

IMPLEMENTATION OF TRANSFORM BASED TECHNIQUES IN DIGITAL IMAGE WATERMARKING

A DISSERTATION

*Submitted in partial fulfillment of the
requirements for the award of the degree*

of

MASTER OF TECHNOLOGY

in

ELECTRICAL ENGINEERING

(With Specialization in Instrumentation and Signal Processing)



By

TARUN RATHI



DEPARTMENT OF ELECTRICAL ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY ROORKEE

ROORKEE-247 667 (INDIA)

JUNE, 2013

No. - MT/250/RPM/2013



INDIAN INSTITUTE OF TECHNOLOGY ROORKEE
ROORKEE

CANDIDATE'S DECLARATION

I hereby certify that the work presented in this dissertation entitled "*Implementation of Transform Based Techniques in Digital Image Watermarking*" submitted in partial fulfilment of the requirements for the award of the degree of **Master of Technology** with specialization in **Instrumentation and Signal Processing**, in the Department of Electrical Engineering, **Indian Institute of Technology Roorkee**, is an authentic record of my own work carried out from July 2012 to June 2013 under the guidance and supervision of **Prof. R. P. Maheshwari and Dr. Manoj Tripathy**, in Department of Electrical Engineering, Indian Institute of Technology Roorkee.

I have not submitted the matter embodied in this dissertation report for the award of any other degree of this or any other institute.

Date: 13-06-2013

Place: Roorkee


TARUN RATHI

M.Tech (I & SP)

I.I.T. Roorkee

CERTIFICATE

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



Dr. R. P. Maheshwari

Professor

Department of Electrical Engineering
Indian Institute of Technology Roorkee
Roorkee-247667, India



Dr. Manoj Tripathy

Assistant Professor

Department of Electrical Engineering
Indian Institute of Technology Roorkee
Roorkee-247667, India

ABSTRACT

Digital image watermarking is used to resolve the problem of data security and copyright protection. In many applications of digital watermarking, watermarked image of good quality is required. But there is tradeoff between number of embedded watermark images and quality of watermarked image. This aspect is quite important in case of multiple digital image watermarking. In this case multiple images singular value decomposition based watermarking algorithm performs much better than other transform based methods. This dissertation presents a robust multiple digital images watermarking using singular value decomposition (SVD) method. The results are compared with Discrete Cosine Transform (DCT) based multiple images watermarking method. In case of SVD image watermarking method only singular values are being varied either in single or multiple image watermarking. This helps in preserving the quality of watermarked image.

To get more robust watermark against geometrical attack and JPEG compression is main issue in most of the watermarking algorithms. Due to the property of SVD, the SVDbased digital image watermarking has replaced DCT and DWT based watermarking. But here combining the property of DCT and SVD, a hybrid algorithm is introduced which gives much better results. DCT of the whole cover image is taken then segmented in to blocks for singular value decomposition. Watermark image is scrambled using Arnold transform and then it is embedded in singular values. This not only improves the robustness but also security of the watermark. To evaluate the algorithm, this hybrid DCT-SVD based watermarking is compared with the pure SVD based algorithm on the basis of PSNR and robustness. Experimental evaluation shows that this algorithm is able to resist a variety of attacks including JPEG compression, different signal processing attacks and geometric attacks.

ACKNOWLEDGEMENT

I would like to express my deep sense of gratitude and sincere thanks to my beloved guide **Prof. R. P. Maheshwari** and **Dr. Manoj Tripathy**, Department of Electrical Engineering, Indian Institute of Technology Roorkee, for being helpful and a great source of inspiration. Their keen interest and constant encouragement gave me the confidence to complete my work. I wish to extend my sincere thanks for his excellent guidance and suggestion for the successful completion of my work.

My sincere thanks to the Head, Electrical Engineering department, I.I.T. Roorkee for providing necessary research facilities to carry out this work and valuable suggestions and motivations provided by other faculty members of the department are duly acknowledged. I also wish to thank supporting staff of Instrumentation & Signal Processing lab for all necessary help provided by them.

I would like to thank my dearest friends Mr. Rahul Saraswat, Mr. Mayank Raut, Mr. Safiullah, Mr. Ashish Chandiok, Mr. Anil Kumar Antil, Mr. Vineet Vajpayee, Mr. Pratul Arvind, Mr. Sachin Singh, Mr. Arvind Arya Yadav and Ms. Neha Nirala for always standing with me by my side and supporting me during my good as well bad period. Whose support and encouragement has been a constant source of guidance to me. Special thanks to my dearest classmates for spending vital time with me.

I dedicate this thesis to my family who supported me during my years of study. Their unremittingly support made this work possible.

TARUN RATHI
(11528023)

Contents

| | |
|--|------------|
| Abstract | i |
| Acknowledgement | ii |
| Contents | iii |
| List of Figures | vii |
| List of Table | ix |
| Abbreviation | x |
| <hr/> | |
| 1. INTRODUCTION | 1 |
| 1.1 Literature Survey | 1 |
| 1.2 Objective of Dissertation Work | 2 |
| 1.3 Organization of Dissertation | 4 |
| 2. DIGITAL IMAGE WATERMARKING | 5 |
| 2.1 Introduction to Watermarking | 5 |
| 2.2 Watermarking Principle | 6 |
| 2.2.1 Embedding Stage | 6 |
| 2.2.2 Distribution Stage | 7 |
| 2.2.3 Extraction Stage | 7 |
| 2.3 Watermarking Properties | 7 |
| 2.4 Performance Measurements | 9 |
| 2.4.1 The Mean Square Error (MSE) | 9 |
| 2.4.2 Peak Signal to Noise Ratio (PSNR) | 9 |
| 2.4.3 Accuracy Rate | 9 |
| 2.4.4 Robustness | 10 |
| 2.5 Classification of Digital Watermarking | 10 |
| 2.5.1 Based on Visibility of Watermark | 10 |
| 2.5.1.1 Visible Watermarking | 10 |
| 2.5.1.2 Invisible Watermarking | 10 |

| | | |
|------------|--|-----------|
| 2.5.2 | Based on Robustness of Watermark | 11 |
| 2.5.2.1 | Robust Watermarking | 11 |
| 2.5.2.2 | Fragile Watermarking | 12 |
| 2.5.2.3 | Semi- Fragile Watermarking | 12 |
| 2.5.3 | Based on Contents | 13 |
| 2.5.4 | Based on Private and Public Watermarking | 13 |
| 2.5.4.1 | Non Blind (or Private) Watermarking | 13 |
| 2.5.4.2 | Blind (or Public) Watermarking | 13 |
| 2.6 | Techniques of Watermarking | 14 |
| 2.6.1 | Spatial Domain Techniques | 14 |
| 2.6.2 | Transform Domain Techniques | 14 |
| 2.7 | Application | 15 |
| 2.7.1 | Copyright Protection | 15 |
| 2.7.2 | Digital Fingerprinting | 15 |
| 2.7.3 | Content Authentication | 16 |
| 2.7.4 | Broadcast Monitoring | 16 |
| 2.7.5 | Miscellaneous Applications | 17 |
| 2.8 | Conclusions | 17 |
| 3. | DIFFERENT TECHNIQUES OF DIGITAL IMAGE WATERMARKING | 19 |
| 3.1 | Introduction | 19 |
| 3.2 | LSB Based Watermarking | 19 |
| 3.3 | Correlation Based Watermarking | 20 |
| 3.4 | Discrete Cosine Transform (DCT) Based Watermarking | 20 |
| 3.4.1 | Watermark Embedding | 23 |
| 3.4.2 | Watermark Extraction | 24 |
| 3.5 | Discrete Wavelet Transform (DWT) Based Watermarking | 24 |
| 3.5.1 | Watermark Embedding | 25 |
| 3.5.2 | Watermark Extraction | 26 |
| 3.6 | Singular Value Decomposition (SVD) Based Watermarking | 27 |
| 3.6.1 | Watermark Embedding | 28 |
| 3.6.2 | Watermark Extraction | 29 |

| | | |
|-------------|---|----|
| 3.7 | Different Noise and Attacks | 30 |
| 3.7.1 | Signal Processing Attacks | 30 |
| 3.7.2 | Geometric Attacks | 30 |
| 3.7.3 | JPEG Compression | 30 |
| 3.8 | Experimental Results and Discussion | 30 |
| 3.9 | Comparison among Different Watermarking Techniques | 35 |
| 3.10 | Conclusions | 36 |
| | | |
| 4. | MULTIPLE IMAGES WATERMARKING | 37 |
| 4.1 | Introduction | 37 |
| 4.2 | DCT Based Multiple Images Watermarking | 37 |
| 4.2.1 | Watermark Embedding | 38 |
| 4.2.2 | Watermark Extraction | 40 |
| 4.3 | SVD Based Multiple Images Watermarking | 41 |
| 4.3.1 | Watermark Embedding | 41 |
| 4.3.2 | Watermark Extraction | 43 |
| 4.4 | Experimental Results and Discussion | 44 |
| 4.4.1 | DCT Based Multiple Images Watermarking | 44 |
| 4.4.2 | SVD Based Multiple Images Watermarking | 46 |
| 4.5 | Conclusions | 48 |
| | | |
| 5. | DCT-SVD BASED HYBRID WATERMARKING TECHNIQUE | 49 |
| 5.1 | Introduction | 49 |
| 5.1.1 | Arnold Transform | 50 |
| 5.2 | SVD Based Watermarking | 51 |
| 5.2.1 | Pure SVD Based Watermarking | 51 |
| 5.2.2 | SVD Based Hybrid Watermarking | 52 |
| 5.3 | DCT-SVD Based Watermarking | 52 |
| 5.3.1 | Watermark Embedding | 52 |
| 5.3.2 | Watermark Extraction | 53 |
| 5.4 | Experimental Results and Discussion | 54 |
| 5.5 | Conclusions | 60 |

| | |
|--|-----------|
| 6. Conclusions and Future Scope | 61 |
| 6.1 Conclusions | 61 |
| 6.2 Future Scope | 62 |
| References | 63 |
| List of Candidate's Publication | 67 |



List of Figures

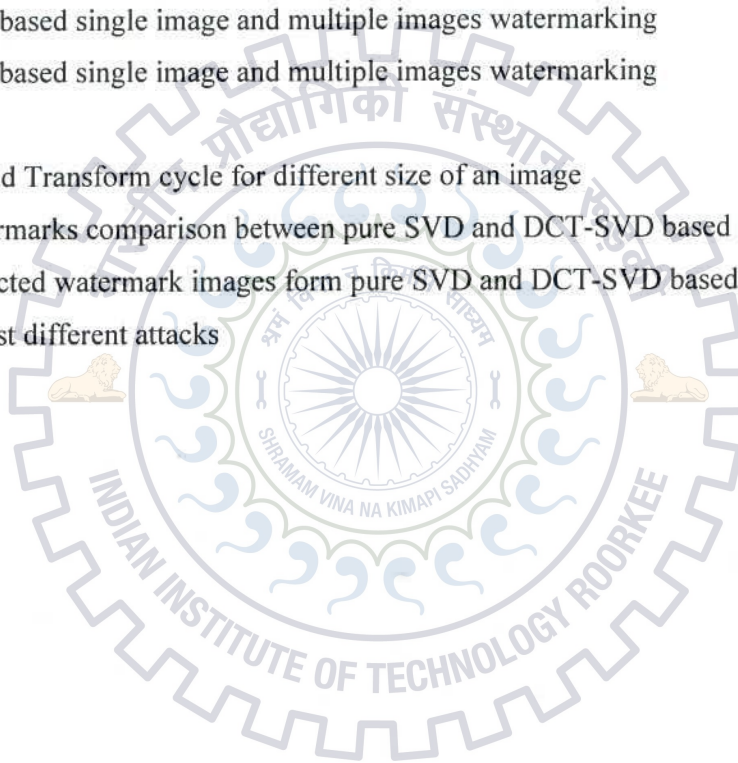
| | | |
|------|---|----|
| 2.1 | Block diagram of a watermarking system | 6 |
| 2.2 | Watermarking classification based on visibility | 10 |
| 2.3 | Watermarking classification based on Robustness | 11 |
| 2.4 | Robust watermarking | 11 |
| 2.5 | Fragile watermarking | 12 |
| | | |
| 3.1 | 8x8 block before DCT | 22 |
| 3.2 | 8x8 block after DCT | 22 |
| 3.3 | Frequency map | 22 |
| 3.4 | Block diagram of DCT based watermark embedding | 23 |
| 3.5 | Block diagram of DCT based watermark extraction | 24 |
| 3.6 | 2D DWT decomposition of an image | 25 |
| 3.7 | Block diagram of DWT based watermark embedding | 26 |
| 3.8 | Block diagram of DWT based watermark extraction | 27 |
| 3.9 | Block diagram of SVD based watermark embedding | 28 |
| 3.10 | Block diagram of SVD based watermark extraction | 29 |
| 3.11 | PSNR variation of extracted watermark images of different watermarking algorithms against different noise/attacks | 32 |
| 3.12 | Robustness variation of extracted watermark images of different watermarking algorithms against different noise/attacks | 32 |
| | | |
| 4.1 | DCT based multiple watermarks embedding | 39 |
| 4.2 | Selected coefficients for two watermarks in a DCT block of the host image | 39 |
| 4.3 | DCT based multiple watermarks extraction | 40 |
| 4.4 | SVD based multiple watermarks embedding | 42 |
| 4.5 | SVD based multiple watermarks extraction | 43 |
| 4.6 | DCT based multiple images watermarking | 44 |
| | (a) Host image (b) Watermarked image (c) First watermark | |
| | (d) First recovered watermark (e) Second watermark | |
| | (f) Second recovered watermark | |

| | | |
|-----|--|----|
| 4.7 | Variation in PSNR of watermarked image in DCT based single and multiple images watermarking | 45 |
| 4.8 | SVD based multiple images watermarking (a) Host image (b) Watermarked image (c) First watermark (d) First recovered watermark (e) Second watermark (f) Second recovered watermark | 46 |
| 4.9 | Variation in PSNR of watermarked image in SVD based single and multiple images watermarking | 47 |
| 5.1 | Images after applying Arnold transform | 50 |
| 5.2 | Block diagram of DCT-SVD watermark embedding | 53 |
| 5.3 | Block diagram of DCT-SVD watermark extraction | 54 |
| 5.4 | PSNR variation of watermark images in pure SVD and DCT-SVD based algorithms against different attacks | 56 |
| 5.5 | Robustness variation of watermark images in pure SVD and DCT-SVD based algorithms against different attacks | 56 |



List of Tables

| | | |
|-----|---|----|
| 2.1 | Comparison between spatial and transform domain watermarking | 14 |
| 3.1 | Comparison of extracted watermarks from different watermarking algorithm | 31 |
| 3.2 | Extracted watermark images of different watermarking methods against different attacks | 33 |
| 4.1 | DCT based single image and multiple images watermarking | 45 |
| 4.2 | SVD based single image and multiple images watermarking | 47 |
| 5.1 | Arnold Transform cycle for different size of an image | 50 |
| 5.2 | Watermarks comparison between pure SVD and DCT-SVD based algorithm | 55 |
| 5.3 | Extracted watermark images form pure SVD and DCT-SVD based method against different attacks | 57 |



Abbreviations

| | |
|--------------------|------------------------------------|
| AR | Accuracy Rate |
| DCT | Discrete Cosine Transform |
| DFT | Discrete Fourier Transform |
| DWT | Discrete Wavelet Transform |
| FRFT | Fractional Fourier Transform |
| HVS | Human Visual System |
| IDCT | Inverse Discrete Cosine Transform |
| IDWT | Inverse Discrete Wavelet Transform |
| JPEG | Joint Photographic Experts Group |
| JND | Just Notable Difference |
| LSB | Least Significant Bit |
| MSE | Mean Square Error |
| NC | Normalized Correlation |
| PN Sequence | Pseudo Random Sequence |
| PSNR | Peak Signal to Noise Ratio |
| SVD | Singular Value Decomposition |
| SVs | Singular Values |

Chapter 1

Introduction

1.1 Literature Survey

Many watermarking algorithms are proposed in the literature. On the basis of working domain there are spatial domain and transform domain watermarking. Spatial domain method is simple and easy for implementation. These watermarking algorithms modify the pixel values of the original image where the watermark is to be embedded, while in transform domain, host image is transformed using any transform method then modifications are made to the transformed coefficients. Transform domain watermarking techniques are more robust in comparison to spatial domain methods.

According to Wang *et al.* [1], a DWT-DCT hybrid robust watermarking is proposed. Watermark is embedded with JND model. Different features like robustness, imperceptibility, secret key, fragility are mentioned for a watermarking algorithm and watermarking is classified on different basis [2 3 4]. According to Tong *et al.* [5], a fragile watermarking is used for tempering detection. This helps in the authentication of the data [5 12]. Suhailet *al.* [8] have used zigzag ordering reordering for jpeg model of host image in DCT based watermarking. Dubolia *et al.* [14] have compared the two transform domain algorithm based on DWT and DCT. These algorithms are evaluated on the basis on PSNR and normalized correlation (NC) of the extracted watermark. A.B. Dehkordiet *al.* [15] have proposed a new LSB based robust watermarking which is optimized for local structural similarity. Majid *et al.* [18] have used a genetic algorithm (GA) based optimization in DCT based watermarking. This will select the best coefficients for embedding the watermark.

Sun *et al.* [21] describes the properties of singular value decomposition and presented three hybrid methods based on SVD. First method presents SVD decomposition of host image in transform domain. Here DCT is used for transforming the image. In second method DWT is used for transforming the host image. The robustness and the invisibility of the watermarked image are satisfied. But there is a false positive and ambiguity problem this

is problem is overcome in third method in which he proposed new hybrid SVD based method using particle swarm optimization.

Rykaczewski [26] presented a SVD based watermarking for rightful ownership. L. Liu and Q. Sun [27] have proposed a hybrid algorithm based on DCT-SVD against geometric attacks. In this method whole host image is transformed using DCT then SVD decomposition takes place. After taking inverse process of SVD and using IDCT the watermarked image is produced. Himanshu *et al.* [28], discussed a singular value decomposition method using masking function. This gives better results than pure SVD based watermarking. M. Ding and F. Jing [29] presented encryption method using improved Arnold transform. A hybrid DCT and SVD based watermarking has been implemented where DCT can be used as block wise DCT or as whole DCT for host image then decomposition using SVD is applied to image [31 32 33 35].

1.2 Objective of Dissertation Work

Digital image watermarking is used in a variety of applications like content labeling, copyright protection, meta-data insertion, tampering detection, broadcast monitoring, and digital fingerprinting. During last two decade, with the growing of the digital communication, more popularity of the internet and the multimedia technology, users have been associated with multimedia data. Consequently it has been necessary to provide protection to the intellectual property rights of digital media. A number of text images, videos and audios are being transmitted over digital media on internet or any other public channel. Due to easy accessing of these contents there may a chance that anyone can fetch or copy data and redistribute as duplicate copy of that content without permission of owner. So some techniques for copyright protection should be used. Watermarking technique is used to resolve the problem of copyright protection. Apart from copyright protection digital watermarking is also being used in many other applications like in meta-data insertion medical X-rays could store patient records.

