Image features from phase congruency. *Videre: Journal of computer vision research*, **1**(3):1–26, 1999.

[110] Kronland-Martinet, R., Morlet, J. and Grossmann, A. Analysis of sound patterns through wavelet transforms. *International Journal of Pattern Recognition and Artificial Intelligence*, **1**(02):273–302, 1987.

[111] Kumar, S., Kumar, S., Raman, B. and Sukavanam, N. Image disparity estimation based on fractional dual-tree complex wavelet transform: A multi-scale approach. *International Journal of Wavelets, Multiresolution and Information Processing*, **11**(1):1350004–1–1350004–21, 2013.

[112] Kundur, D. *Multiresolution Digital Watermarking: Algorithms and Implications for Multimedia Signals*. PhD thesis, Graduate Department of Electrical and Computer Engineering University of Toronto, 1999.

[113] Kundur, D. and Hatzinakos, D. Digital watermarking for telltale tamper proofing and authentication. *Proceedings of the IEEE*, **87**(7):1167–1180, 1999.

[114] Kundur, D. and Hatzinakos, D. Toward robust logo watermarking using multiresolution image fusion principles. *IEEE Transactions on Multimedia*, **6**(1):185–198, 2004.

[115] Kundur, D. and Karthik, K. Video fingerprinting and encryption principles for digital rights management. *Proceedings of the IEEE*, **92**(6):918–932, 2004.

[116] Lai, C. C. A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm. *Digital Signal Processing*, **21**(4):522–527, 2011.

[117] Lai, C. C. and Tsai, C. C. Digital image watermarking using discrete wavelet transform and singular value decomposition. *IEEE Transactions on Instrumentation and Measurement*, **59**(11):3060–3063, 2010.

[118] Li, C. L., Wang, Y. H. and Liu, L N. A biometric templates secure transmission method based on bi-layer watermarking and PKI. In *IEEE International Conference on Multimedia Information Networking and Security*, volume 2, pages 95–98, Hubei, 2009.

[119] Li, C. T., Yang, F. M. and Lee, C. S. Oblivious fragile watermarking scheme for image authentication. In *IEEE International Conference on Acoustics, Speech, and Signal Processing*, volume 4, pages IV–3445 – IV–3448, Orlando, FL, USA, 2002.

[120] Li, J., Levine, M. D. and An, X. et al. Visual saliency based on scale-space analysis in the frequency domain. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, **35**(4):996–1010, 2013.

[121] Li, Q., Yuan, C. and Zhong, Y. Z. Adaptive DWT-SVD domain image watermarking using human visual model. In *IEEE 9th International Conference on Advanced Communication Technology*, volume 3, pages 1947–1951, Gangwon-Do, 2007.

[122] Lin, C. Y., Wu, M., Bloom, J. A. et al. Rotation, scale, and translation resilient watermarking for images. *IEEE Transactions on Image Processing*, **10**(5):767–782, 2001.

[123] Lin, T. C. and Lin, C. M. Wavelet-based copyright-protection scheme for digital images based on local features. *Information Sciences*, **179**(19):3349–3358, 2009.

[124] Lin, W. H., Horng, S. J., Kao, T. W. et al. An efficient watermarking method based on significant difference of wavelet coefficient quantization. *IEEE Transactions on Multimedia*, **10**(5):746–757, 2008.

[125] Lin, W. H., Horng, S. J., Kao, T. W. et al. Image copyright protection with forward error correction. *Expert systems with applications*, **36**(9):11888–11894, 2009.

[126] Lin, W. H., Wang, Y. R. and Horng, S. J. A wavelet-tree-based watermarking method using distance vector of binary cluster. *Expert Systems with Applications*, **36**(6):9869–9878, 2009.

[127] Lin, W. H., Wang, Y. R., Horng, S. J. et al. A blind watermarking method using maximum wavelet coefficient quantization. *Expert Systems with Applications*, **36**(9):11509–11516, 2009.

[128] Ling, H., Zou, F., Yan, W. Q. et al. Efficient image copy detection using multi-scale fingerprints. *IEEE Multimedia*, **19**(1):60–69, 2012.