Many successful works and research have been completed on digital watermarking. Like watermarking is also used in tamper detection. In this application by embedding fragile watermarks digital data can be detected for tampering. If the fragile watermark is degraded or

destroyed, then it indicates the occurrence of tampering and consequently the digital content should not be trusted.

Watermarking is classified in to two categories spatial and transform domain. Spatial domain watermarking methods are earlier methods and easy for implementation but these techniques are not robust to attacks. In this method the set of pixels of the cover image are changed according to the watermark.

In transform domain watermarking, transformation is applied to the cover image then transform coefficients are modified according to the watermark. These watermarking techniques are more robust than spatial domain methods. This is due to the fact that transform based watermarking makes the attacker difficult to read or modify the watermarked image.

The advantages of transform domain method are:

- a) Computational complexity is low.
- b) Signal processing operations and manipulations can be easily performed.
- c) Robust to attacks.
- d) Can be used in compression based transmission

The objective of this work includes:

- (1) SVD based watermarking method is performed and compared with spatial domain and transform domain methods. Comparison has been made on the basis of the quality of extracted watermark from the noisy/attacked watermarked image in recovering algorithm.
- (2) DCT based and SVD based multiple images watermarking are performed and Watermarked images of these watermarking methods are compared with the watermarked image of single image watermarking method.
- (3) A hybrid DCT-SVD based robust watermarking is proposed. This watermarking method is robust against JPEG compression and geometric attack. To increase the security of this watermarking system an Arnold transform as watermark scrambling is used.

1.3 Organization of Dissertation

- Chapter 2** This chapter gives an overview about digital watermarking, what is watermarking and why it is required. First of all we present a watermarking system which shows the three stage of a watermarking stage. Different properties of watermarking and desirable properties for a watermarking are described. After then digital watermarking has been classified on different basis like robustness, visibility, content and privacy. In the end of this chapter different applications of digital watermarking are discussed.
- Chapter 3** In this chapter different spatial and transform based techniques of watermark embedding are discussed. In spatial domain LSB based and correlation based algorithm and in transform domain DCT based and DWT based algorithm are implemented. Apart from these algorithms, a SVD based algorithm is implemented which dominates on all techniques. To evaluate the performance of all watermarking algorithms (discussed above), noise and attacks are inserted in to the watermarked images before extracting watermark. Then on the basis of PSNR, robustness and accuracy rate of extracted watermarks, all the watermarking methods are compared.
- Chapter 4** This chapter introduces a DCT based multiple images watermarking and an SVD based multiple images watermarking. In multiple images watermarking more than one message (information) can be embedded. On the basis of different parameter of watermarked images and extracted watermarks, both the algorithms are compared and results have been shown in tables and graphs.
- Chapter 5** In this chapter a new hybrid watermarking algorithm based on DCT-SVD is proposed. To provide more security to this algorithm, Arnold transform is used as watermark scrambling. In the end of this chapter we present experimental results obtained with this watermarking scheme aiming at more robustness against different geometric attacks and JPEG compression.
- Chapter 6** We presented our conclusions from the results presented in this thesis and discussed the scope of future research work.

Chapter 2

Digital Image Watermarking

2.1 Introduction of Watermarking

Growth of internet and multimedia because of information digitization has been very fast during the last few years. It has also become necessary to provide authentication of content and copyright protection so that, it should not be easy for some individual or groups to copy digital data or contents without agreement with the owner [1]. To stop the illegal copying and tracking of the digital contents and for several other important applications, digital watermarking is introduced.

The digital watermarking covers many topics such as communication theory, signal processing and encryption/decryption. The research in digital watermark is to provide copyright protection to digital products, and to stop and track illegal copying and transmission of them [2]. Watermarking stands for embedding information, which is able to show the ownership or detect copyright intrusion, into the digital image, audio or video. Purpose of watermarking determines that the watermark should be indivisible and robust to common signal processing and attacks.

Digital watermarking is a technique of hiding data(message or information) related to a digital signal within the signal itself. Its concept is closely related to steganography, in that they both hide information inside a digital signal. However, what distinguishes them is their goal. Watermarking tries to hide a message related to the actual content of the digital signal, while in steganography the digital signal has no relation to the message, and it is merely used as a cover to hide its existence. “Watermarking” deals with embedding information like name of the creator, recipient and status etc. into the cover object in such a way that it remains undetectable and transparent. Watermarking is more robust to malicious attacks than steganography [3].

2.2 Watermarking Principal

A watermarking system can be divided into three stages: embedding, distribution, and extraction. A watermarking algorithm embeds the watermark into the host signal and generates a watermarked image. This watermarked image is then transmitted through a medium or channel. Attacks may make some modifications to the watermarked image, but in the case of a robust watermark, it is possible to extract the watermark even after malicious attacks. A secret key provides security to the watermarking system. The watermarking process may be divided into three stages described below.

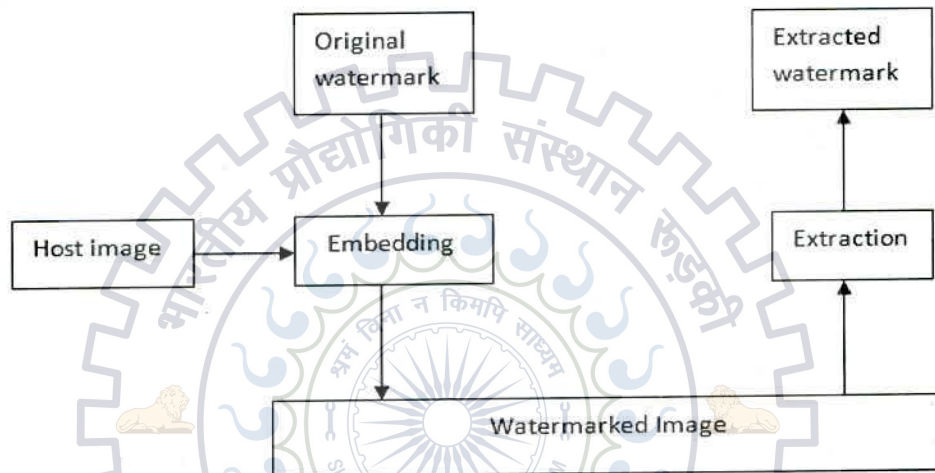


Fig. 2.1: Block diagram of a watermarking system

2.2.1 Embedding Stage

Embedding of watermarking can be done in two ways either directly or after transforming the host image using any of transform algorithms. Transform based watermarking involves changing the image to the desired transform. This includes the discrete cosine transform (DCT), the discrete Fourier transforms (DFT) and the wavelet transform domain. The watermark to be embedded may be a bit stream, a binary image or a pseudo-random number that is to be placed into host or cover image. The watermark is then attached to the desired coefficients of the transform as recommended by human visual system (HVS) research [4]. The watermarked image is the output of this process and is obtained by performing an inverse transform on the modified transform coefficients.

2.2.2 Distribution Stage

The watermarked image obtained above is then distributed through digital channels (on an internet site). In this process, watermarked image in the channel may have undergone one of several mappings, such as image manipulations, compression, and enhancements etc. In addition, malicious attacks are also possible in this stage to degrade or destroy the watermark.

2.2.3 Extraction Stage

In this stage, watermark is extracted from the distributed watermarked image [4]. This stage may need a secret key without knowing this one cannot extract the message or watermark image.

2.3 Watermarking Properties

Digital image watermarking is having many properties. On the basis of that we can compare one method of watermarking to another. There are many properties of watermarking like transparency, capacity, robustness, security, imperceptibility etc.

2.3.1 Transparency

This is the most fundamental necessity for any watermarking system. Watermarking method shall be such that it is transparent to the user [3]. The digital watermark should not change original image after it is watermarked. "Transparency (fidelity) can be defined as perceptual similarity between the watermarked image and host image". There should be no visible distortions [5].

2.3.2 Capacity

Capacity means the amount of information that is embedded into a host signal as a watermark to successfully recover during extraction. Watermarking should be able to carry enough information. Different application has different capacity requirement [5]. Often, requirement of capacity always struggle against two important requirements, that is robustness and imperceptibility. So there is a tradeoff between capacity and either imperceptibility or robustness or both.

2.3.3 Robustness

Watermark robustness accounts for the capability of the message or watermark to detect watermark after common signal manipulations and different noise and attacks. Apart from malicious attacks, common signal processing operations can create a threat to the detection of watermark, thus there is a need to make such watermarking so that watermark can survive those operations [5]. For example, a good strategy for robustly embedding a watermark into an image is to insert it into perceptually significant parts of the coverimage. Not all watermarking applications require a watermark to be robust enough to survive all attacks and signal manipulation operations. Indeed, in an extreme case, robustness may be irrelevant in some cases where fragility of the watermarking system is desirable[6].

2.3.4 Imperceptibility

The imperceptibility means the perceptual transparency or visual quality of the watermarked image. Ideally, there should not be any perceptible difference between the watermarked and original signal [7]. The watermark should be embedded in the host signal in such a way that it cannot be seen. However, watermark invisibility may conflict with other requirements such as capacity or robustness or both [8].

2.3.5 Security

A watermarking technique will be secure if the algorithms for embedding and extracting the watermark do not help an unauthorized party to detect the presence of the watermark. Security of watermarking algorithm needs a secret key which is to be used for embedding and extracting. In this case known values of coefficients, pseudo random sequences or any description may be used as secret key. There are two way securities. In the first one, one needs secret key for extracting the watermark. In the second one unauthorized user cannot decode watermark without knowing decryption or decoding method [9].

2.3.6 Effect on Bandwidth

Watermarking should be done in such a way that it does not increase the required bandwidth for transmission of watermarked image. Watermarking should not become a burden for the available bandwidth; otherwise the method will be rejected.

2.4 Performance Measurements

For evaluation and comparing the watermarking algorithm we require few parameters are required on the basis of that we can find out the quality of extracted watermark and watermarked image with respect of original watermark and host image respectively.

2.4.1 The Mean Square Error (MSE)

The Mean Square Error (MSE) is used to compare image quality. The MSE represents the cumulative squared error between the modified and the original image, whereas PSNR represents a measure of the peak error. Lower the value of MSE, lower the error will be [10].

$$MSE = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N (p_1[i, j] - p_2[i, j])^2 \quad \dots\dots (2.1)$$

Where M, N = dimensions of image

$P_1 [i, j]$ = component values of the pixel [i, j] in the original image.

$P_2 [i, j]$ = component value of the pixel [i, j] in the modified image.

In this equation (2.1), M and N are the number of rows and columns in the input images, respectively.

2.4.2 Peak Signal to Noise Ratio(PSNR)

The PSNR computes the peak signal-to-noise ratio in decibels, between two images. This ratio is often used as a quality measurement between the original and a modified image. Higher the PSNR, better the quality of the modified or reconstructed image is obtained. To compute the PSNR, we need to calculate the mean-squared error. The PSNR is defined as [11].

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} \quad (dB) \quad \dots\dots (2.2)$$

2.4.3 Accuracy Rate

Accuracy rate is used to compare original image and processed image. It is defined by using equation (2.3).

$$Accuracy \text{ rate} = \left(\frac{\text{Number of pixels in processed image}}{\text{Number of pixels in original image}} \right) \times 100 \% \dots\dots (2.3)$$

2.4.4 Robustness

Robustness is the ability of the watermark image to preserve information even after different noise and malicious attacks [10]. This is similarity measurement between the original watermark and extracted watermark and measured by normalized correlation (NC) given in equation (2.4).

$$NC = \frac{\sum_i w_i w_i^*}{\sum_i w_i^2} \dots\dots\dots (2.4)$$

Here w_i is the original watermark and w_i^* is the extracted watermark [10]. Bigger the NC value means better similarity between two images.

2.5 Classification of Digital Watermarking

2.5.1 Based on Visibility of Watermark



Fig. 2.2: Watermarking classification based on visibility

2.5.1.1 Visible Watermarking

As name says visible watermark images are the visual patterns like logos, which are to be embedded into or overlaid on digital signal which is very similar to visible paper watermarks. However, the name is confusing since visible watermarks are not watermarks in the sense of the paper. Visible watermarks are mainly related to images, for example, to visibly mark preview images available in image databases or on the internet in order to stop people from commercial use of such images [9].

2.5.1.2 Invisible Watermarking

The watermark is embedded into the image in such a way that it should not be perceived by human eye. It is used in image authentication and prevents it from being copied.

2.5.2 Based on Robustness of Watermark

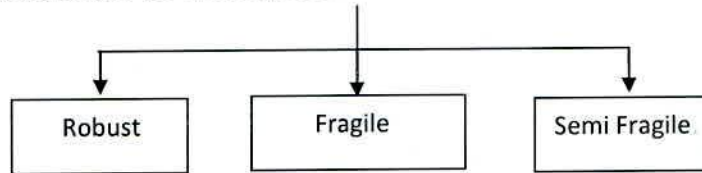


Fig. 2.3: Watermarking classification based on robustness

2.5.2.1 Robust Watermarking

Without disturbing the host signal invisible watermark cannot be manipulated. This is by far the important requirement for a watermarking system. There are various noise, intentional attacks (cropping, compression, scaling) and unintentional attacks which are aimed at destroying the watermark. So the embedded watermark should be such that it is invariant to various noise and attacks. They are designed to resist any signal manipulations that may be encountered [12]. All applications where security is the main issue robust watermarking is used.

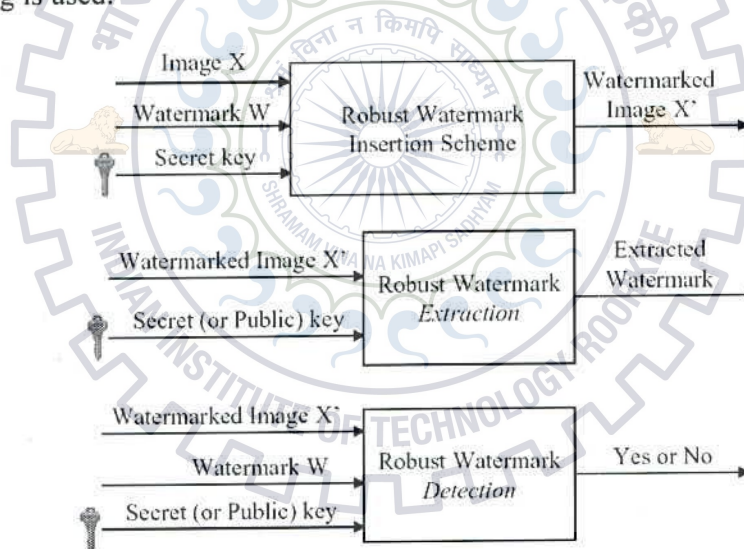


Fig. 2.4: Robust watermarking

The desirable properties of a robust watermarking are

1. Perceptual transparency
2. Data capacity

3. Robustness to unintentional image processing operations (e.g., linear and non linear filtering, compression rotation and scale, random noise, cropping and analog conversion).
4. Tamper resistance: difficult for an attacker to destroy or remove a message once it has been embedded.
5. Computational complexity

2.5.2.2 Fragile Watermarking

Fragile watermarking is designed with low robustness. They are used to check the integrity of objects (data). The small alteration of the image destroys the watermark. Fragile watermark is used for authentication of the data at a pixel or small block level. The problem with fragile watermarking is that JPEG compression is not possible [3 12].

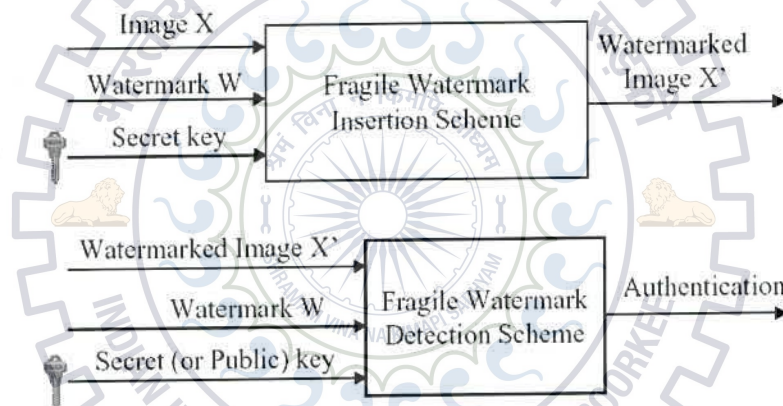


Fig.2.5: Fragile watermarking

2.5.2.3 Semi- Fragile Watermarking

Earlier fragile watermarking is used in data authentication. In this case, a single bit change in a watermarked image will be classified as unauthentic. An image can be authenticated using cryptographic hash or digital signature as the fragile watermark. There are several benefits of watermarking over cryptographic methods for this purpose. Firstly the fragile watermark embedded into an image eliminates the need for extra storage of original image. Secondly it is also immune to format conversion because it stays intact with the image and undergoes the same transformation as the image. Finally in addition to the integrity check of the whole image, the watermark can also be designed to determine which

part of the image is unauthentic. This is tamper localization. For this purpose robust watermark is used in authentication. To ensure that fragile watermark does not interfere with the authentication information of an image, the embedding space can be divided into a watermark embedding space and watermark generation subspace. Both fragile and robust watermarks can be used in data authentication [3, 4]. So a semi-fragile watermark can be designed to tolerate genuine change while highlighting intentional distortions. This characteristic made the semi fragile watermarks appropriate for many applications. For example, we may want to allow image compression (JPEG compression) in order to save storage space.

2.5.3 Based on Contents

Watermarking may be classified on the basis of cover or host image used. If cover is used as image for embedding watermark that this is called image watermarking, similarly audio and video watermarking can be used for embedding watermark.

2.5.4 Based on Private and Public Watermarking

2.5.4.1 Non blind (or Private) Watermarking

Non blind watermarking are those where the original host or cover image is required for extracting the watermark. Without original cover image, one cannot extract watermark [4]. So this watermarking is also called private or informed watermarking.

2.5.4.2 Blind (or Public) Watermarking

At the extraction part one does not require original host or cover image for extracting the watermark image. So this watermarking is also called public watermarking [4].

2.6 Techniques for Digital Image Watermarking

2.6.1 Spatial Domain Techniques

In case of spatial domain watermarking the watermark is embedded into the host image by changing the pixels value directly. Spatial domain technique may have the large capacity than transform domain but the problem is that it can be easily detected by means of computer analysis [13] or can be easily destroyed by signal manipulation or by different type of attacks. So spatial domain techniques are easy for implementation but these are not robust to attacks. Following are the spatial domain techniques

- a) LSB based Technique
- b) Predictive Coding Schemes
- c) Correlation-Based Technique
- d) Patchwork Technique

2.6.2 Transform Domain Techniques

In the transform domain the host image is converted using any of frequency transform methods, then coefficients are varied according to the watermark. So it is difficult to extract hidden information [13]. So this is robust than spatial domain technique. There are following types of main frequency domain watermarking

- a. Discrete Fourier Transform (DFT) Based
- b. Discrete Cosine Transform (DCT) Based
- c. Discrete Wavelet Transform (DWT) Based
- d. Fractional Fourier Transform (FRFT) Based

Table 2.1: Comparison between spatial and transform domain watermarking

| Parameters | Spatial Domain | Frequency Domain |
|--------------------|----------------|------------------|
| Perceptual quality | Low | High |
| Capacity | High | low |
| Computational cost | Low | High |
| Robustness | Fragile | More Robust |
| Example | Authentication | Copyrights |

2.7 Application

There are many application scenarios of watermarking. They can be classified in a number of different ways. The following classification is based on the information type, conveyed by the watermark. In the following section we will provide a more explanation of possible application scenarios involving watermarking.