[129] Linnartz, J. P., Kalker, T. and Depovere, G. Modelling the false alarm and missed detection rate for electronic watermarks. In *Information Hiding*, pages 329–343, 1998.

[130] Liu, J. L., Lou, D. C., Chang, M. C. and Tso, H. K. A robust watermarking scheme using self-reference image. *Computer Standards & Interfaces*, **28**(3):356–367, 2006.

[131] Liu, R. and Tan, T. An SVD-based watermarking scheme for protecting rightful ownership. *IEEE Transactions on Multimedia*, **4**(1):121–128, 2002.

[132] Liu, T. Y. and Tsai, W. H. Generic lossless visible watermarkinga new approach. *IEEE Transactions on Image Processing*, **19**(5):1224–1235, 2010.

[133] Loo, P. and Kingsbury, N. G. Digital watermarking using complex wavelets. In *IEEE International Conference Image Processing*, volume 3, pages 29–32, Vancouver, BC, 2000.

[134] Lumini, A. and Maio, D. Adaptive positioning of a visible watermark in a digital image. In *IEEE International Conference on Multimedia and Expo*, volume 2, pages 967–970, Taipei, 2004.

[135] Ma, B., Wang, Y., Li, C. et al. Secure multimodal biometric authentication with wavelet quantization based fingerprint watermarking. *Multimedia Tools and Applications*, pages 1–30, 2013. DOI: 10.1007/s11042-013-1372-5.

[136] Magarey, J. and Kingsbury, N.G. Motion estimation using a complex-valued wavelet transform. *IEEE Transactions on Signal Processing*, **46**(4):1069–1084, 1998.

[137] Maity, S. P. and Kundu, M. K. A blind CDMA image watermarking scheme in wavelet domain. In *IEEE International Conference on Image Processing*, volume 4, pages 2633–2636, 2004.

[138] Mallat, S. G. A theory for multiresolution signal decomposition: The wavelet representation. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, **2**(7):674–693, 1989.

[139] Mathai, N. J., Kundur, D., Sheikholeslami, A. Hardware implementation perspectives of digital video watermarking algorithms. *IEEE Transactions on Signal Processing*, **51**(4):925–938, 2003.

[140] Memon, N. and Wong, P. W. Protecting digital media content. *Communications of the ACM*, **41**(7):35–43, 1998.

[141] Memon, N. and Wong, P. W. A buyer-seller watermarking protocol. *IEEE Transactions on Image Processing*, **10**(4):643–649, 2001.

[142] Miller, M., Kingsbury N., Hobbs R. Seismic imaging using complex wavelets. In *IEEE International Conference on Acoustic, Speech, Signal Processing*, volume 2, pages 557–560, Philadelphia, Pennsylvania, USA, 2005.

[143] Miller, M. L. and Bloom, J. A. Computing the probability of false watermark detection. In *Information Hiding*, pages 146–158, 2000.

[144] Mintzer, F., Braudaway, G. W. and Yeung, M. M. Effective and ineffective digital watermarks. In *IEEE International Conference on Image Processing*, volume 3, pages 9–12, Santa Barbara, CA, 1997.

[145] Mohammad, A. A., Alhaj, A. and Shaltaf, S. An improved SVD-based watermarking scheme for protecting rightful ownership. *Signal Processing*, **88**(9):2158–2180, 2008.

[146] Mohanty, S. P. A secure digital camera architecture for integrated real-time digital rights management. *Journal of Systems Architecture*, **55**(10):468–480, 2009.

[147] Mohanty, S. P., Adamo, O. B. and Kougianos, E. VLSI architecture of an invisible watermarking unit for a biometric-based security system in a digital camera. In *IEEE International Conference on Consumer Electronics, Digest of Technical Papers.*, pages 1–2, Las Vegas, NV, 2007.

[148] Mohanty, S. P. and Bhargava, B. K. Invisible watermarking based on creation and robust insertion-extraction of image adaptive watermarks. *ACM Transactions on Multimedia Computing, Communications, and Applications*, **5**(2):12, 2008.

[149] Mohanty, S. P., Pati, N. and Kougianos, E. A watermarking co-processor for new generation graphics processing units. In *IEEE International Conference on Consumer Electronics, Digest of Technical Papers*, pages 1–2, Las Vegas, NV, 2007.

[150] Mohanty, S. P., Ramakrishnan, K. R. and Kankanhalli, M. S. A dual watermarking technique for images. In *Seventh ACM international conference on Multimedia (Part 2)*, pages 49–51, Orlando, FL, USA, 1999.

[151] Mohanty, S. P., Ramakrishnan, K. R. and Kankanhalli, M. S. A DCT domain visible watermarking technique for images. In *IEEE International Conference on Multimedia and Expo*, volume 2, pages 1029–1032, New York, NY, 2000.

[152] Mohanty, S. P., Sheth, R., Pinto, A. and Chandy, M. Cryptmark: a novel secure invisible watermarking technique for color images. In *IEEE International Symposium on Consumer Electronics*, pages 1–6, Irving, TX, 2007.

[153] Mooney, A., Keating, J. G. and Pitas, I. A comparative study of chaotic and white noise signals in digital watermarking. *Chaos, Solitons & Fractals*, **35**(5):913–921, 2008.

[154] Morimoto, N. Digital watermarking technology with practical applications. *Informing Science Special Issue on Multimedia Informing Technologies-Part 1*, **2**(4):107–111, 1999.

[155] Naor, M. and Shamir, A. Visual cryptography. In *Springer, Advances in cryptology – EUROCRYPT'94, Workshop on the Theory and Application of Cryptographic Techniques*, pages 1–12, Perugia, Italy, 1994.

[156] Nikolaidis, N. and Pitas, I. Robust image watermarking in the spatial domain. *Signal processing*, **66**(3):385–403, 1998.

[157] Noore, A., Singh, R., Vatsa, M. and Houck, M. M. Enhancing security of fingerprints through contextual biometric watermarking. *Forensic Science International*, **169**(2):188–194, 2007.

[158] Unique Identification Authority of India Planning Commission government of India. Aadhaar. http://uidai.gov.in/, last accessed on July, 2014.

[159] Pandey, P., Kumar, S. and Singh, S. K. Rightful ownership through image adaptive DWT-SVD watermarking algorithm and perceptual tweaking. *Multimedia Tools and Applications*, pages 1–26, 2013. DOI: 10.1007/s11042-013-1375-2.

[160] Park, K. R., Jeong, D. S., Kang, B. J. and Lee, E. C. A study on iris feature watermarking on face data. *Adaptive and Natural Computing Algorithms Lecture Notes in Computer Science, Springer*, **4432**:415–423, 2007.

[161] Parker, K. M. and Fowler, J. E. Redundant-wavelet watermarking with pixel-wise masking. In *IEEE International Conference on Image Processing*, pages I685 –I688, Genova, Italy, 2005.

[162] Patra, J. C., Karthik, A. and Bornand, C. A novel CRT-based watermarking technique for authentication of multimedia contents. *Digital Signal Processing*, **20**(2):442–453, 2010.

[163] Patra, J. C., Phua, J. E. and Bornand, C. A novel DCT domain CRT-based watermarking scheme for image authentication surviving JPEG compression. *Digital Signal Processing*, **20**(6):1597–1611, 2010.

[164] Peng, H., Wang, J. and Wang, W. Image watermarking method in multiwavelet domain based on support vector machines. *Journal of Systems and Software*, **83**(8):1470–1477, 2010.

[165] Pereira, S., Ruanaidh, J. J., Deguillaume, F. et al. Template based recovery of Fourier-based watermarks using log-polar and log-log maps. In *IEEE International Conference on Multimedia Computing and Systems*, volume 1, pages 870–874, Florence, 1999.

[166] Pereira, S., Voloshynovskiy, S. and Pun, T. Effective channel coding for DCT watermarks. In *IEEE International Conference on Image Processing*, volume 3, pages 671–673, Vancouver, BC, Canada, 2000.

[167] Petitcolas, F. A. Watermarking schemes evaluation. *IEEE Signal Processing Magazine*, **17**(5):58–64, 2000.

[168] Pittner, S. and Kamarthi, S. V. Feature extraction from wavelet coefficients for pattern recognition tasks. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, **21**(1):83–88, 1999.