- Copyright Protection
- Digital Fingerprinting
- Content Authentication
- Broadcast Monitoring
- Miscellaneous Applications

2.7.1 Copyright Protection

Copyright Protection is the most important application of watermarking. A lot of information are being transmitted over insecure networks daily, so copyright protection becomes a very prominent issue. Watermarking an image will stop redistribution of copyrighted images. Copyright protection is the first application for which digital watermarking was targeted for. It is imperceptibly embedded as a watermark in the cover image. If users of digital content (audio, images, and video) have an easy access to watermark detectors, they should be able to recognize and interpret the embedded watermark and identify the copyright owner of the watermarked content.

A copyright owner distributes digital contents with invisible watermark embedded in it. In the case of a copyright ownership dispute, a legal owner has to prove his ownership by showing that original work is his/her, and that the disputed work has been obtained from the original by inserting a watermark into it. This could be done by providing the original work together with the watermark detector to detect the owner's watermark in a disputed work.

2.7.2 Digital Fingerprinting

There are few applications where the more information associated with a digital content should contain information about the end user, rather than about the owner of



that digital content. For example in a film making environment, the incremental works are often distributed every day to a number of people associated in a movie making activities. These are secret. If a version is disclosed then the studio would like to identify the source of that leak. The problem of identifying the source of a leak can be solved by distributing somewhat different copy to each recipient, thus associating uniquely watermark with each copy for a person makes the digital fingerprinting.

2.7.3 Content Authentication

Multimedia editing software programs make easy to modify digital content. Since it is also easy to interfere with a digital data, there is a requirement to verify integrity and authenticity of the data. Problem of temper detection can be solved by using fragile watermarking [5]. Watermarks can obviously be used for embedding signature directly into the content. Since watermarks used for authentication of content have to be designed to become invalid if even small modifications of digital content take place. These type of watermarks are fragile watermarks. Fragile watermarks can also be used in applications where it is necessary to figure out how digital content was modified or which part of it has been tampered with.

2.7.4 Broadcast Monitoring

There are many valuable products which are regularly broadcast over the television network like news, sports movies, events, advertisements etc. Broadcast time is very expensive, and advertisers pay hundreds of thousands of rupees for each run of their short commercial that appears during breaks of important serial, movies, or sporting events. To provide bill accurately in this environment is more important. So advertisers who would like to make sure that they will pay only for the commercials which will be actually broadcast. Broadcast monitoring is important for the performers in commercials who would like to ask for advertisers royalty payments accurately. It is usually used to collect information about the data being broadcast, and this information is used for billing as well as other purposes. This monitoring can be done by two types. One by human observers who watch the broadcast and keep track of all they see. This is expensive and erroneous. So automated monitoring is used.

Watermarking can also be used as automated monitoring which is having major application in commercial advertisement [5].

2.7.5 Miscellaneous Applications

2.7.5.1 Content Labeling

In content labeling information embedded in the data, comprise an annotation which gives some more information about the data. Examples are digital cameras takes images with the date and time, when the photograph was taken. Another example is medical imaging machines which annotate X-Ray images with patient's name, ID.

2.7.5.2 Usage Control and Copy Protection

In this application digital watermark is inserted to indicate the number of copies permitted. If a copy is made every time the hardware alters the watermark and at the same time it would not create any more copies of the data (content). In DVD technology this application is commonly used.

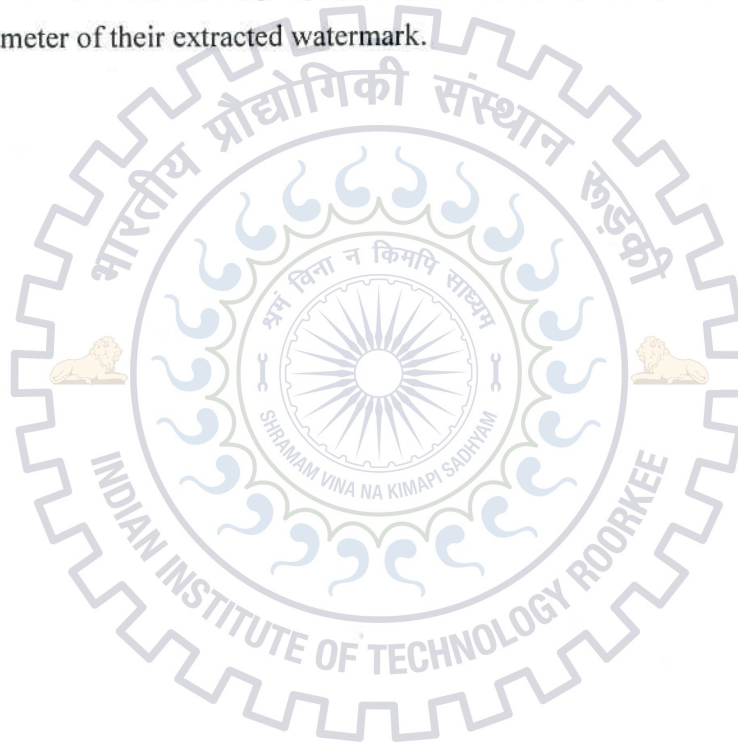
2.7.5.3 ID Card Security

Information in a passport or ID (e.g., person's name, passport number, , etc.) can also be included in the person's photo that appears on the ID. This information can be embedded as watermark. Information written on ID can be compared by extraction and this verifies the ID card. So the adhesion of the watermark can provide an additional level of security in this application. For example, if the ID card is lost or stolen and the picture may be replaced by a forged copy, the failure in extracting the watermark will invalidate that ID card.

2.8 Conclusions

Digital watermarking is a rapidly growing area of research and development. In this chapter an overview of digital watermarking is presented. First of all general model of the watermarking process is shown, and identified its two main components embedded and detector. Watermarking systems is classified on different basis

In the overview of watermarking techniques, various watermarking algorithms are mentioned for embedding a message in different domains like spatial, block DCT, Wavelet, and discrete Fourier domains etc. then we looked at the range of applications that could benefit from applying digital watermarking technology. Protection of intellectual property is very important nowadays because digital multimedia content can be copied and distributed easily, quickly, inexpensively and with high quality. Watermarking has been accepted as a complementary technology to multimedia encryption, providing some additional level of protection. Other applications, such as fingerprinting, content authentication, copy protection and device copy control have also been identified. In next chapter spatial and transform based five watermarking algorithms are described and compared on the basis of different parameter of their extracted watermark.



Chapter 3

Different Techniques of Digital Image Watermarking

3.1 Introduction

There are two domain of the watermarking algorithm. One is spatial domain in which data bits are inserted in to the host image or cover image directly but problem with spatial domain watermarking is that watermark can easily be detected by computer analysis [13] or can be destroyed by using malicious attacks in the channel. So these algorithms are not robust and secure. Another domain is transform domain which is much better than the spatial one. In this domain the message bits are embedded after transforming the host image by using one of transforms based method like discrete Fourier transform (DFT), discrete wavelet transform (DWT) discrete cosine transform (DCT) based algorithm. It is very tough to detect the hidden information (message) from the watermarked image in transform based algorithm. If coefficients of large values are taken for embedding the message bits than extracted watermark image would be more robust [13].

There are many features of digital image watermarking like security, capacity, imperceptibility, robustness etc. but there is a tradeoff between three features capacity, imperceptibility and robustness. So for a better watermarking system to get better features is also important issue. In recent years much work has been done to find the best tradeoff between the capacity, imperceptibility and robustness [15]. SVD based algorithm or SVD based hybrid algorithm gives better features.

3.2 LSB Based Watermarking

Least significant bit based watermarking is very earlier and simple spatial domain method for information embedding [13, 16]. Using LSB based algorithm, large amount of data can be embedded with a little impact to watermarked image quality. In this algorithm watermark image is changed in to bit stream. The least significant bits of the selected subset of pixels of the host image are replaced by these message bits. The message bits can be embedded in a sequence of a set of pixels which acts as a secret key without knowing this

one cannot extract watermark from watermarked image. In the extraction part, the message bits are recovered from the host image and reshaped to generate watermark image [16]. In this algorithm The LSBs of the host image are varying which contribute less in the watermarked image which means quality of the watermarked image is not affected much.

3.3 Correlation Based Watermarking

This is generalized spatial domain technique which is based on correlation technique for extracting the watermark. In this watermarking algorithm, two pseudo random noise (PN) sequences for message bit '1' and '0' are used. These pseudo random sequences also work as secret key without knowing this watermark extraction will not be possible. Same pseudo random sequence is required at extraction part. These pseudo random noise sequences are used to make a mask pattern $W(x,y)$. This watermarking mask will be of the same size of host image. Using a gain factor, this watermarking mask is added to the host image to produce watermarked image [10].

$$Im_w(x,y) = Im(x,y) + k * W(x,y) \dots\dots\dots (3.1)$$

Where

$Im_w(x,y)$ = Watermarked image

$Im(x,y)$ = Original image

K = Gain factor

$W(x,y)$ = Watermarking mask made of PN sequences

Increasing k increases the robustness of the watermark at the expense of the quality of watermarked image. At the extraction algorithm the correlation between random noise and the watermarked image is found out from which watermark is extracted [16].

3.4 Discrete Cosine Transform (DCT) Based Watermarking

This is a transform domain algorithm which is more robust than spatial domain method. A discrete cosine transform (DCT) converts the image in terms of a sum of cosine function oscillating at different frequencies [14].

(a) The One-Dimensional DCT

The most common DCT definition of a 1-D sequence of length N is

$$C(u) = \alpha(u) \sum_{x=0}^{N-1} f(x) \cos\left[\frac{\pi(2x+1)u}{2N}\right] \quad \dots\dots\dots(3.2)$$

for $u = 0, 1, 2, \dots, N-1$.

Similarly, the inverse transformation is defined as

$$f(x) = \sum_{u=0}^{N-1} \alpha(u) \cdot c(u) \cdot \cos\left[\frac{\pi(2x+1)u}{2N}\right] \quad \dots\dots\dots(3.3)$$

for $x = 0, 1, 2, \dots, N-1$. In both equations (3.2) and (3.3), $\alpha(u)$ is defined as

$$\alpha(u) = \sqrt{\frac{1}{N}} \quad \text{when } u=0 \text{ and}$$

$$\alpha(u) = \sqrt{\frac{2}{N}} \quad \text{when } u \neq 0$$

(b) The Two-Dimensional DCT

The 2-D DCT is a direct extension of the 1-D case and is given by

$$C(u,v) = \alpha(u) \alpha(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x,y) \cos\left[\frac{\pi(2x+1)u}{2N}\right] \cdot \cos\left[\frac{\pi(2y+1)v}{2N}\right] \quad \dots\dots\dots(3.4)$$

for $u, v = 0, 1, 2, \dots, N-1$ and $\alpha(u)$ and $\alpha(v)$ are defined in (3.5). The inverse transform is defined as

$$f(x,y) = \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} \alpha(u) \cdot \alpha(v) \cdot c(u,v) \cos\left[\frac{\pi(2x+1)u}{2N}\right] \cdot \cos\left[\frac{\pi(2y+1)v}{2N}\right] \quad \dots\dots\dots(3.5)$$

for $x, y = 0, 1, 2, \dots, N-1$.

The 8x8 matrix block of host image, and its DCT coefficient after taking DCT transform are shown in following fig. 3.1 and fig. 3.2.

| | | | | | | | |
|----|----|-----|-----|-----|-----|-----|-----|
| 75 | 76 | 75 | 75 | 69 | 66 | 77 | 71 |
| 73 | 74 | 73 | 74 | 63 | 64 | 68 | 69 |
| 69 | 68 | 71 | 72 | 67 | 58 | 48 | 41 |
| 59 | 55 | 56 | 52 | 47 | 40 | 24 | 9 |
| 51 | 50 | 45 | 41 | 33 | 22 | 7 | -5 |
| 43 | 37 | 32 | 24 | 15 | 5 | -6 | -25 |
| 29 | 21 | 9 | -2 | -10 | -21 | -44 | -69 |
| 9 | -4 | -17 | -35 | -52 | -61 | -57 | -35 |

Fig. 3.1: 8x8 block before DCT

| | | | | | | | |
|-----|-----|-----|-----|----|----|----|----|
| 251 | 118 | -13 | 6 | -2 | 6 | -1 | 0 |
| 279 | -68 | -8 | -7 | -1 | 4 | -4 | -1 |
| -51 | -14 | 34 | -14 | 5 | 0 | -1 | 0 |
| 27 | 5 | -10 | 8 | -7 | 4 | -5 | 1 |
| -22 | -7 | 14 | -9 | 4 | -2 | 1 | 1 |
| -3 | 15 | -18 | 15 | -6 | 2 | -1 | 2 |
| 7 | -9 | 6 | -6 | 4 | 0 | 0 | 2 |
| 3 | 7 | -9 | 3 | 0 | -2 | -1 | 0 |

Fig. 3.2: 8x8 block after DCT

As shown in following fig. 3.3 higher transform coefficients of DCT are concentrated on the top left corner and small amount of low frequency coefficients dominates over rest coefficients [18]. So low frequency coefficients are having advantage over higher one. Because of this the reducing of data does not affect more.

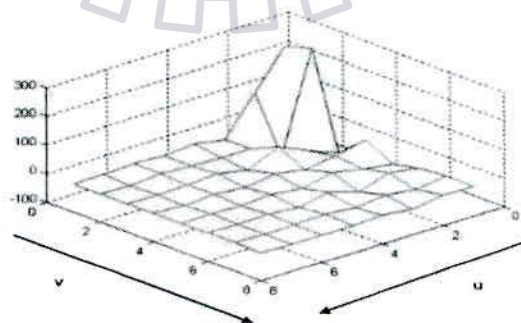


Fig. 3.3: Frequency map

In blind DCT watermarking the host image is segmented in to blocks of same size [18]. DCT based algorithm transforms every block in different coefficients matrix. After modification in coefficients, the inverse DCT is taken and combining all blocks produces the watermarked image [14 18].

3.4.1 Watermark Embedding

Steps:

1. Host image is segmented in to non overlapping blocks.
2. Perform DCT to each block of host image.
3. Select two mid frequency pixels in each block. Let we select (5, 2) & (4, 3) positions from each block. These two coefficients will be the secret key.
4. Modify these DCT coefficients to satisfy the following equations
 If message bit = 1, then $\text{Pixel}(5, 2) - \text{pixel}(4, 3) \geq k$... (3.6)
 If message bit = 0, then $\text{Pixel}(4, 3) - \text{pixel}(5, 2) \geq k$... (3.7)
 Here k is gain factor
5. Apply inverse DCT to each block and combine all blocks to get the watermarked image.

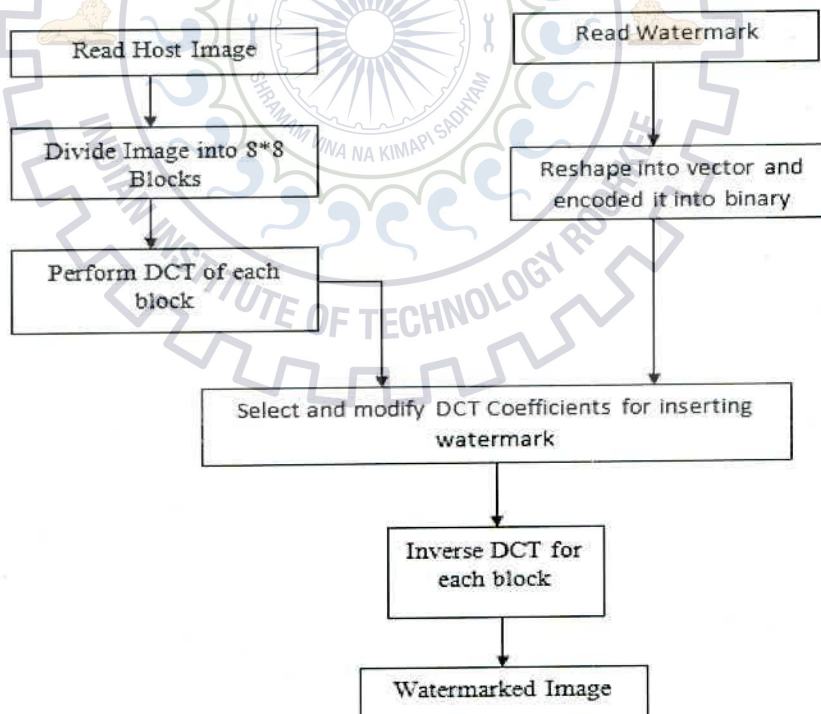


Fig. 3.4: Block diagram of DCT based watermark embedding

3.4.2 Watermark Extraction

Steps:

1. Divide the watermarked image into non over-lapping blocks.
2. Perform DCT to each block.
3. Extract the watermark from same coefficients, here embedding was done in pixel (5, 2) and (4, 3).
If pixel (5, 2) > pixel (4, 3) Then message = 0
Else message = 1
4. Reshape the recovered message to get watermark.

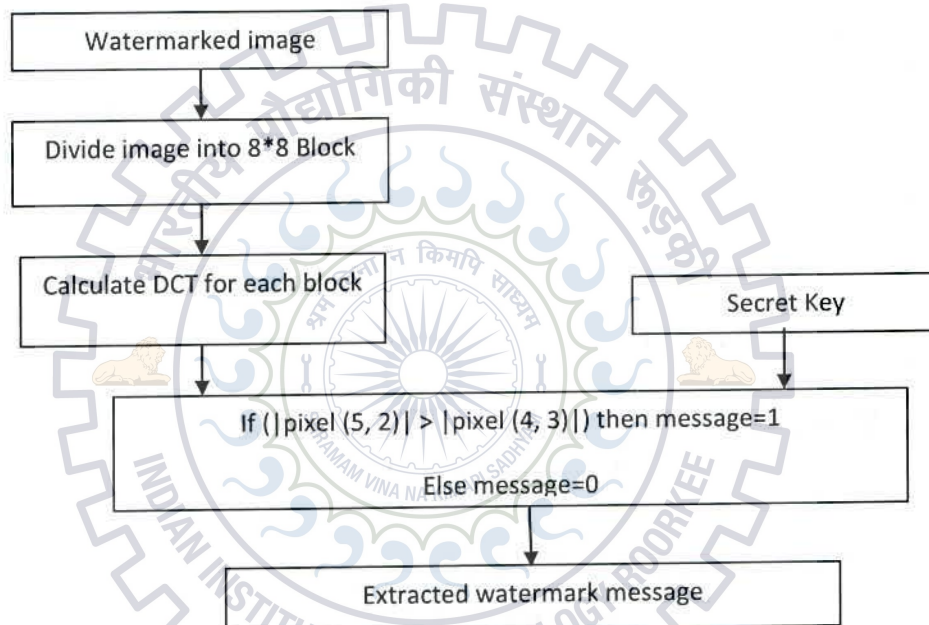


Fig. 3.5: Block diagram of DCT based watermark extraction

3.5 Discrete Wavelet Transform (DWT) Based Watermarking

There are many advantages of using discrete wavelet transform over DCT and other earlier transform based watermarking. At high compression ratio DCT produces blocking artifacts this problem is overcome using DWT algorithm. The DWT exploits the image in to spatial and frequency information and provides multi resolution description of the image. It separates an image into a lower resolution approximation image (LL) as well as horizontal

(HL), vertical (LH), and diagonal (HH) detail components. It makes DWT as more accurate model aspects for human visual system (HVS) as compared to the FFT or DCT. Higher energy watermark can be embedded in the region which is less sensitive for HVS such as high resolution detail bands (HH, HL, and LH). This improves the robustness of the watermark without affecting the quality of watermark image [17].