[169] Podilchuk, C. I. and Delp, E. J. Digital watermarking: algorithms and applications. *IEEE Signal Processing Magazine*, **18**(4):33–46, 2001.

[170] Podilchuk, C. I. and Zeng, W. Image-adaptive watermarking using visual models. *IEEE Journal on Selected Areas in Communications*, **16**(4):525–539, 1998.

[171] Prabhakar, S. and Pankanti, S. and Jain, A. K. Biometric recognition: Security and privacy concerns. *IEEE Security & Privacy*, **1**(2):33–42, 2003.

[172] Pu, R. and Gong, P. Wavelet transform applied to EO-1 hyperspectral data for forest LAI and crown closure mapping. *Remote Sensing of Environment*, **91**(2):212–224, 2004.

[173] Qi, H., Zheng, D. and Zhao, J. Human visual system based adaptive digital image watermarking. *Signal Processing*, **88**(1):174–188, 2008.

[174] Qi, M., Lu, Y., Du, N. et al. A novel image hiding approach based on correlation analysis for secure multimodal biometrics. *Journal of Network and Computer Applications*, **33**(3):247–257, 2010.

[175] Ramkumar, M., Akansu, A. N., Alatan, A. A. A robust data hiding scheme for images using DFT. In *International Conference on Image Processing*, volume 2, pages 211–215, Kobe, Japan, 1999.

[176] Ramkumar, M. and Akansu, A. N. Information theortic bounds for data hiding in compressed images. In *IEEE Second Workshop on Multimedia Signal Processing*, pages 267–272, California, USA, 1998.

[177] Rangaswamy, D. M. A. A novel invisible and blind watermarking scheme for copyright protection of digital images. *International Journal of Computer Science and Network Security*, **9**(4):71–78, 2009.

[178] Rani, A., Raman, B., Kumar, S. A robust watermarking scheme exploiting balanced neural tree for rightful ownership protection. *Multimedia Tools and Applications*, pages 1–24, 2013. DOI: 10.1007/s11042-013-1528-33.

[179] Ratha, N. K., Connell, J. H. and Bolle, R. M. Secure data hiding in wavelet compressed fingerprint images. In *ACM workshops on Multimedia*, pages 127–130, Los Angeles, CA, USA, 2000.

[180] Ratha, N. K., Connell, J. H. and Bolle, R. M. An analysis of minutiae matching strength. In *Third International Conference Audio and Video Based Biometric Person Authentication*, pages 223–228, Halmstad, Sweden, 2001.

[181] Rawat, S. *Digital Watermarking for Copyright Protection and Authentication*. PhD thesis, Department of Mathematics, Indian Institute of Technology Roorkee, 2011.

[182] Rawat, S. and Raman, B. A chaotic system based fragile watermarking scheme for image tamper detection. *AEU-International Journal of Electronics and Communications*, **65**(10):840–847, 2011.

[183] Rawat, S. and Raman, B. A blind watermarking algorithm based on fractional Fourier transform and visual cryptography. *Signal Processing*, **92**(6):1480–1491, 2012.

[184] Reddy, A. A. and Chatterji, B. N. A new wavelet based logo-watermarking scheme. *Pattern Recognition Letters*, **26**(7):1019–1027, 2005.

[185] Rioul, O. and Duhamel, P. Fast algorithms for discrete and continuous wavelet transforms. *IEEE Transactions on Information Theory*, **38**(2):569–586, 1992.

[186] Romberg, J., Choi, H., Baraniuk, R. and Kingsbury, N. Multiscale classification using complex wavelets and hidden markov tree models. In *IEEE International Conference on Image Processing*, volume 2, pages 371–374, Vancouver, BC, Canada, 2000.

[187] Roy, S. D., Li, X., Shoshan, Y. et al. Hardware implementation of a digital watermarking system for video authentication. *IEEE Transactions on Circuits and Systems for Video Technology*, **22**(2):289–301, 2013.

[188] Run, R. S., Horng, S. J., Lin, W. H. et al. An efficient wavelet-tree-based watermarking method. *Expert Systems with Applications*, **38**(12):14357–14366, 2011.

[189] Schyndel, R. G. V., Tirkel, A. Z. and Osborne, C. F. A digital watermark. In *IEEE International Conference Image Processing*, volume 2, pages 86–90, Austin, Texas, USA, 1994.

[190] Selesnick, I. 2-D dual-tree wavelet transform. http://eeweb.poly.edu/iselesni/WaveletSoftware/dt2D.html, last accessed on July, 2014.

[191] Selesnick, I. W., Baraniuk, R. G. and Kingsbury, N. G. The dual-tree complex wavelet transform. *IEEE Signal Procesing Magazine*, pages 123–151, 2005.

[192] Shaffrey, C. W., Kingsbury, N. G. and Jermyn, I. H. Unsupervised image segmentation via markov trees and complex wavelets. In *IEEE Internationl Conference on Image Processing*, volume 3, pages 801–804, Rochester, New York, USA, 2002.

[193] Sharma, J. B., Sharma, K. K. and Sahula, V. Digital image dual watermarking using self-fractional Fourier functions, bivariate empirical mode decomposition and error correcting code. *Journal of Optics*, **42**(3):214–227, 2013.

[194] Sharma, J. B., Sharma, K. K. and Sahula, V. Hybrid image fusion scheme using self-fractional Fourier functions and multivariate empirical mode decomposition. *Signal Processing*, **100**:146–159, 2014.

[195] Sharma, K. K. and Fageria, D. K. Watermarking based on image decomposition using self-fractional Fourier functions. *Journal of Optics*, **40**(2):45–50, 2011.

[196] Shejul, A. A. and Kulkarni, U. L. A DWT based approach for steganography using biometrics. In *IEEE International Conference on Data Storage and Data Engineering*, pages 39–43, Bangalore, 2010.

[197] Shia, X. and Xiaoa D. A reversible watermarking authentication scheme for wireless sensor networks. *Information Sciences*, **240**:173–183, 2013.

[198] Shih, F. Y. and Wu, Y. T. Robust watermarking and compression for medical images based on genetic algorithms. *Information Sciences*, **175**(3):200–216, 2005.

[199] Shoshan, Y., Fish, A., Jullien, G. A. and Yadid-Pecht, O. Hardware implementation of a DCT watermark for CMOS image sensors. In *IEEE 15th International Conference on Electronics, Circuits and Systems*, pages 368–371, St. Julien's, 2008.

[200] Singh, P. and Agarwal, S. A visual cryptography based watermarking scheme incorporating the concepts of homogeneity analysis and singular value decomposition. *International Journal of Computer Applications*, **80**(16):1–9, 2013.

[201] Singh, S. K. and Kumar, S. Singular value decomposition based sub-band decomposition and multi-resolution (SVD-SBD-MRR) representation of digital colour images. *Pertanika Journal of Science & Technology*, **19**(2):229–235, 2011.

[202] Singh, S. K., Kumar, S., Srivastava, M., et al. Wavelet based robust digital watermarking technique using reverse additive algorithm (RAA). In *IEEE Third UKSim European Symposium on Computer Modeling and Simulation*, pages 241–244, Athens, Greece, 2009.

[203] Skodras, A., Christopoulos, C. and Ebrahimi, T. The JPEG 2000 still image compression standard. *IEEE Signal Procesing Magazine*, pages 36–58, 2001.

[204] Soheili, M. R. Redundant watermarking using wavelet packets. In *IEEE/ACS International Conference on Computer Systems and Applications*, pages 591–598, Doha, 2008.

[205] Su, Q., Niu, Y., Liu, X. and Zhu, Y. A blind dual color images watermarking based on iwt and state coding. *Optics Communications*, **285**(7):1717–1724, 2012.

[206] Subramanyam, A. V., Emmanuel, S. and Kankanhalli, M. S. Robust watermarking of compressed and encrypted JPEG 2000 images. *IEEE Transactions on Multimedia*, **14**(3):703–716, 2012.

[207] Suhail, M.A., Obaidat, M. S., Ipson, S. S. and Sadoun, B. A comparative study of digital watermarking in JPEG and JPEG 2000 environments. *Information Sciences*, **15**:93–105, 2003.