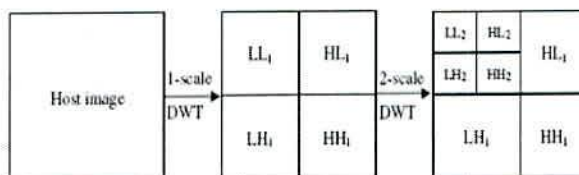


Fig. 3.6: 2D DWT decomposition of an image

To embed the watermark image first of all watermark image is converted in to bits. Host image is decomposed using the 1-level DWT algorithm into sub bands LL, LH, HL, and HH. Two PN sequence of the size of sub bands are taken. Using a gain factor these PN sequences are added with the LH and HL component. Inverse DWT operation is taken to get watermarked image. At the extraction algorithm same PN sequences are used which act as a secret key. From correlation between the PN sequence and watermarked image message bits are recovered and reshaped to get watermark image [20].

3.5.1 Watermark Embedding

Steps:

1. Decompose original image using 1- level DWT into sub bands LL, HL, LH and HH.

2. The dimension of PN sequence should be same as dimension of sub bands. Dimension of sub bands are found using dimension of watermark image.

3. Add pn sequence to the LH and HL components when message $m(k)=0$

$$W_i = W_i + \alpha * \text{PN sequence} \quad \dots\dots(3.8)$$

Where W_i is the image coefficients and ' α ' is the gain factor.

Here PN- sequence is used as watermarking coding. Same PN-sequence is required in watermarking detection.

4. Perform IDWT to produce watermarked image.

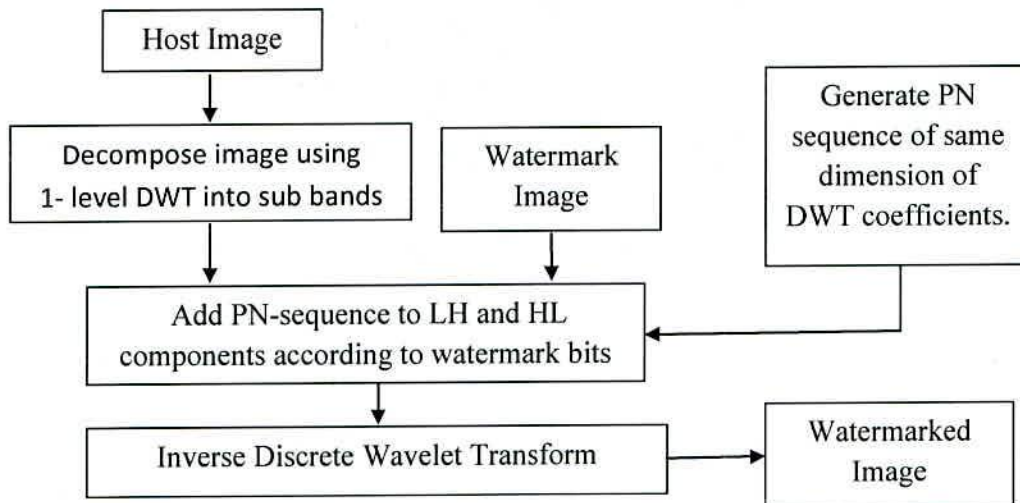


Fig. 3.7: Block diagram of DWT based watermark embedding

3.5.2 Watermark Extraction

Steps:

1. Determine the size of watermarked image and watermark message.
2. Initialize message vector to all '1' which has same dimension as original message.
3. Decompose watermarked image into sub bands LL, LH, HL and HH using 1 level DWT.
4. To detect the watermark we generate the same pseudo-random sequence (pn sequence) which is used in embedding and determine its correlation with two transformed detail bands LH and HL.
5. If the correlation exceeds threshold (mean of correlations) then "1" is recovered otherwise "0".
6. Reshape the recover bits to get watermark.

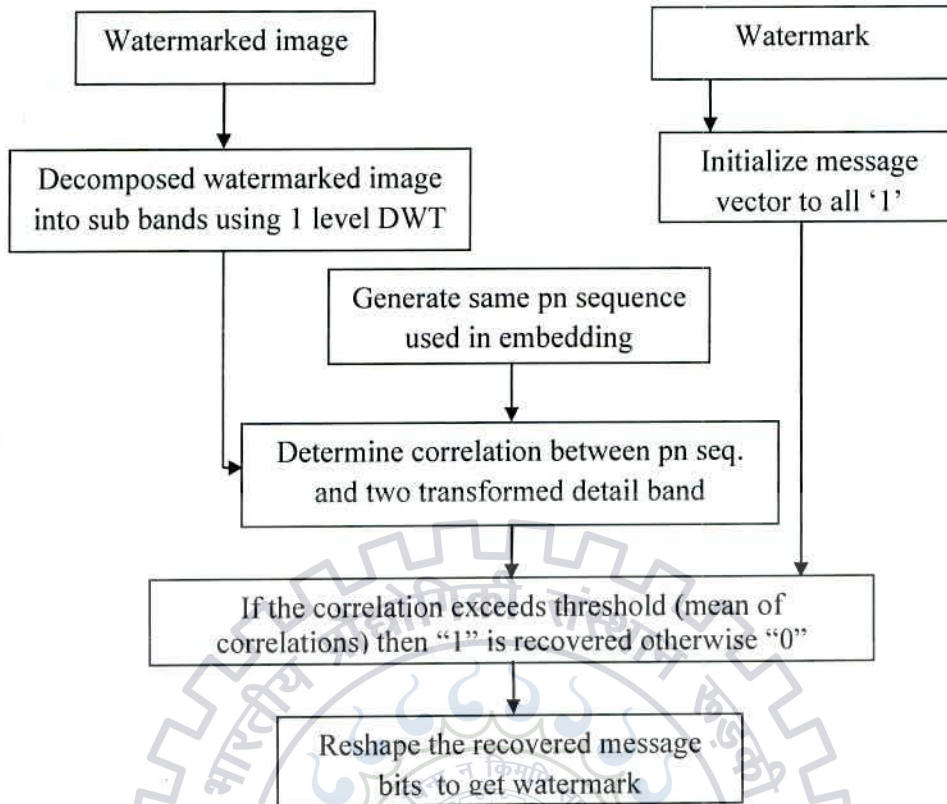


Fig. 3.8: Block diagram of DWT based watermark extraction

3.6 Singular Value decomposition (SVD) Based Watermarking

Singular value decomposition is an algorithm to analyze the image matrix. It converts image in to three different metrics [21]. It is a kind of orthogonal transform used for matrix analysis. The SVD of image I_m can be describe as

$$I_m = HSV^T \quad \dots(3.9)$$

$$I_m = \begin{bmatrix} h_1 & h_2 & \dots & h_N \end{bmatrix} \begin{bmatrix} s_1 & & & \\ & s_2 & & \\ & & \dots & \\ & & & s_N \end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \\ \dots \\ v_N \end{bmatrix}^T \quad \dots (3.11)$$

I_m is the image matrix. H and V are two $M \times N$ and $N \times N$ unitary orthogonal matrices, and S is an $N \times N$ diagonal matrix [22]. Where the horizontal detail component of image I_m is represented by H matrix and vertical detail component of the image I_m is represented by V . Both V and H are orthogonal matrices and S is a singular matrix which consists of singular

values. Singular values in S matrix are arranged diagonally and in decreasing order. One of the important properties of SVD is stability which means small variation in the singular values does not affect the watermark image [23]. This makes SVD algorithm much robust than other transform based algorithm.

After dividing the host image in to blocks, each block of host image is transformed using SVD. Singular values of singular diagonal matrix are modified according to the message bits. Two random sequences for two binary digits '1' and '0' are added to singular values with a gain factor. After modifying singular values, inverse process of the SVD is taken to generate watermarked image. At the extraction algorithm correlation between stored singular values (SVs) and modified singular values (SVs) are found. Using this, message bits are recovered and reshaped in to the watermark image.

3.6.1 Watermark Embedding

Steps:

1. Host image is segmented into 8x8 blocks
2. Apply SVD to each block, and obtain H, V and S matrix
SVD of host image = HSV^T
3. Modify singular matrix S, according to the watermark image using two random sequence and a gain factor α , $S_1 = S + \alpha(\text{rand sequence})$ (3.11)
4. SVD of modified singular matrix = $H_1 S_1 V_1^T$.
5. Using inverse SVD process obtain watermarked image according to $HS_1 V^T$.

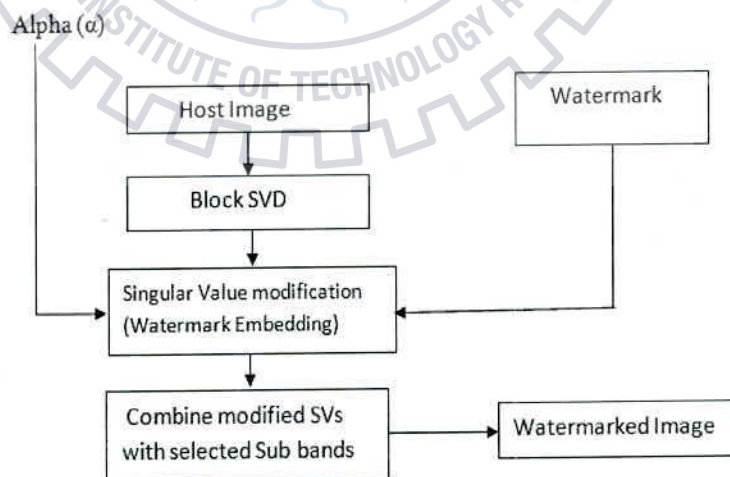


Fig. 3.9: Block diagram of SVD based watermark embedding

3.6.2 Watermark Extraction

Steps:

1. Watermarked image is segmented in to 8x8 blocks.
2. Apply SVD to every 8x8 block of watermarked image.
3. Using SVD obtain H^* , V^* and $S1^*$ matrix to get modified singular values $s1$ matrix
$$s1 = H^* S^* V^{*T}$$
4. From the stored value of $H1$ $V1$ and $S1^*$, take the inverse process of SVD to get stored singular values.
5. Take the difference from the modified and stored SVs to get the new sequence
6. From the correlation between rand sequences and this new sequence the message bits are extracted.
7. Extracted bits are reshaped to get watermark image.

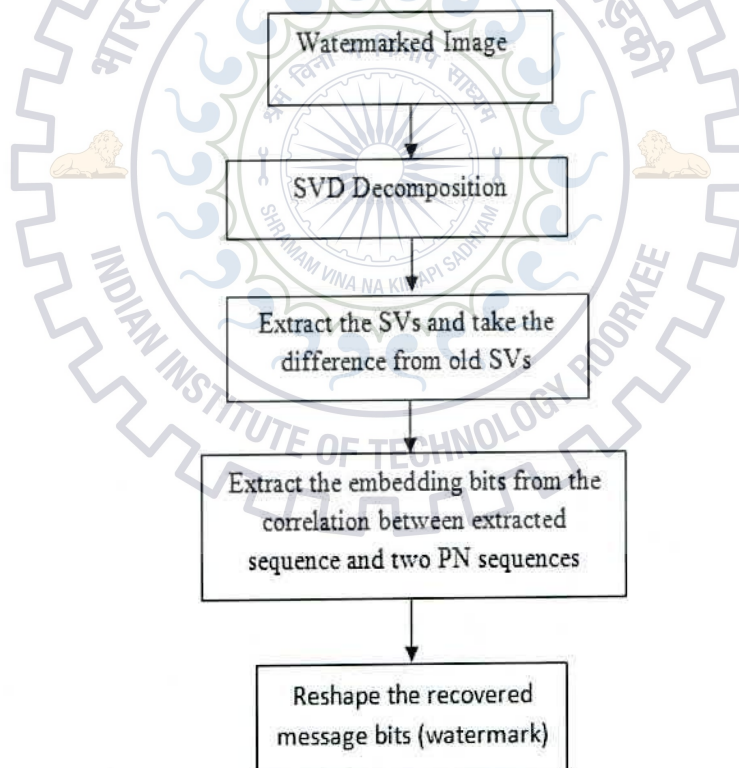


Fig. 3.10:Block diagram of SVD based watermark extraction

3.7 Different Noise and Attacks

To evaluate the performance of the watermarking algorithms different noise and attacks are applied to the watermarked image. These are described below.

3.7.1 Signal Processing Attacks

Salt and pepper attack represents itself as randomly occurring black and white pixels. An image containing salt-and-pepper noise will have bright pixels in dark regions and dark pixels in bright regions [31]. Poisson noise creates Poisson noise from the data itself instead of adding artificial noise to the data. Speckle noise is a granular and multiplicative noise that inherently exists in and degrades the image quality. Median Filter is a non linear spatial filter which is usually used to remove noise/spikes from an image [32]. Here 3x3 mask median filter is used to attack watermark.

3.7.2 Geometric Attacks

Image rotation, scaling shifting cropping comes in the category of geometric attacks. In image rotation, image is rotated by an angle in degrees either in a clockwise or anticlockwise direction, around the center point. Intensity variation operation maps the new intensity value to gray scale watermarked image. Image cropping operation cut some portion of watermarked image [32]. Here the watermarked image is cut from the four sides and cropped image is given to the extraction algorithm.

3.7.3 JPEG Compression

This operation compresses the watermarked image. Less percentage means most compression and more degraded watermarked image. JPEG compressing is used to increase the capacity of watermarking algorithm [33]. JPEG compression can be applied with different quality factor which shows different compression value.

3.8 Experimental Results and Discussion

In different watermarking algorithm (discussed above), variation in PSNR and robustness with respect of different noise and attacks are shown by the chart in Fig. 3.11 and

Fig. 3.12 respectively. In spatial domain Correlation based method gives better watermark image than LSB based algorithm. Transform domain algorithms performs better than spatial domain. Noisy/Attacked watermarked images, extracted watermark images, and different parameters of different algorithms are shown in table.3.1 and table 3.2, which shows that extracted watermark image from SVD based algorithm is of higher PSNR and better robustness among all performed algorithms.

Table 3.1: Comparison of extracted watermarks from different watermarking algorithm

| SN | Attacks | Digital Image Watermarking | | | | | | | | | |
|----|---------------------|----------------------------|------|-------------------|------|-----------|------|-----------|------|-----------|------|
| | | LSB based method | | correlation based | | DCT based | | DWT based | | SVD based | |
| | | PSNR | NC | PSNR | NC | PSNR | NC | PSNR | NC | PSNR | NC |
| 1 | No attack | 20.99 | 1 | 36.12 | 1 | 36.12 | 1 | 36.12 | 1 | 36.12 | 1 |
| 2 | Salt & pepper noise | 18.87 | 0.99 | 18.42 | 0.99 | 15.75 | 0.97 | 7.69 | 0.89 | 28.34 | 1 |
| 3 | Gaussian noise | 2.95 | 0.49 | 15.95 | 0.98 | 9.89 | 0.89 | 15.22 | 0.97 | 36.12 | 1 |
| 4 | Poisson noise | 3.01 | 0.5 | 24.36 | 1 | 23.57 | 1 | 3.01 | 0.5 | 36.12 | 1 |
| 5 | Speckle noise | 3 | 0.5 | 23.34 | 1 | 19.13 | 0.99 | 7.64 | 0.88 | 36.12 | 1 |
| 6 | Median filter noise | 20.78 | 1 | 6.92 | 0.78 | 21.5 | 0.99 | 3.01 | 0.5 | 27.67 | 1 |
| 7 | Image rotation | 2.63 | 0.45 | 2.25 | 0.38 | 3.39 | 0.55 | 2.92 | 0.49 | 10.31 | 0.9 |
| 8 | JPEG comp. (Q=8) | 2.29 | 0.39 | 14.33 | .96 | 13.22 | .96 | 14.72 | .96 | 8.31 | 0.88 |
| 9 | Image Cropping | 3.74 | 0.59 | 3.29 | 0.53 | 3.1 | 0.51 | 3.11 | 0.5 | 16.53 | 0.98 |

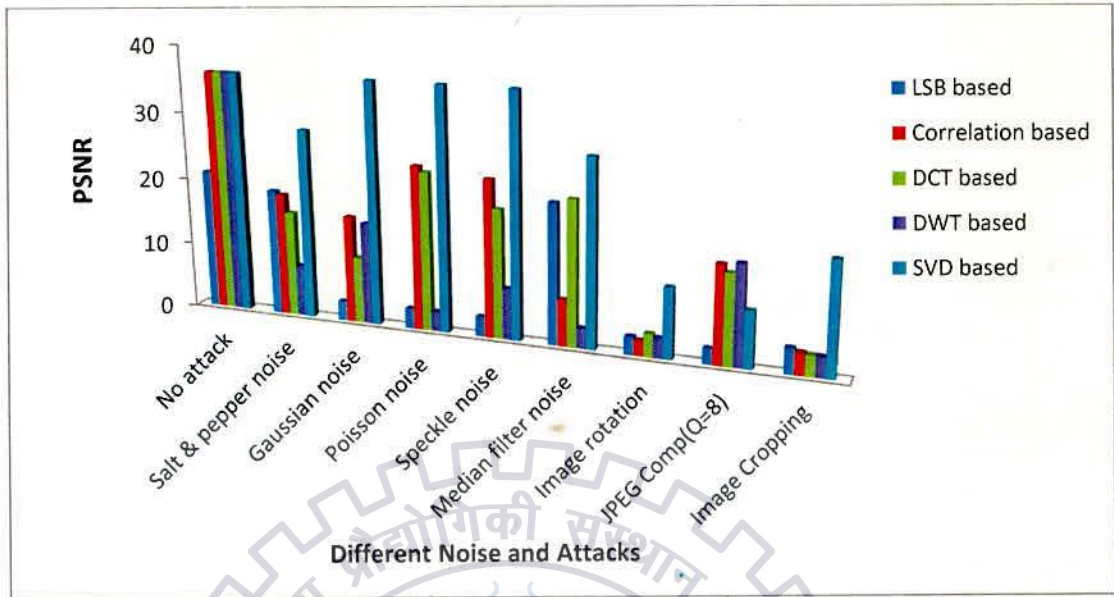


Fig. 3.11: PSNR variation of extracted watermark images of different watermarking algorithms against different noise/attacks