[208] Suresh, N. and Karthik, K. Secure fingerprint embedding based on modified GDFT based parametric transform. In *IEEE International Conference on Image Information Processing*, pages 1–6, Himachal Pradesh, India, 2011.

[209] Talwai, A., Sengupta, D., Karthik, K. A transparent encryption scheme for watermarked biometric and medical images. *International Journal of Computer & Electrical Engineering*, **4**(3):278–282, 2012.

[210] Tang, C. W. and Hang, H. M. A feature-based robust digital image watermarking scheme. *IEEE Transactions on Signal Processing*, **51**(4):950–959, 2003.

[211] Tay, R. and Havlicek, J. P. Image watermarking using wavelets. In *IEEE 45th Midwest Symposium on Circuits and Systems*, volume 3, pages 258–261, Tulsa, Oklahoma, 2002.

[212] Tefas, A., Nikolaidis, A., Nikolaidis, N., et al. Statistical analysis of markov chaotic sequences for watermarking applications. In *IEEE International Symposium on Circuits and Systems*, number 2, pages 57–60, Sydney, NSW, 2001.

[213] Terzija, N. and Geisselhardt, W. Digital image watermarking using complex wavelet transform. In *ACM Workshop on Multimedia and Security*, pages 193–198, Magdeburg, Germany, 2004.

[214] Thodi, D. M. and Rodríguez, J. J. Expansion embedding techniques for reversible watermarking. *IEEE Transactions on Image Processing*, **16**(3):721–730, 2007.

[215] Thomas, T., Emmanuel, S., Subramanyam, A. V. and Kankanhalli, M. S. Joint watermarking scheme for multiparty multilevel DRM architecture. *IEEE Transactions on Information Forensics and Security*, **4**(4):758–767, 2009.

[216] Tian, J., Bloom, J. A. and Baum, P. G. False positive analysis of correlation ratio watermark detection measure. In *IEEE International Conference on Multimedia and Expo*, pages 619–622, Beijing, China, 2007.

[217] Topkara, M., Kamra, A., Atallah, M. J. and Nita-Rotaru, C. Viwid: Visible watermarking based defense against phishing. In *Digital Watermarking, Springer*, pages 470–483. 2005.

[218] Tripathi, S., Jain, R. C. and Gayatri, V. Novel DCT and DWT based watermarking techniques for digital images. In *18th IEEE International Conference on Pattern Recognition*, volume 4, pages 358–361, Hong Kong, 2006.

[219] Tsai, H. M. and Chang, L. W. A high secure reversible visible watermarking scheme. In *IEEE International Conference on Multimedia and Expo*, pages 2106–2109, Beijing, China, 2007.

[220] Turk, M. and Pentland, A. Eigenfaces for recognition. *Journal of Cognitive Neuroscience*, **3**(1):71–86, 1991.

[221] Vatsa, M., Singh, R. and Noore, A. Feature based RDWT watermarking for multimodal biometric system. *Image and Vision Computing*, **27**(3):293–304, 2009.

[222] Vatsa, M., Singh, R., Mitra, P. and Noore, A. Comparing robustness of watermarking algorithms on biometrics data. In *Workshop on Biometrics: Challenges Arising from Theory to Practice*, pages 5–8, Cambridge, UK, 2004.

[223] Voloshynovskiy, S., Pereira, S., Iquise, V. and Pun, T. Attack modelling: towards a second generation watermarking benchmark. *Signal processing*, **81**(6):1177–1214, 2001.

[224] Voloshynovskiy, S., Pereira, S., Pun, T., et al. Attacks on digital watermarks: classification, estimation based attacks, and benchmarks. *IEEE Communications Magazine*, **39**(8):118–126, 2001.

[225] Wallace, G. K. The JPEG still picture compression standard. *IEEE Transactions on Consumer Electronics*, **38**(1):18–34, 1992.

[226] Wang, C., Wang, Q., Ren, K. and Lou, W. Privacy-preserving public auditing for data storage security in cloud computing. In *IEEE INFOCOM*, pages 1–9, San Diego, CA, 2010.

[227] Wang, N. and Men, C. Reversible fragile watermarking for locating tampered blocks in 2D vector maps. *Multimedia Tools and Applications*, **67**(3):709–739, 2013.