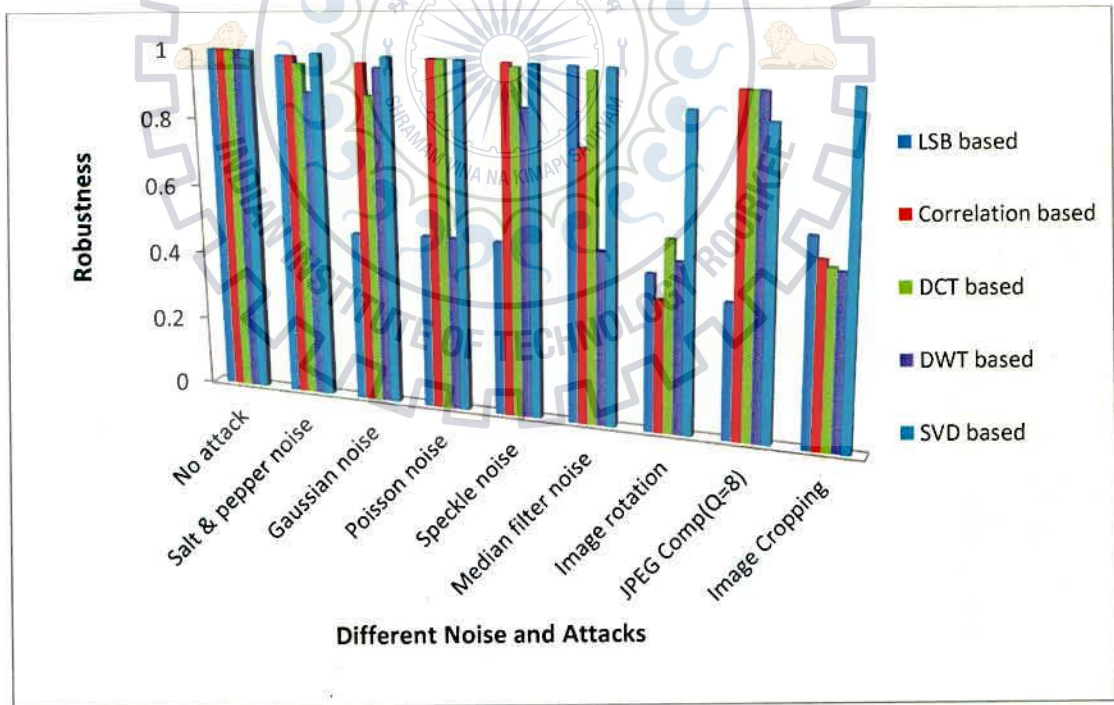





































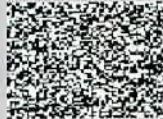



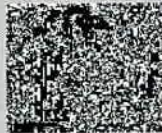



















Fig. 3.12: Robustness variation of extracted watermark images of different watermarking algorithms against different noise/attacks

Table 3.2: Extracted watermark Images of different watermarking methods against different attacks

| S N | Type of Noise/ Attack | Digital Image Watermarking | | | | |
|--------|-----------------------------|--|--|--|--|--|
| | | LSB based | Correlation based | DCT based | DWT based | SVD based |
| 1. | No attack | watermarked image psnr=50.12 | watermarked image psnr=21.66 | watermarked image psnr=31.74 | watermarked image psnr=20.05 | watermarked image psnr=29.44 |
| | | recovered watermark nc=1.00, psnr=20.99 | recovered watermark nc=1.00, psnr=36.12 | recovered watermark nc=1.00, psnr=36.12 | recovered watermark nc=1.00, psnr=36.12 | recovered watermark nc=1.00, psnr=36.12 |
| | | TAR | TAR | TAR | TAR | TAR |
| 2. | Salt & Pepper attack | watermarked image psnr=24.18 | watermarked image psnr=19.83 | watermarked image psnr=23.44 | watermarked image psnr=18.72 | watermarked image psnr=23.08 |
| | | recovered watermark nc=0.99, psnr=18.87 | recovered watermark nc=0.99, psnr=18.42 | recovered watermark nc=0.97, psnr=15.75 | recovered watermark nc=0.89, psnr=7.69 | recovered watermark nc=1.00, psnr=28.34 |
| | | TAR | TAR | TAR | TAR | TAR |
| 3. | Gaussian noise | watermarked image psnr=19.05 | watermarked image psnr=17.26 | watermarked image psnr=18.86 | watermarked image psnr=16.63 | watermarked image psnr=18.74 |
| | | recovered watermark nc=0.49, psnr=2.95 | recovered watermark nc=0.98, psnr=15.95 | recovered watermark nc=0.89, psnr=9.89 | recovered watermark nc=0.97, psnr=15.22 | recovered watermark nc=1.00, psnr=36.12 |
| | | TAR | TAR | TAR | TAR | TAR |

| | | | | | | |
|----|---------------------|---|--|---|--|---|
| 4. | Poisson noise | watermarked image psnr=26.28  recovered watermark nc=0.50, psnr=3.01  | watermarked image psnr=20.39  recovered watermark nc=1.00, psnr=24.36  | watermarked image psnr=25.24  recovered watermark nc=1.00, psnr=23.57  | watermarked image psnr=19.15  recovered watermark nc=0.50, psnr=3.01  | watermarked image psnr=24.63  recovered watermark nc=1.00, psnr=36.12  |
| 5. | Speckle noise | watermarked image psnr=24.72  recovered watermark nc=0.50, psnr=3.00  | watermarked image psnr=19.94  recovered watermark nc=1.00, psnr=23.34  | watermarked image psnr=23.97  recovered watermark nc=0.99, psnr=19.13  | watermarked image psnr=18.82  recovered watermark nc=0.88, psnr=7.64  | watermarked image psnr=23.47  recovered watermark nc=1.00, psnr=36.12  |
| 6. | Median filter noise | watermarked image psnr=33.96  recovered watermark nc=1.00, psnr=20.78  | watermarked image psnr=29.63  recovered watermark nc=0.78, psnr=6.92  | watermarked image psnr=32.85  recovered watermark nc=0.99, psnr=21.50  | watermarked image psnr=27.31  recovered watermark nc=0.50, psnr=3.01  | watermarked image psnr=32.05  recovered watermark nc=1.00, psnr=27.67  |
| 7. | Image rotation | watermarked image psnr=9.47  recovered watermark nc=0.45, psnr=2.63  | watermarked image psnr=9.41  recovered watermark nc=0.38, psnr=2.25  | watermarked image psnr=9.47  recovered watermark nc=0.55, psnr=3.39  | watermarked image psnr=9.37  recovered watermark nc=0.49, psnr=2.92  | watermarked image psnr=9.43  recovered watermark nc=0.90, psnr=10.31  |

| | | | | | | |
|----|------------------------|---|---|---|---|--|
| 8. | JPEG comp. (Q=8) | watermarked image psnr=31.97  recovered watermark nc=0.39, psnr=2.29  | watermarked image psnr=25.38  recovered watermark nc=0.96, psnr=14.33  | watermarked image psnr=28.69  recovered watermark nc=0.96, psnr=13.22  | watermarked image psnr=11.36  recovered watermark nc=0.96, psnr=14.72  | watermarked image psnr=31.76  recovered watermark nc=0.88, psnr=8.31  |
| 9. | Image cropping | watermarked image psnr=11.80  recovered watermark nc=0.59, psnr=3.74  | watermarked image psnr=11.48  recovered watermark nc=0.53, psnr=3.29  | watermarked image psnr=11.78  recovered watermark nc=0.51, psnr=3.10  | watermarked image psnr=11.36  recovered watermark nc=0.51, psnr=3.11  | watermarked image psnr=11.66  recovered watermark nc=0.98, psnr=16.53  |

3.9 Comparison among Different Watermarking Techniques

In case of LSB based watermarking the visual quality of watermarked image does not change significantly because watermark bits only change the least significant bit of the pixels. It means embedding watermarking in LSB technique is quite imperceptible. On the other hand this algorithm is not robust against signal manipulation, geometric attack, or JPEG compression.

Correlation based technique does not impact on the visual quality if gain factor is kept small and noise pattern does not contain large values. This algorithm is more robust than LSB based algorithm against Gaussian noise, salt & pepper noise. But translation, rotation, scaling, cropping, median filter noise affect the obtained correlation values and caused the watermark to be destroyed.

In DCT based algorithm the visual quality of watermarked image is not affected if gain factor is kept low. Greater the value of gain factor guarantees more robustness of

watermark image but perceptual quality of the watermarked image decreases. So there is tradeoff between the quality of watermarked image and robustness of extracted watermark.

In DWT method, a scaling factor α is used. If α increases then the strength of message in watermarked image increases i.e. the quality of watermark message increases and for watermarked image it decreases with increasing in α . Disadvantage of DWT based algorithm is computational complexity. And not fast as compared to DCT.

Due to the property of SVD, SVD based watermarking has dominated over all transform based algorithm. One of the important properties of SVD is stability which means small variation in the singular values does not affect the watermark image. This makes SVD algorithm much robust than other transform based algorithm. Imperceptibility of this algorithm is also good.

3.10 Conclusions

In this chapter, five algorithms of spatial domain and transform domain are implemented using MATLAB. For comparison purpose, host and watermark image are kept same for all algorithms. These algorithms are examined after inserting the different noise and attacks in watermarked image at extraction algorithm.

LSB based watermarking performs well in case of Poisson and speckle attack which affects less in the watermarked image spatially. In transform domain algorithm the watermark bits are inserted after transforming the image using any of transform method. So noise and attacks affect less unlike spatial domain algorithm. In transform domain algorithms, DWT provides multi resolution description of an image and gives better result than DCT based algorithm without blocking artifacts. The advantage of DCT algorithm is that it is much robust against JPEG compression of image. It means DCT algorithm is suitable where large capacity data is transferred. And another advantage is that this is fast algorithm. On the other hand DCT based algorithm gives poor results in case of geometric attacks.

SVD based algorithm extracts more robust and good quality watermark image than DCT, DWT based algorithm. In case of geometric attacks like image rotation and scaling SVD based algorithm is able to extract watermark image unlike other algorithms. This is due to the stability, flipping and transpose etc. properties of SVD.

Chapter 4

Multiple Images Watermarking

4.1 Introduction

In many applications of digital image watermarking, watermarked image of good quality is required. But there is a tradeoff between number of embedded watermark images and quality of watermarked image. This aspect is quite important in case of multiple digital image watermarking. The advantage of multiple image watermarking is that we can send more data related with a digital content like name of creator, recipient, status etc. In case of multiple images watermarking, singular value decomposition based watermarking algorithm performs much better than other transform based methods. This chapter presents a robust multiple digital images watermarking using singular value decomposition (SVD) method. The results are compared with Discrete Cosine Transform (DCT) based multiple images watermarking method. In case of multiple images DCT based watermarking or in other transform based method more coefficients are varied according to the more watermark images which degrade the quality of watermarked image. In case of SVD image watermarking method only singular values are being varied either in single or multiple image watermarking. This helps in preserving the quality of watermarked image.

4.2 DCT Based Multiple Images Watermarking

Discrete cosine transform (DCT) is a very useful method for image processing which converts the image in to different frequency coefficients [5]. In blind multiple images DCT watermarking the host image is segmented in to multiple blocks of same size [18] then each block is transformed using DCT. Message bits are embedded as coefficient modification. In case of more watermarking images more coefficients are varied. Here four coefficients are modified for two watermark image as shown in fig. 4.2. High frequency coefficients are more sensitive to image processing attacks and low frequency coefficients are having visual effect so mid frequency coefficients are selected for embedding the watermark message.

These selected coefficients work as secret key, without knowing that one cannot extract watermark. After modification in coefficients the inverse DCT is taken to produce the watermarked image [18]. At extraction part, watermarked image is segmented in blocks and DCT is applied to every block. From known values of coefficients, message bits are recovered and reshaped in to watermark image.

4.2.1 Watermark Embedding

Steps:

1. Read the host image and determine the size of it. Find the maximum possible message size which can be embedded.
2. Determine the size of both watermark images and convert both watermarks in to bits stream.
3. If the numbers of message bits are more than the maximum message size we should display a warning that the message is too large to embed. If the numbers of message bits are less, then we pad the remaining by 1.
4. Divide the host image of size $M \times N$ into non over-lapping blocks.
5. Perform DCT to each block.
6. Select two mid frequency coefficients in each block (5, 2) & (4, 3) for first watermark and another two (5, 3) & (6, 2) for second watermark. These selections behave as secrete key.
7. Modify these DCT coefficients to satisfy the following equations

For first watermark

If message bit = 1, then Pixel (5, 2) - pixel (4, 3) \geq k (4.1)

If message bit = 0, then Pixel (4, 3) - pixel (5, 2) \geq k (4.2)

For second watermark

If message bit = 1, then Pixel (6, 2) - pixel (5, 3) \geq k (4.3)

If message bit = 0, then Pixel (5, 3) - pixel (6, 2) \geq k (4.4)
8. Apply inverse DCT to each block.
9. Combine all blocks to get the watermarked image.

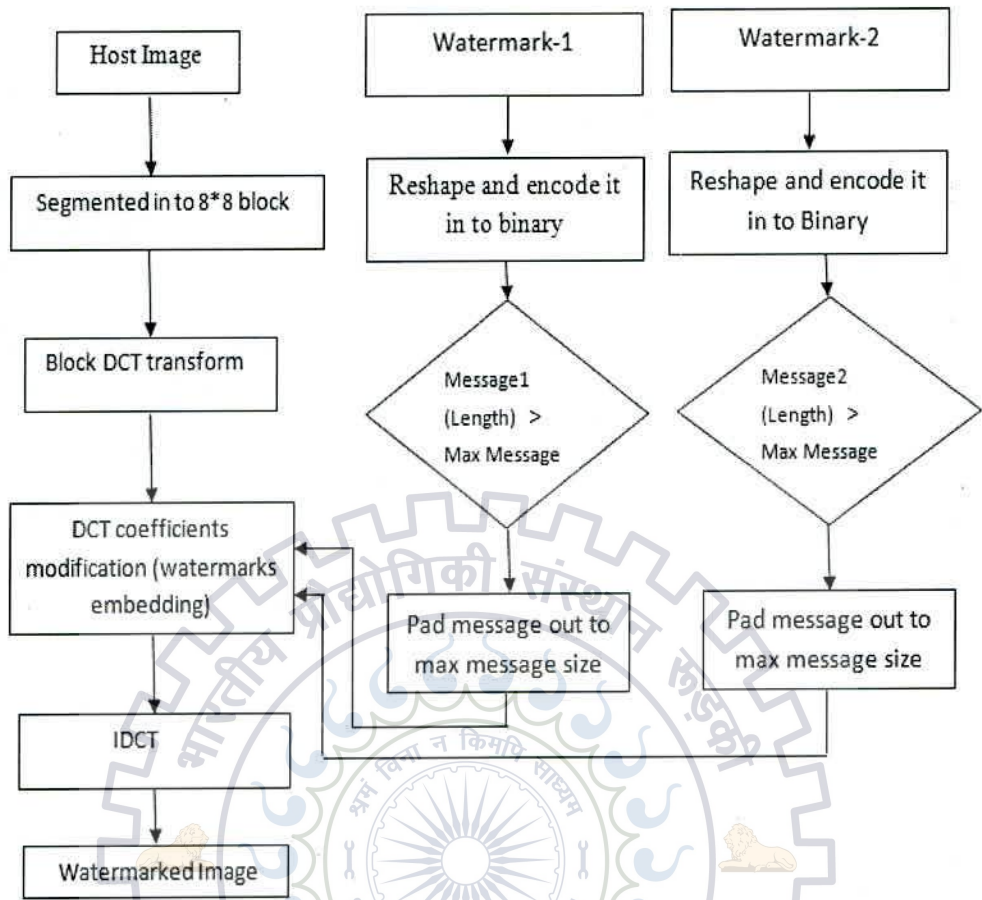


Fig. 4.1: DCT based multiple watermarks embedding

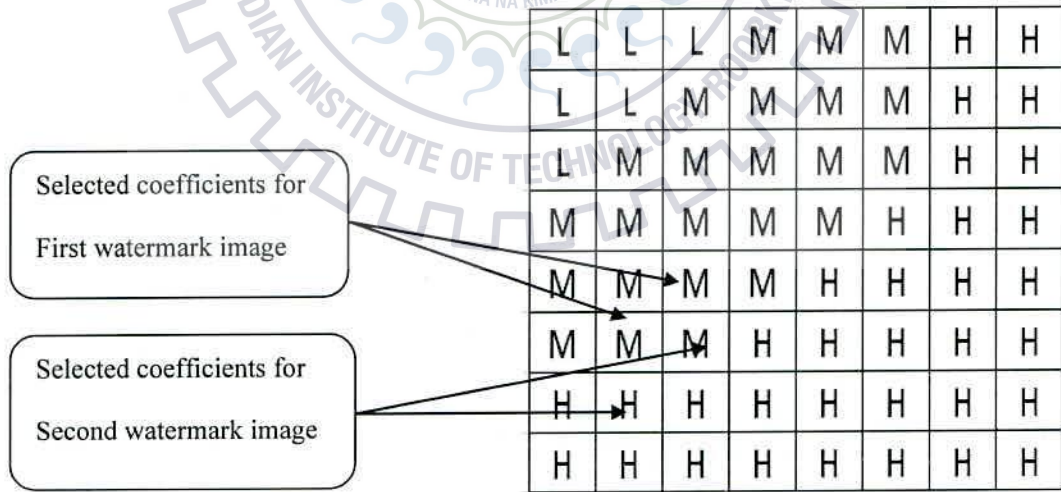


Fig. 4.2: Selected coefficients for two watermarks in a DCT block of the host image

4.2.2 Watermark Extraction

Steps:

1. Divide the watermarked image of size $M \times N$ into non over-lapping blocks
2. Perform DCT to each block.
3. Extract the first and second watermark from the known values of coefficients for first watermark.

If pixel (5, 2) > pixel (4, 3) then message = 1

Else message = 0

For second watermark

If pixel (6, 2) > pixel (5, 3) then message = 1

Else message = 0

4. Reshape both recovered both message bits to get first and second watermark.

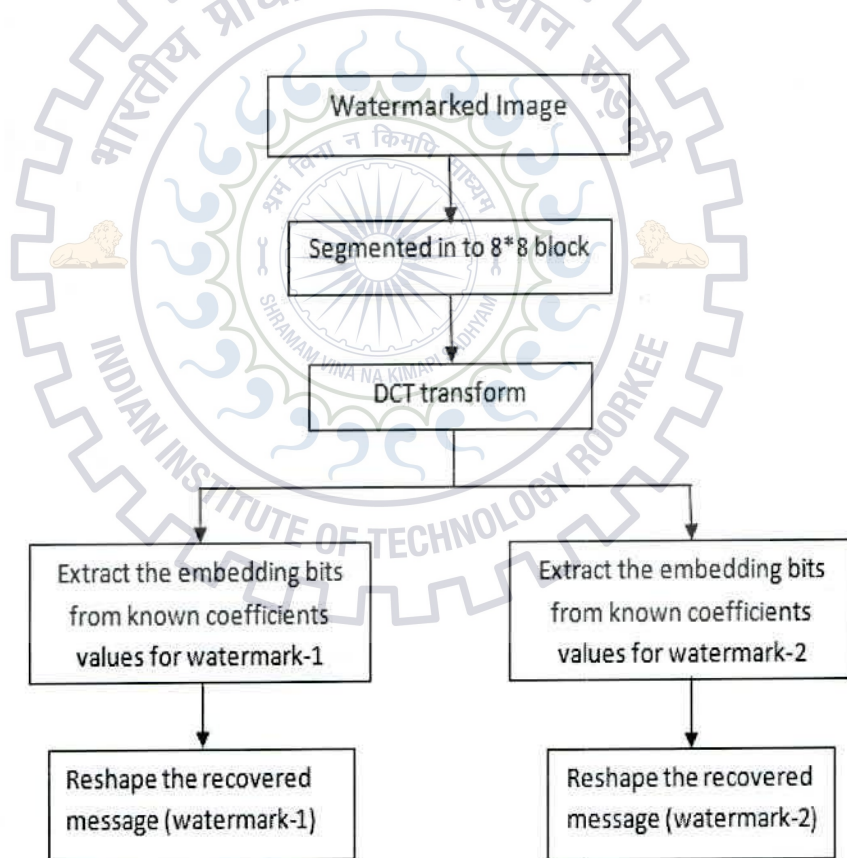


Fig. 4.3: DCT based multiple watermarks extraction

4.3 SVD Based Multiple Images Watermarking

Singular value decomposition is very useful for image processing. This is a numerical technique to analyze the image matrix which converts image in to three different metrics [24]. The SVD of image I_m can be described as

$$I_m = HSV^T$$

I_m is the image matrix. H and V are two $M \times N$ and $N \times N$ unitary orthogonal matrices, and S is an $N \times N$ diagonal matrix [23]. Where H represents the horizontal detail component of image I_m and V represents the vertical detail component of image I_m . Both H and V are orthogonal matrices and S is a singular matrix which consists of singular values. Singular values in S matrix are arranged diagonally and in decreasing order. One of the important properties of SVD is that a little change in the singular values does not affect the quality of watermark image [25]. Due to the property of SVD, SVD algorithm produces more robust watermark [26].

After dividing the host image in to blocks the SVD is applied to each block. Two watermark images are embedded in the form of singular values modification. For this purpose different random sequence for different bit of every watermark image is added to singular values with a gain factor. For this purpose four random sequences are required. After modifying singular values we take inverse of the SVD process to produce watermarked image. At extraction part SVD is applied to watermarked image. From the correlation between stored singular values and modified singular values message bits are recovered and reshaped in to watermark image.

4.3.1 Watermark Embedding

Steps:

1. Read the host image and determine the size of it. Find the maximum possible message size which can be embedded.
2. Determine the size of both watermark images and convert both watermarks in to bits stream.
3. If the numbers of message bits are more than the maximum message size we should display a warning that the message is too large to embed. If the numbers of message bits are less, then we pad the remaining by 1.

4. Divide the host image of size $M \times N$ into non over-lapping blocks.
5. Perform SVD to each block.
6. Generate the four random sequences (different sequence for different message) and multiply it with a known value of gain factor and add to S matrix to modify the singular values of s matrix.

message1= 0 for $i=1:4$

$$s1(i,j)=s(i,j)+\alpha*\text{sequence1} \quad \dots (4.5)$$

$$\text{Otherwise } s1(i,j)=s(i,j)+\alpha*\text{sequence2} \quad \dots (4.6)$$

message2= 0 for $i=5:8$

$$s1(i,j)=s(i,j)+\alpha*\text{sequence3} \quad \dots (4.7)$$

$$\text{Otherwise } s1(i,j)=s(i,j)+\alpha*\text{sequence4} \quad \dots (4.8)$$

7. Combine modified singular values matrix with selected matrix to generate watermarked image.

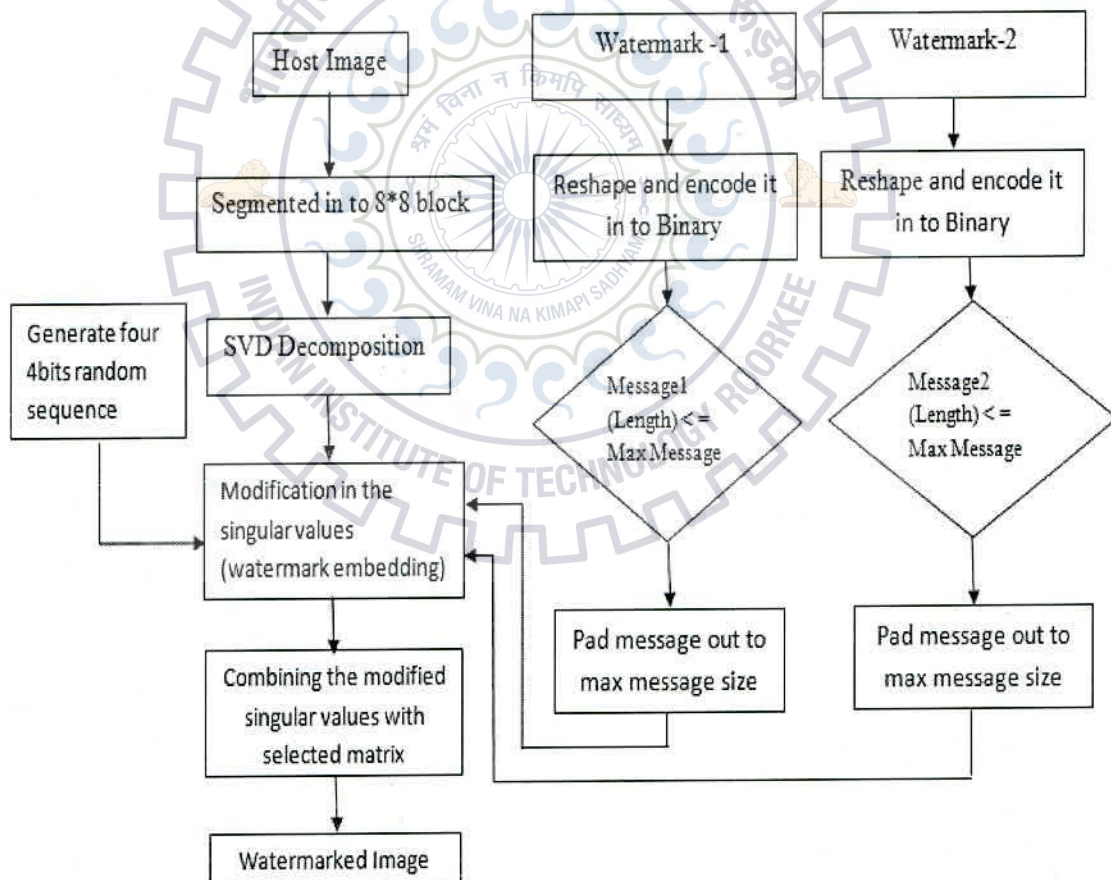


Fig. 4.4: SVD based multiple watermarks embedding

4.3.2 Watermark Extraction

Steps:

1. Read the watermarked image and determine the size of it.
2. Divide the input image of size $M \times N$ into 8×8 blocks.
3. Perform SVD to each block.
4. Extract the sequence from the difference between modified SVs and stored SVs.
5. Extract the first message bits using the correlation between first two sequences and extracted new sequence. Similarly second message bits are extracted using the correlation between other two sequences and extracted sequence.
6. Reshape the recovered both message bits to get first and second watermark.

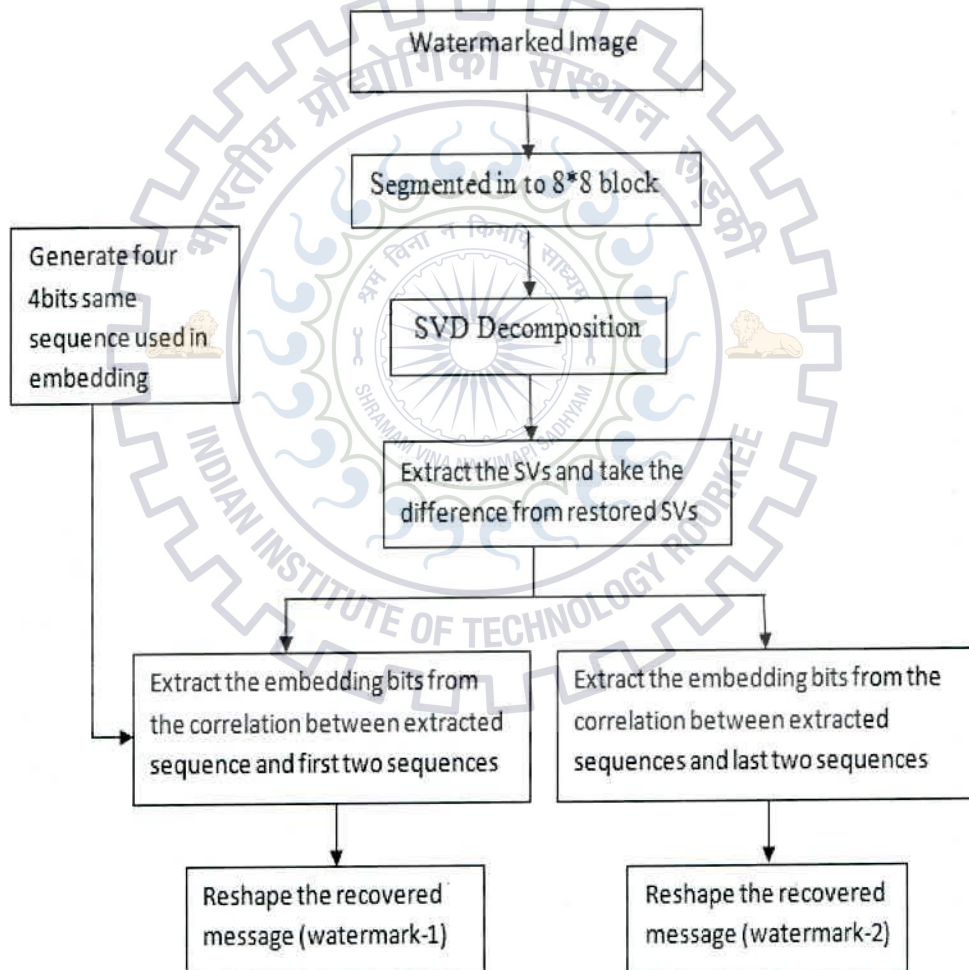


Fig. 4.5: SVD based multiple watermarks extraction

4.4 Experimental Results and Discussion

4.4.1 DCT Based Multiple Images Watermarking

For single and multiple image watermarking the values of accuracy rate (AR), PSNR and normalized correlation (NC) with respect to gain factor k , are shown in Table 4.1. This shows that for the same value of k , PSNR of the watermarked image in single image watermarking is more than the PSNR of watermarked image in multiple images watermarking because more coefficients are varied in multiple images watermarking which degrades the quality of watermarked image. While PSNR of watermark images depends on the selected coefficients in which watermark bits are embedded. Two different watermarks embedding and extraction using DCT algorithm are shown in Fig.4.6. Where gain factor is kept same for both images.

PSNR variation of watermarked images in case of single and multiple images watermarking with respect of gain factor k are shown through graph in fig.4.7, this shows that for same value of k , watermarked image-1 for single image DCT based watermarking is having higher PSNR value than the watermarked image-2 of multiple images DCT based watermarking.

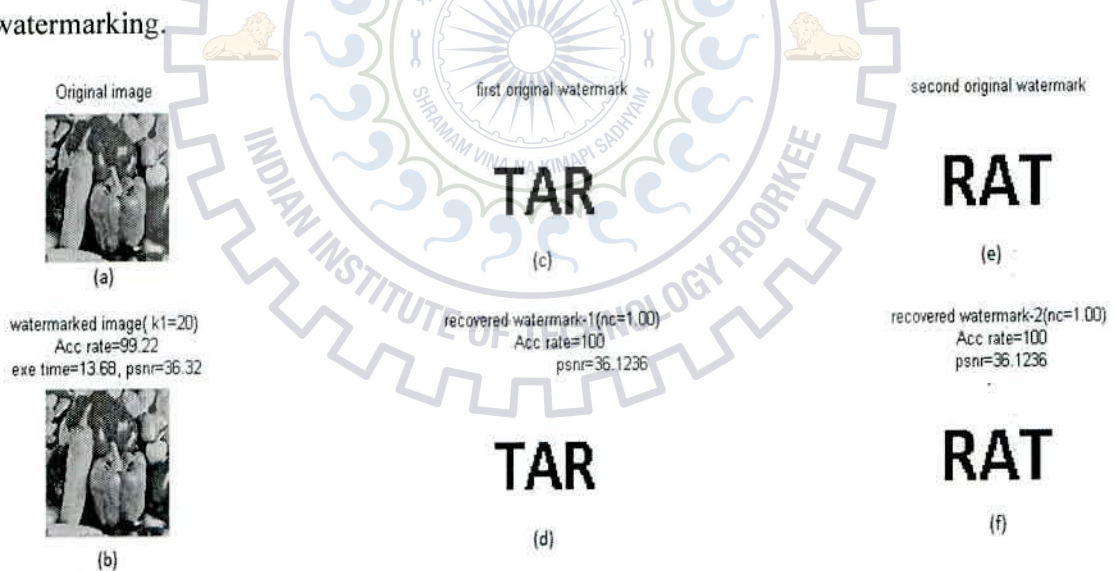


Fig. 4.6: DCTbased multiple images watermarking,

- (a) Host image (b) Watermarked image(c) First watermark (d) First recovered watermark
(e) Second watermark, (f) Second recovered watermark

Table 4.1: DCT based single image and multiple images watermarking

| k | DCT single image watermarking | | | | | DCT multiple images watermarking | | | | | | | | |
|----|-------------------------------|------|-----------|------|------|----------------------------------|------|-------------|------|------|-------------|------|------|--|
| | Watermarked image | | Watermark | | | Watermarked image | | Watermark-1 | | | Watermark-2 | | | |
| | AR | PSNR | NC | AR | PSNR | AR | PSNR | NC | AR | PSNR | NC | AR | PSNR | |
| 1 | 100 | 43.4 | 0.7 | 81.2 | 5.2 | 100 | 41.2 | 0.7 | 82.8 | 5.2 | 0.59 | 70.3 | 3.8 | |
| 2 | 100 | 43.3 | 0.71 | 81.2 | 5.3 | 100 | 41.2 | 0.7 | 79.6 | 5.2 | 0.59 | 70.3 | 3.8 | |
| 5 | 100 | 43.0 | 0.79 | 82.8 | 6.8 | 100 | 40.7 | 0.8 | 82.8 | 7.0 | 0.61 | 78.1 | 4.0 | |
| 8 | 99.8 | 42.3 | 0.95 | 95.3 | 13.5 | 99.8 | 40 | 0.94 | 95.3 | 12.5 | 0.67 | 76.5 | 4.7 | |
| 10 | 99.4 | 41.8 | 0.99 | 98.4 | 21.0 | 99.4 | 39.3 | 0.99 | 100 | 20.4 | 0.74 | 90.6 | 5.7 | |
| 12 | 99.2 | 41.3 | 1 | 100 | 36.1 | 99.2 | 38.6 | 1 | 100 | 36.1 | 0.83 | 95.9 | 7.6 | |
| 15 | 98.8 | 40.4 | 1 | 100 | 36.1 | 99.2 | 37.7 | 1 | 100 | 36.1 | 0.93 | 96.8 | 11.9 | |
| 18 | 98.8 | 39.6 | 1 | 100 | 36.1 | 99.2 | 36.8 | 1 | 100 | 36.1 | 1 | 100 | 31.3 | |
| 20 | 98.8 | 39 | 1 | 100 | 36.1 | 98.9 | 36.3 | 1 | 100 | 36.1 | 1 | 100 | 36.1 | |

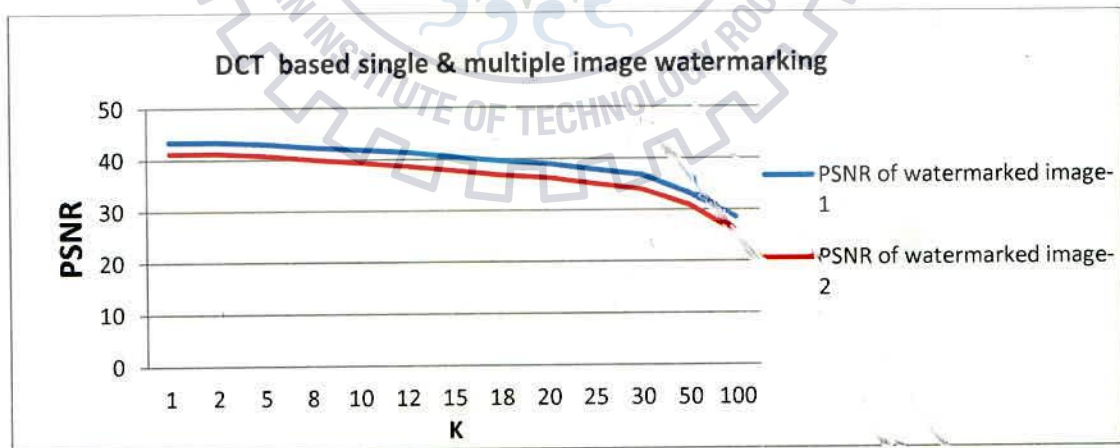


Fig. 4.7: Variation in PSNR of watermarked image in DCT based single and multiple images watermarking

4.4.2 SVD Based Multiple Images Watermarking

For single and multiple images watermarking the values of accuracy rate, PSNR and normalized correlation (NC) with respect to gain factor alpha, are shown in table 4.2. This shows that for the same value of alpha, PSNR of the watermarked image in single image watermarking is slightly more than the PSNR of watermarked image in multiple images watermarking unlike more difference in DCT based method because in SVD based method only singular values are varied in either multiple or single image watermarking. Two different images embedding and extraction are shown in Fig.4.8.

PSNR variation of watermarked images with respect of gain factor alpha is shown through graph in Fig.4.9. This shows that for the same value of alpha watermarked image-1 of single image SVD watermarking method is having slightly higher PSNR value than the watermarked image-2 of multiple images SVD based watermarking method.