[228] Wang, X. Y., Yang, Y. P. and Yang, H. Y. Invariant image watermarking using multi-scale Harris detector and wavelet moments. *Computers & electrical engineering*, **36**(1):31–44, 2010.

[229] Wang, Y., Doherty, J. F. and Van-Dyck, R. E. A wavelet-based watermarking algorithm for ownership verification of digital images. *IEEE Transactions on Image Processing*, **11**(2):77–88, 2002.

[230] Wang, Z. and Li, Q. Information content weighting for perceptual image quality assessment. *IEEE Transactions on Image Processing*, **20**(5):1185–1198, 2011.

[231] Wanga, X. Y., Wanga, C. P., Yanga, H. Y. and Niua, P. P. A robust blind color image watermarking in quaternion Fourier transform domain. *The Journal of Systems and Software*, **86**(2):255–277, 2013.

[232] Wei, Z. H., Qin, P. and Fu, Y. Q. Perceptual digital watermark of images using wavelet transform. *IEEE Transactions on Consumer Electronics*, **44**(4):1267–1272, 1998.

[233] Weir, J. and Yan, W. Q. A comprehensive study of visual cryptography. In *Transactions on data hiding and multimedia security V, Springer*, pages 70–105. 2010.

[234] Wolfgang, R. B., Podilchuk, C. I. and Delp, E. J. Perceptual watermarks for digital images and video. *Proceedings of the IEEE*, **87**(7):1108–1126, 1999.

[235] Wong, P. W. and Memon, N. Secret and public key image watermarking schemes for image authentication and ownership verification. *IEEE Transactions on Image Processing*, **10**(10):1593–1601, 2001.

[236] Wu, Y., Guan, X., Kankanhalli, M. S. and Huang, Z. Robust invisible watermarking of volume data using the 3D DCT. In *IEEE Computer Graphics International*, pages 359–362, Hong Kong, 2001.

[237] Xiao, J. and Wang, Y. False negative and positive models of dither modulation watermarking. In *IEEE Fourth International Conference on Image and Graphics*, pages 318–323, Sichuan, 2007.

[238] Yang, H. and Yin, J. A secure removable visible watermarking for btc compressed images. *Multimedia Tools and Applications*, pages 1–15, 2013. DOI 10.1007/s11042-013-1714-3.

[239] Yang, H., Jiang, X. and Kot, A. C. Embedding binary watermarks in dual-tree complex wavelets domain for access control of digital images. *Transactions on DHMS, Springer*, **6**:18–36, 2011.

[240] Yang, H. Y., Wang, X. Y. and Wang, C. P. A robust digital watermarking algorithm in undecimated discrete wavelet transform domain. *Computers & Electrical Engineering*, **39**(3):893–906, 2012.

[241] Yang, Y., Sun, X., Yang, H., et al. A contrast-sensitive reversible visible image watermarking technique. *IEEE Transactions on Circuits and Systems for Video Technology*, **19**(5):656–667, 2009.

[242] Ye, Z. and Lu, C. C. A complex wavelet domain markov model for image denoising. In *IEEE International Conference on Image Processing*, volume 3, pages 365–368, Barcelona, Catalonia, Spain, 2003.

[243] Yeung, M. M. and Mintzer, F. An invisible watermarking technique for image verification. In *IEEE International Conference on Image Processing*, volume 2, pages 680–683, Santa Barbara, California, USA,, 1997.

[244] Yeung, M. M., Mintzer, F. C., Braudaway, G. W. and Rao, A. R. Digital watermarking for high-quality imaging. In *IEEE First Workshop on Multimedia Signal Processing*, pages 357–362, Princeton, NJ, 1997.

[245] Yip, S. K., Au, O. C., Ho, C. W. and Wong, H. M. Lossless visible watermarking. In *IEEE International Conference on Multimedia and Expo*, pages 853–856, Toronto, Ontario, Canada, 2006.

[246] Yoo, K. S. and Lee, W. H. Wavelet-based blind watermarking technique for real-time watermark interpretation. In *Computational Science and Its Applications, Springer*, pages 348–355. 2003.