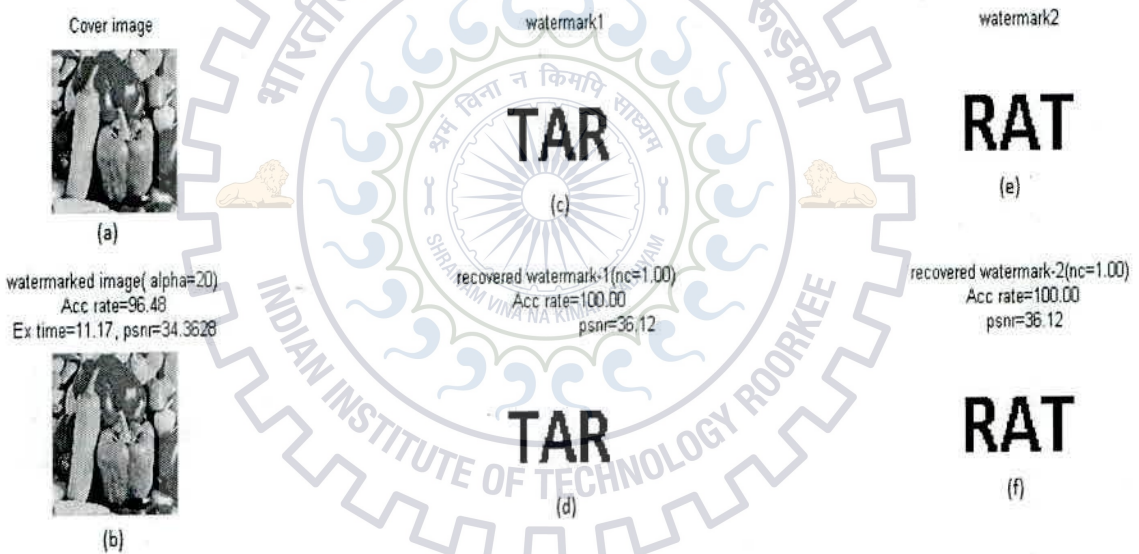


Fig. 4.8: SVD based multiple images watermarking,

- (a) Host image (b) Watermarked image(c) First watermark (d) First recovered watermark
 (e) Second watermark, (f) Second recovered watermark

Table 4.2: SVD based single image and multiple images watermarking

| α | SVD single image watermarking | | | | | SVD multiple images watermarking | | | | | | | |
|----------|-------------------------------|------|-----------|------|------|----------------------------------|------|-------------|------|------|-------------|------|------|
| | Watermarked image | | Watermark | | | Watermarked image | | Watermark-1 | | | Watermark-2 | | |
| | AR | PSNR | NC | AR | PSNR | AR | PSNR | NC | AR | PSNR | NC | AR | PSNR |
| 1 | 100 | 60.3 | 0.04 | 7.8 | 0.73 | 100 | 59.2 | 0.05 | 4.69 | 0.76 | 0.07 | 12.5 | 0.96 |
| 1.3 | 100 | 58.2 | 0.66 | 71.8 | 5.1 | 100 | 57.0 | 0.72 | 79.6 | 6.03 | 0.75 | 75 | 6.73 |
| 1.5 | 100 | 57.0 | 0.97 | 96.8 | 15.1 | 100 | 55.9 | 0.98 | 100 | 16.7 | 0.98 | 96.8 | 18.7 |
| 1.7 | 100 | 56 | 1 | 100 | 33.1 | 100 | 54.8 | 1 | 100 | 36.1 | 1 | 100 | 36.1 |
| 2 | 100 | 54.6 | 1 | 100 | 36.1 | 100 | 53.5 | 1 | 100 | 36.1 | 1 | 100 | 36.1 |
| 5 | 99.4 | 47.4 | 1 | 100 | 36.1 | 99.2 | 46.3 | 1 | 100 | 36.1 | 1 | 100 | 36.1 |
| 8 | 99.2 | 43.7 | 1 | 100 | 36.1 | 99.2 | 42.4 | 1 | 100 | 36.1 | 1 | 100 | 36.1 |
| 10 | 99.0 | 41.9 | 1 | 100 | 36.1 | 98.8 | 40.5 | 1 | 100 | 36.1 | 1 | 100 | 36.1 |

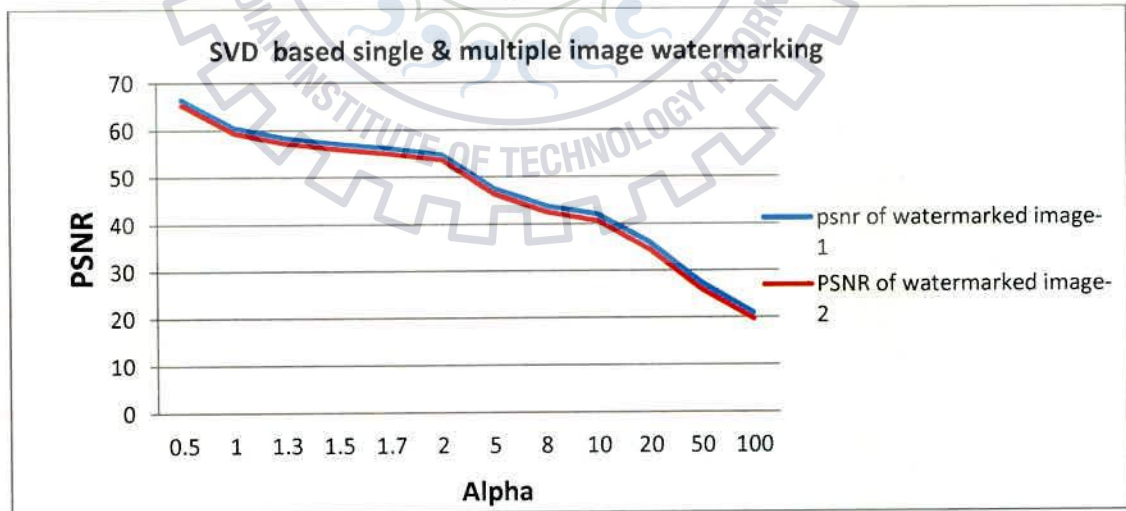


Fig. 4.9: Variation in PSNR of watermarked image in SVD based single and multiple images watermarking

4.5 Conclusions

In this chapter, two multiple images digital image watermarking algorithm is implemented using MATLAB which is based on DCT and SVD. Experiment results conclude that SVD based multiple images watermarking algorithm has better watermarked image compared to DCT based multiple images watermarking algorithm.

A hybrid multiple images watermarking algorithm using SVD and other transform based method can also be used to extract much better watermark image. In next chapter a DCT-SVD based watermarking scheme has been proposed.



Chapter 5

DCT-SVD Based Robust Watermarking

5.1 Introduction

Geometric attacks such as rotation, cropping scaling are easy to apply in digital watermarking and this may lead to many watermark detector total failure due to loss of synchronization between the embedded and correlated watermark [4]. To get more robust watermark against geometrical attack is main issue in most of the watermarking algorithm. Due to the property of SVD, the SVD based digital image watermarking has replaced DCT and DWT based watermarking. This is improved algorithm over these transform based method. But SVD based watermarking is not robust to JPEG compression. During data transmission JPEG compression can be used to make data transfer in a large capacity.

In all watermarking method, SVD based algorithm is more robust against geometric attacks while DCT based watermarking algorithm is more robust against JPEG compression. So a hybrid algorithm based on DCT-SVD is introduced this is having the combined property of DCT and SVD and is resilient algorithm to signal processing and geometric attacks and JPEG compression [28].

In this hybrid algorithm, first of all DCT of the whole cover image is taken then segmented in to blocks for singular value decomposition. Watermark image is scrambled using Arnold transform and then this encrypted watermark is embedded in singular values. This not only improves the robustness but also security of the watermark. To evaluate the algorithm, this hybrid DCT-SVD based watermarking is compared with the pure SVD based algorithm on the basis of PSNR and robustness. Experimental evaluation shows that this algorithm is able to resist a variety of attacks including JPEG compression different signal processing attacks like pepper and salt, Gaussian noise, Poisson noise, median filter noise, and geometric attacks like image cropping, image rotation and image scaling.

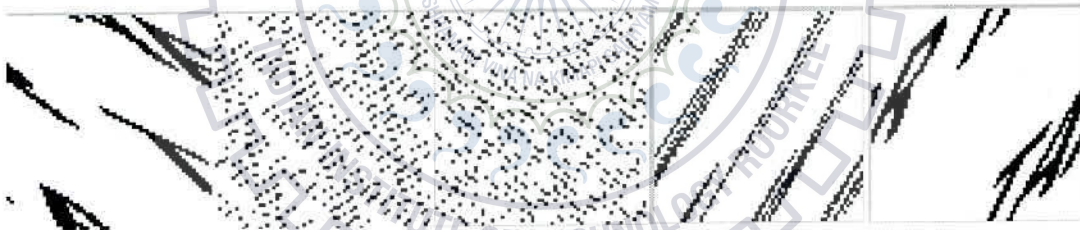
5.2 Arnold Transform

Arnold transform is an image scrambling technique, used as encryption for watermark image. This is a simple and easy method to implement which perturbs the original watermark image and spreads information which reduces the losses of information after attacking [29].

This is also known as cat face transform, Arnold transform changes the gray image by changing the coordination of pixels. This is a periodic process when it is iterated then after some iteration times we get original watermark. This not only hides the information but also provides a description key as no of iteration times without knowing original transform times anyone can not extract the hidden information.

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \pmod{N} \quad \dots\dots\dots (5.1)$$

After taking Arnold transform, x' and y' indicate the new position of coordinates of pixel x, y. Mod N is to ensure that pixel filling is in the range of {0 to N-1} [30]. Encrypted watermark image is obtained by this equation (5.1) and original watermark image is restored according to the periodicity and original transform times. The images after applying Arnold's transform are shown below.



No. of iteration: 1 No. of iteration: 20 No. of iteration: 35 No. of iteration: 46 No. of iteration: 47

Fig.5.1: watermark Image after Arnold transform

It is found that iterations to complete Arnold transform cycle increases with the increasing the size of the image. The original image can be obtained using following no. of iteration in a cycle or by Arnold inverse transform [29].

Table 5.1: Arnold transforms cycle for different size of an image

| | | | | | |
|------------------|----|----|-----|-----|-----|
| Size of Image | 32 | 64 | 128 | 256 | 512 |
| No. of iteration | 24 | 48 | 96 | 192 | 384 |

5.3 SVD Based Watermarking

Singular value decomposition is a very useful tool for a matrix analysis. This converts a matrix into three matrices [6]. It packs maximum energy into a small number of coefficients as possible [35]. It has the ability to adapt changes in local statistics of an image.

The SVD of image I_m can be described as

$$I_m = HSV^T$$

I_m is the image matrix. H and V are two $M \times N$ and $N \times N$ unitary orthogonal matrices, and S is an $N \times N$ diagonal matrix [10]. Where the horizontal detail component of image I_m is represented by H matrix and vertical detail component of the image I_m is represented by V matrix. Both V and H are orthogonal matrices and S is a singular matrix which consists of singular values arranged diagonally and in decreasing order. One of the important properties of SVD is stability which means a small change in the singular values does not affect the visual perception of watermark image (message) [23] and flipping, transpose property make SVD algorithm more immune to geometrical attack.

There are two methods to insert a watermark in SVD based watermarking. In the first case, the watermark is directly embedded in the singular values of the host image. In the second method, the watermark is embedded in the transform coefficients of the host image. The second method offers the idea of hybrid watermarking [34].

5.3.1 Pure SVD Based Watermarking

In pure SVD based, no other watermarking method is combined with SVD based algorithm. In this watermarking method, first of all the host image is divided into blocks. Then each block of the host image is decomposed using SVD. Singular values of the singular diagonal matrix are modified according to the message bits. Two random sequences for two binary digits '1' and '0' are added to the singular values with a gain factor. These random sequences work here as a secret key. After modifying the singular values, the inverse process of the SVD is taken to generate the watermarked image. At the extraction algorithm, the correlation between the stored singular value and the modified singular values is found. Using this, the message bits are recovered and reshaped into the watermark image.

5.3.2 SVD Based Hybrid Watermarking

SVD based Hybrid watermarking is used to produce better result. In this hybrid watermarking SVD based algorithm is combined with another transform based algorithm either DCT or DWT or both. Here SVD based algorithm is combined with DCT based algorithm and described below.

5.4 DCT-SVD Based Watermarking

In this method the property of DCT and SVD algorithms are combined to produce more robust watermarking against geometric attack and JPEG compression. A discrete cosine transform (DCT) converts the image in terms of a sum of cosine function oscillating at different frequencies [18]. This is a transform domain algorithm which is more robust against JPEG compression.

First of all, DCT is applied to whole host image then host image is segmented into 8x8 blocks for singular value decomposition. Using a gain factor alpha (α), two random sequences are added with singular values according to the watermark bits. Before embedding watermark, the watermark image is scrambled using Arnold transform. This makes the watermarking more secure. After modifying singular values, the block wise inverse SVD process is taken. Then inverse DCT of whole image is taken to produce watermarked image.

At the extraction algorithm the DCT of the whole watermarked image is taken then singular value decomposition of this transformed image gives the modified singular values. Correlation between stored singular values (SVs) and modified singular values are found. Using this, message bits are recovered and reshaped in to the watermark image.

5.4.1 Watermark Embedding

Steps:

1. Compute the non-blocking DCT of whole cover image.
2. Transformed image is segmented into 8x8 blocks.
3. Apply SVD to each block to obtain H, V and S matrix.

$$\text{SVD of transformed image} = HSV^T$$

4. Apply Arnold transform to scramble the watermark image.
5. Using a gain factor α add two random sequences (according to the encrypted watermark bits) with singular values to modify singular matrix S

$$S1 = S + \alpha * (\text{rand sequence}) \quad \dots (5.3)$$
6. Apply SVD to S1 to get $H_1 S_1 V_1^T$.

$$\text{SVD of modified singular matrix} = H_1 S_1 V_1^T \quad \dots (5.4)$$
7. Using inverse SVD process, obtain image according to $H S_1 V^T$.
8. Apply inverse DCT to get watermarked image.

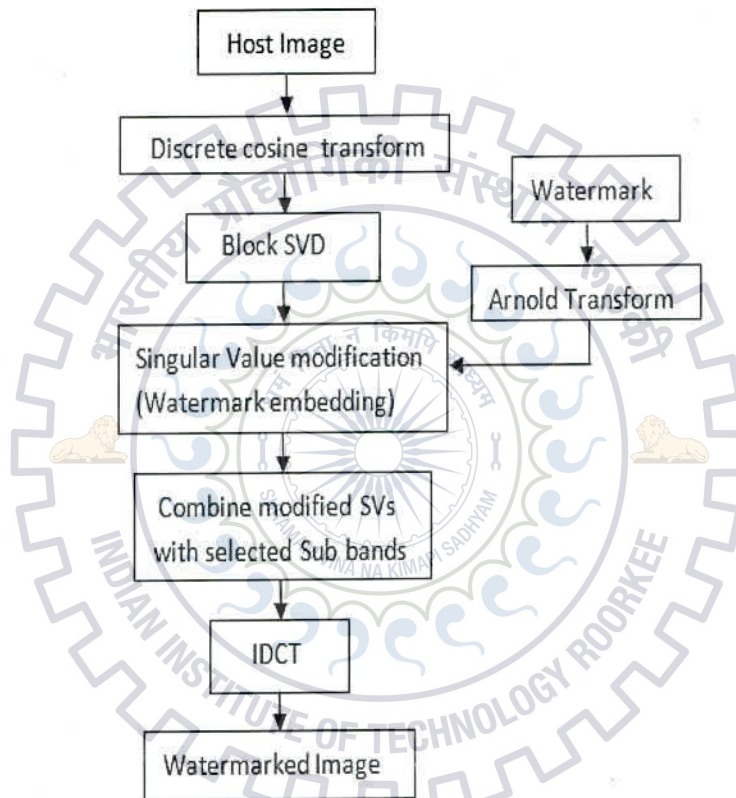


Fig. 5.2: Block diagram of DCT-SVD watermark embedding

5.4.2 Watermark Extraction

1. Apply DCT to the whole watermarked image.
2. Transformed image is segmented in to 8x8 blocks.
3. Apply SVD to each 8x8 block of transformed image,
4. Obtain H^* , V^* and $S1^*$ matrix to get modified singular values s matrix.

$$\text{SVD of transformed image} = H^* S^* V^{*T} \quad \dots (5.5)$$

5. From the stored value of $H1$, $V1$ and $S1^*$, take the inverse process of SVD to get S matrix.
6. Take the difference between the modified and stored SVs to get the new sequence
7. From the correlation between rand sequences and this new sequence the message bits are extracted and reshaped to get watermark image.

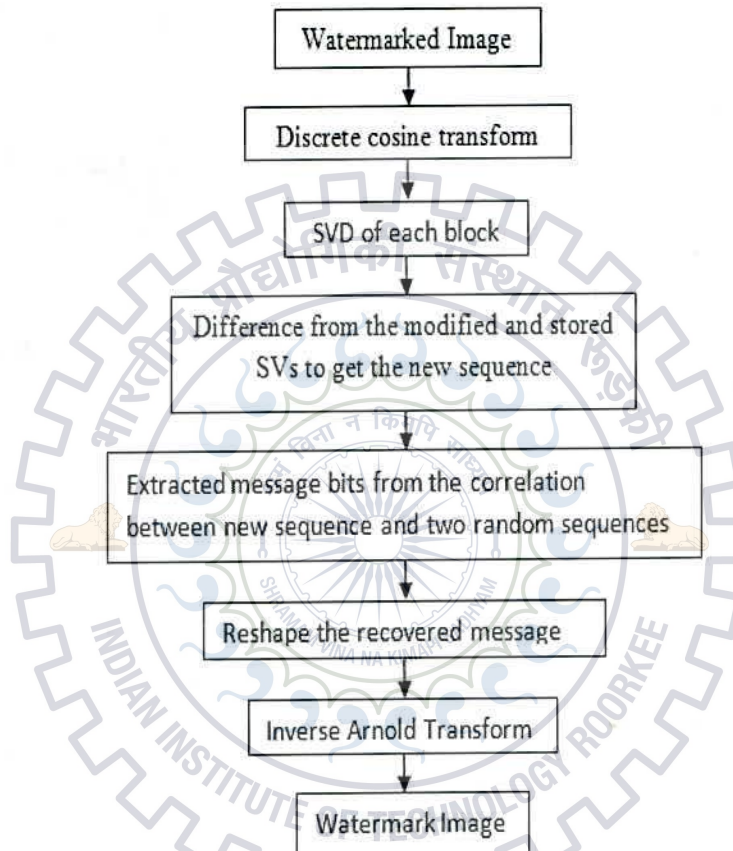


Fig. 5.3: Block diagram of DCT-SVD watermark extraction

5.5 Experimental Results and Discussion

To evaluate the performance of pure SVD based and DCT-SVD based watermarking, a 512x512 pixels “peppers.jpg” image is taken as host image and 64x64 pixels “tar.tif” image is taken as watermark and block size is kept 8x8 pixels. Both Algorithms are implemented using MATLAB and different image processing toolbox is used to insert the attacks.

Performance of DCT-SVD hybrid method is evaluated and compared with SVD algorithm. PSNR is computed between watermarked image and original host image, and between original watermark image and extracted watermark image. Normalized correlation is computed between original watermark and extracted watermark. Both algorithms are tested after inserting a variety of attacks like pepper and salt, Poisson noise, speckle noise, median filter noise, geometric attacks like cropping, image rotating and JPEG compression in watermarked image. Values of PSNR and NC are shown in table 5.2 below. PSNR and robustness variation against different noise and attacks are shown in fig. 5.4 and in fig. 5.5 respectively.