[247] You, X., Du, L., Cheung, Y. M. and Chen, Q. A blind watermarking scheme using new nontensor product wavelet filter banks. *IEEE Transactions on Image Processing*, **19**(12):3271–3284, 2010.

[248] Yu, F. Q., Zhang, Z. K. and Xu, M. H. A digital watermarking algorithm for image based on fractional Fourier transform. In *1ST IEEE Conference on Industrial Electronics and Applications*, pages 1–5, Singapore, 2006.

[249] Zebbiche, K., Ghouti, L., Khelifi, F. and Bouridane, A. Protecting fingerprint data using watermarking. In *First NASA/ESA Conference on Adaptive Hardware and Systems*, pages 451–456, Istanbul, 2006.

[250] Zebbiche, K., Khelifi, F. and Bouridane, A. An efficient watermarking technique for the protection of fingerprint images. *EURASIP Journal on Information Security*, pages 1–20, 2008.

[251] Zhang, H., Shu, H., Coatrieux, G., et al. Affine legendre moment invariants for image watermarking robust to geometric distortions. *IEEE Transactions on Image Processing*, **20**(8):2189–2199, 2011.

[252] Zhang, X. D., Feng, J. and Lo, K. T. Image watermarking using tree-based spatial-frequency feature of wavelet transform. *Journal of Visual Communication and Image Representation*, **14**(4):474–491, 2003.

[253] Zhao, J., Koch, E. and Luo, C. In business today and tomorrow. *Communications of the ACM*, **41**(7):67–72, 1998.

[254] Zhaoa, B., Koub, W., Lid, H., et al. Effective watermarking scheme in the encrypted domain for buyerseller watermarking protocol. *Information Sciences*, **180**(23):4672–4684, 2010.

[255] Zhu, C. and Yang, X. Study of remote sensing image texture analysis and classification using wavelet. *International Journal of Remote Sensing*, **19**(16):3197–3203, 1998.

List of Publications

***Refereed Journals*:**

1. **Himanshu Agarwal**, Balasubramanian Raman and Ibrahim Venkat, Blind reliable invisible watermarking method in wavelet domain for face image watermark, *Multimedia Tools and Applications (Springer)*, Published online: 23 March 2014, DOI: 10.1007/s11042-014-1934-1.

2. **Himanshu Agarwal**, Pradeep Kumar Atrey and Balasubramanian Raman, Image watermarking in real oriented wavelet transform domain, *Multimedia Tools and Applications, (Springer)*, (under second revision).

3. **Himanshu Agarwal** and Balasubramanian Raman, Study of finite word length effect on the performance of watermarking methods, *International Journal of Computational Vision and Robotics, (Inderscience)*, (under review).

***Conference Proceedings*:**

4. **Himanshu**, Sanjay Rawat, Balasubramanian Raman and Gaurav Bhatnagar, DCT and SVD based new watermarking scheme, *The IEEE International Conference on Emerging Trends in Engineering and Technology (ICETET'2010)*, pp. 146-151, November 2010, Goa, India.

5. **Himanshu** and Balasubramanian Raman, Indexing scheme for iris using discrete cosine and discrete wavelet transform, *K. Deep et al. (Eds.): Proceedings of the International Conference on Soft Computing for Problem Solving (SocProS'2011), Advances in Intelligent and Soft Computing 131*, pp. 391-399, December 2011, Roorkee, India.

6. **Himanshu Agarwal**, Balasubramanian Raman and Pradeep Kumar Atrey, Watermarking schemes to secure the face database and test images in a biometric system, *The IEEE International Conference on Signal and Image Processing Applications (ICSIPA'2013)*, pp. 128-133, October 2013, Melaka, Malaysia.

7. Ravinder Katta, **Himanshu Agarwal** and Balasubramanian Raman, A reference watermarking scheme for color images using discrete wavelet transform and singular value decomposition, *M. Pant et al. (eds.), Proceedings of the Third International Conference on Soft Computing for Problem Solving (SocProS'2013), Advances in Intelligent Systems and Computing 259*, pp. 577-587, December 2013, Greater Noida, India.

***To be Communicated*:**

8. Visible watermarking based on importance and just noticeable distortion of image regions.

9. Study of comparators for binary watermarks.