Table 5.2: Watermarks comparison between pure SVD and DCT-SVD based algorithm

| SN | Attack Type | Extracted watermark of SVD based algorithm | | Extracted watermark of DCT-SVD based algorithm | |
|----|---------------------|--|------|--|------|
| 1 | No attack | 36.12 | 1 | 36.12 | 1 |
| 2 | Salt & pepper noise | 27.67 | 1 | 36.12 | 1 |
| 3 | Poisson noise | 36.12 | 1 | 36.12 | 1 |
| 4 | Speckle noise | 36.12 | 1 | 36.12 | 1 |
| 5 | Median filter noise | 23.11 | 1 | 27.67 | 1 |
| 6 | Intensity variation | 9.16 | 0.89 | 20.68 | 0.99 |
| 7 | Image rotation | 9.63 | 0.88 | 19.4 | 0.99 |
| 8 | Image cropping | 14.11 | 0.96 | 19.4 | 0.99 |
| 9 | JPEG Comp (Q=8) | 5.31 | 0.75 | 22.7 | 0.99 |
| 10 | JPEG Comp (Q=20) | 10.26 | 0.92 | 26.58 | 1 |
| 11 | JPEG Comp (Q=45) | 23.82 | 1 | 27.09 | 1 |

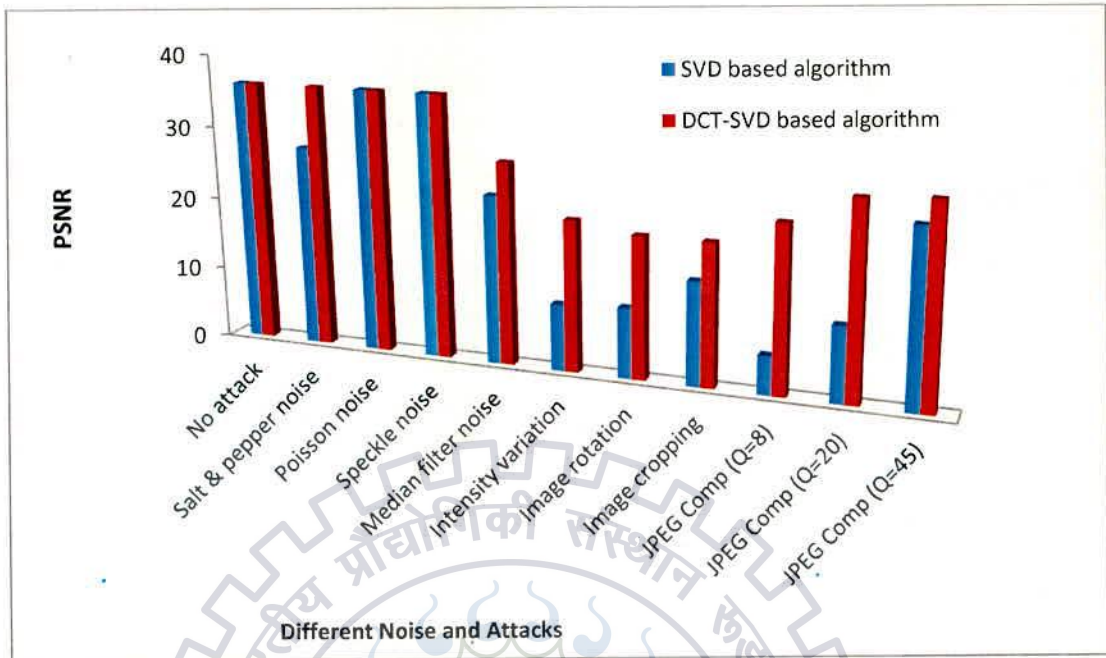


Fig. 5.4: PSNR variation of watermark images in pure SVD and DCT-SVD based algorithms against different attacks

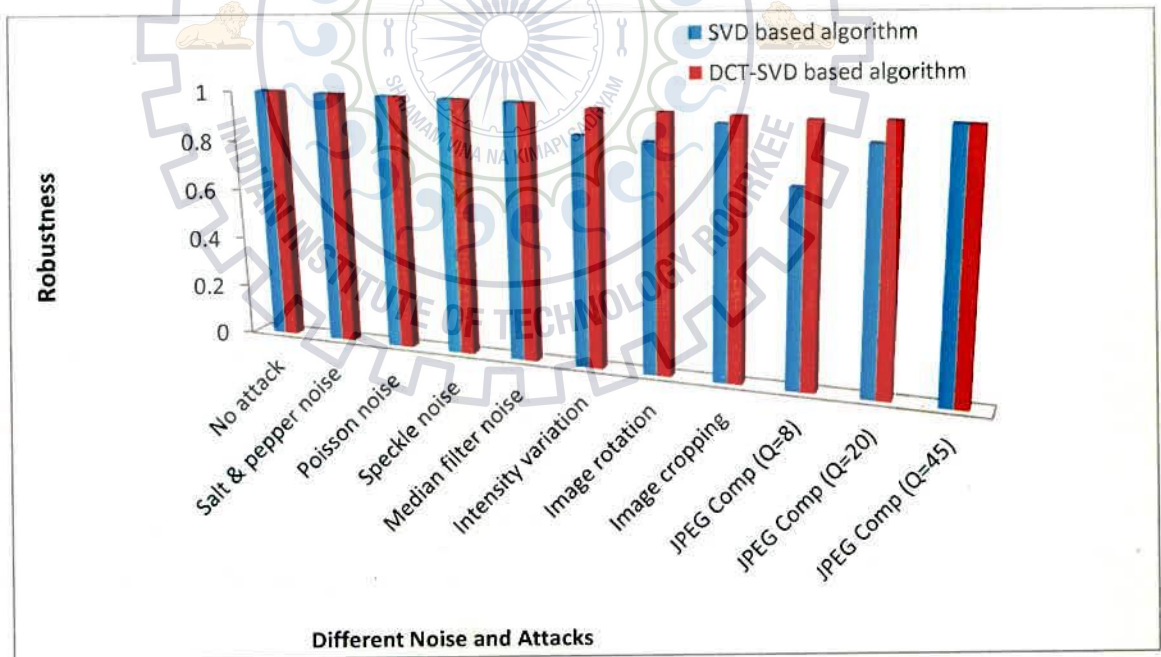

















































Fig. 5.5: Robustness variation of watermark images in pure SVD and DCT-SVD based algorithms against different attacks

Table 5.3: Extracted watermark images form Pure SVD and DCT-SVD based algorithm against different attacks

| SN | Type of Noise/ Attack | Pure SVD based watermarking | DCT-SVD based watermarking |
|----|---|--|--|
| 1. | No attack | <p>watermarked image psnr=32.15</p>  <p>recovered watermark nc=1.00, psnr=36.12</p>  | <p>watermarked image psnr=33.02</p>  <p>recovered watermark nc=1.00, psnr=36.12</p>  |
| 2. | <p>Salt & Pepper attack</p>  | <p>watermarked image psnr=23.55</p>  <p>recovered watermark nc=1.00, psnr=27.67</p>  | <p>watermarked image psnr=23.84</p>  <p>recovered watermark nc=1.00, psnr=36.12</p>  |
| 3. | Poisson noise | <p>watermarked image psnr=25.31</p>  <p>recovered watermark nc=1.00, psnr=36.12</p>  | <p>watermarked image psnr=25.48</p>  <p>recovered watermark nc=1.00, psnr=36.12</p>  |

| | | | |
|----|---|---|--|
| 4. | Speckle noise | <p>watermarked image psnr=24.02</p>  <p>recovered watermark nc=1.00, psnr=36.12</p>  | <p>watermarked image psnr=24.13</p>  <p>recovered watermark nc=1.00, psnr=36.12</p>  |
| 5. | Median filter noise | <p>watermarked image psnr=32.81</p>  <p>recovered watermark nc=1.00, psnr=23.11</p>  | <p>watermarked image psnr=32.55</p>  <p>recovered watermark nc=1.00, psnr=27.67</p>  |
| 6. | Intensity variation  | <p>watermarked image psnr=11.22</p>  <p>recovered watermark nc=0.89, psnr=9.16</p>  | <p>watermarked image psnr=11.18</p>  <p>recovered watermark nc=0.99, psnr=20.68</p>  |
| 7. | Image rotation | <p>watermarked image psnr=9.45</p>  <p>recovered watermark nc=0.88, psnr=9.63</p>  | <p>watermarked image psnr=9.43</p>  <p>recovered watermark nc=0.99, psnr=19.40</p>  |

| | | | |
|-----|--|--|--|
| 8. | Image cropping | <p>watermarked image psnr=11.71</p>  <p>recovered watermark nc=0.96, psnr=14.11</p>  | <p>watermarked image psnr=11.68</p>  <p>recovered watermark nc=0.99, psnr=19.40</p>  |
| 9. | JPEG compression (Q=8) | <p>watermarked image psnr=27.94</p>  <p>recovered watermark nc=0.75, psnr=5.31</p>  | <p>watermarked image psnr=27.96</p>  <p>recovered watermark nc=0.99, psnr=22.70</p>  |
| 10. |  <p>JPEG compression (Q=20)</p> | <p>watermarked image psnr=30.37</p>  <p>recovered watermark nc=0.92, psnr=10.26</p>  | <p>watermarked image psnr=30.46</p>  <p>recovered watermark nc=1.00, psnr=26.58</p>  |
| 11. | JPEG compression (Q=45) | <p>watermarked image psnr=31.40</p>  <p>recovered watermark nc=1.00, psnr=23.82</p>  | <p>watermarked image psnr=31.31</p>  <p>recovered watermark nc=1.00, psnr=27.09</p>  |

5.6 Conclusions

This chapter presents a combined digital image watermarking based on DCT and the stability and algebraic property of SVD, with encrypted watermark image. Performance of this new DCT-SVD algorithm is compared with pure SVD algorithm on the basis of PSNR and robustness. Table.5.3 shows this hybrid algorithm gives better results and is able to extract watermark from JPEG compressed watermarked image unlike pure SVD based method. Arnold transform is used to enhance the security of this watermarking.



Chapter 6

Conclusions and Future Scope

6.1 Conclusions

In this dissertation multiple images watermarking and a DCT-SVD based hybrid watermarking are presented. All the watermarking algorithms are implemented using MATLAB. For comparison purpose, host and watermark image are kept same for all algorithms. On the basis of PSNR and robustness of extracted watermark images these algorithms are examined after inserting the different noise and attacks in watermarked image at extraction algorithm.

In DCT based algorithm the visual quality of watermarked image is not affected if gain factor is kept low. Greater the value of gain factor guarantees more robustness of watermark image but perceptual quality of the watermarked image decreases. So there is a tradeoff between the quality of watermarked image and robustness of extracted watermark. The advantage of DCT algorithm is that it is much robust against JPEG compression of image. It means DCT algorithm is suitable where large capacity data is transferred. On the other hand DCT based algorithm gives poor results in case of geometric attacks.

SVD based watermarking has dominated over all transform based algorithm due to the property of SVD. In case of geometric attacks like image rotation and cropping, SVD algorithm is able to extract watermark image unlike other algorithms. This is due to the stability, flipping and transpose etc properties of SVD.

DCT based and SVD based multiple images digital image watermarking algorithms are implemented and discussed in chapter 4. Experiment results conclude that SVD based multiple images watermarking algorithm has better watermarked image compared to DCT based multiple images watermarking algorithm.

A hybrid watermarking based on DCT and the stability and algebraic property of SVD with encrypted watermark image is proposed. SVD based watermarking belongs to

spatial domain and robust against geometric attack due to the property of SVs. DCT transform of host image provides it into low frequency image before SVD decomposition which makes this hybrid method more robust against JPEG compression. Watermark scrambling using Arnold transform is used to enhance the security of this watermarking. Performance of this hybrid DCT-SVD algorithm is evaluated with pure SVD algorithm on the basis of PSNR and robustness. Results show that this hybrid algorithm is more robust than SVD algorithm in case of geometric attacks and JPEG compression.

6.2 Future Scope

Good imperceptibility of watermarked image and robustness of watermark, are important issues in digital image watermarking algorithm. A lot of work and research has been done in digital watermarking to get best tradeoff. There are more scopes to improve our work like DCT-SVD hybrid watermarking, the properties of two or more watermarking algorithms can be combined to produce more robust watermarking. Values of coefficients in frequency transform domain can be made based on human visual characteristics with our proposed method. Some future works related to digital watermarking are pointed below.

1. SVD based algorithm can be combined with one or two algorithm to get better results.
2. In digital image watermarking different encryption technique can be used to scramble or encode the watermark. This can provide additional security to watermarking algorithm.
3. Artificial neural network, Genetic algorithm or any other optimization method can also be used to select the best coefficient in transform based watermarking for watermark embedding which will give better results.
4. A real time implementation of watermarking method can also be done and it should be performed for a particular application.
5. Principle component analysis, feature extraction etc methods can also be used for watermarking algorithm and these methods can also be combined with any other to get robust watermark.
6. Our work and research can be extended for color image watermarking. Like image, we can look for more research in audio and video watermarking.

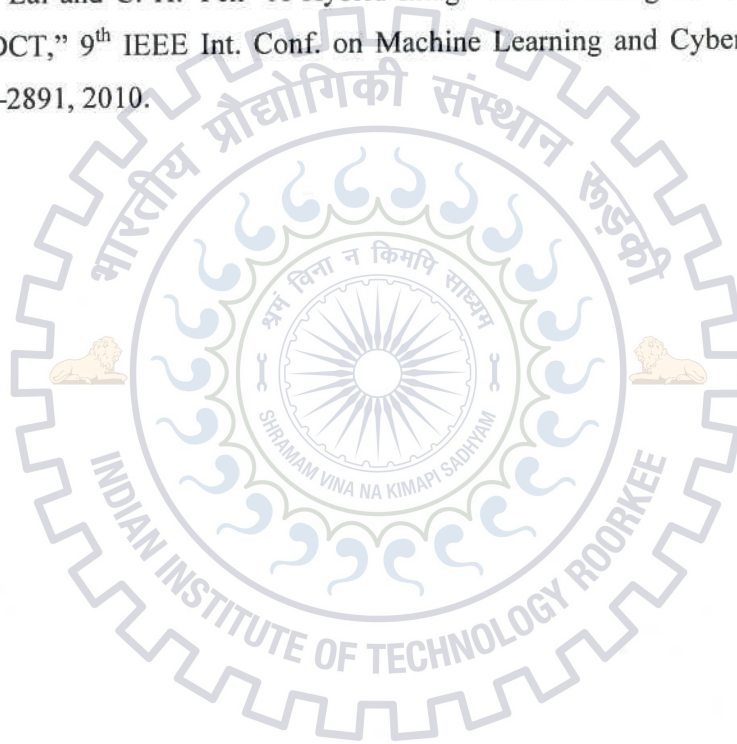
References

- [1] N. wang, W. Yunjin and X. Li, "A Novel Robust Watermarking Algorithm Based on DWT and DCT," IEEE Int. Conf. on Computational Intelligence and Security, Vol. 1, pp. 437- 441, 2009.
- [2] V. M. Potdar, S. Han and E. Chang, "A Survey of Digital Image Watermarking Techniques," 3rd IEEE Int. Conf. on Industrial Informatics, pp. 709-716, 2005.
- [3] R. B. Wolfgang, C. I. Podilchuk and E. J. Delp, "Perceptual Watermarks for Digital Images and Video," IEEE Int. Conf., vol. 87, no. 7, pp. 1108-1126, 1999.
- [4] D.Y. Chen, Ming. Ouhyoung and J. L. Wu, "A Shift Resisting Public Watermark System for Protecting Image Processing Software," IEEE Trans. on Consumer Electronics, vol. 46, no.3, pp. 404 - 414, 2000.
- [5] T. Liu and Z. D. Qiu, "The Survey of Digital Watermarking Based Image Authentication Techniques," 6th IEEE Int. Conf. on Signal Processing, vol.2, pp. 1556 - 1559, 2002.
- [6] R. Liu and T. Tan, "An SVD-Based Watermarking Scheme for Protecting Rightful Ownership," IEEE Trans. on Multimedia, vol. 4, no. 1, pp. 121-128, 2002.
- [7] J. Sang and M. S. Alam, "Fragility and Robustness of Binary-phase-only Filter-Based Fragile/Semifragile Digital Image Watermarking," IEEE Trans. on Instrumentation and Measurement, vol. 57, no. 3, pp. 595 - 606, 2008.
- [8] M. A. Suhail and M. S. Obaidat, "Digital Watermarking Based DCT and JPEG Model," IEEE Trans. on Instrumentation and Measurement, vol. 52, no. 5, pp. 1640 - 1647, 2003.
- [9] F. Hartung and M. Kutter, "Multimedia Watermarking Techniques," IEEE Int. Conf., vol. 87, no. 7, pp. 1079-1107, 1999.
- [10] Z. M. Lu, H.Y. Zheng and Ji-Wu Huang, "A Digital Watermarking Scheme Based on DCT and SVD," 3rd IEEE Int. Conf. on Intelligent Information Hiding and Multimedia Signal Processing, vol.1, pp. 241- 244, 2007.

- [11] B. Wang, J. Ding, Q. Wen, X Liao and C. Liu, "An Image Watermarking Algorithm Based on DWT DCT and SVD," IEEE Int. Conf. on Network Infrastructure and Digital Content, pp. 1034 - 1038, 2009.
- [12] F. Bartolini, A. Tefas, M. Barni, and I. Pitas, "Image Authentication Techniques for Surveillance Applications," IEEE Int. Conf., vol. 89, no.10 , pp. 1403 - 1418, 2001.
- [13] G. J. Lee, E. J. Yoon and K. Y. Yoo, "A New LSB Based Digital Watermarking Scheme with Random Mapping Function," IEEE Int. Conf. on Ubiquitous Multimedia Computing, pp. 130 - 134, 2008.
- [14] R. Dubolia, R. Singh, S.S.Bhadoria and R. Gupta, "Digital Image Watermarking by Using Discrete Wavelet Transform and Discrete Cosine Transform and Comparison Based on PSNR," IEEE Int. Conf. on Communication and Network Technologies, pp. 593-596, 2011.
- [15] A. B. Dehkordi, S.N. Esfahani and A. N. Avanaki, "Robust LSB Watermarking Optimized for Local Structural Similarity," 19th Iranian IEEE Int. Conf. on Electrical Engineering, pp. 1- 6, 2011.
- [16] A. K. Singh, N. Sharma, M. Dave and A. Mohan, "A Novel Technique for Digital Image Watermarking in Spatial Domain," 2nd IEEE Int. Conf. on Parallel Distributed and Grid Commuting, pp. 497 - 501, 2012.
- [17] D. Kundur and D. Hatzinakos, "A Robust Digital Image Watermarking Method Using Wavelet-Based Fusion," IEEE Int. Conf. on Image Processing, vol. 1, pp. 544-547, 1997.
- [18] M. Rafigh and M. E. Moghaddam, "A Robust Evolutionary Based Digital Image Watermarking Technique in DCT domain," 7th IEEE Int. Conf. on Computer Graphics, Imaging and Visualization, pp. 105-109, 2010.
- [19] N. Kaewkamnerd and K.R. Rao, "Wavelet Based Image Adaptive Watermarking Scheme," IEEE Electronic Letters, vol. 36, no.4, pp. 312-313, 2000.
- [20] S. E. El-Khamy, M. I. Lotfy and R. A. Sadek, "A Block Based Wavelet Watermarking Technique for Copyright Protection and Authentication," IEEE Trans. on Image Processing, vol. 1, pp. 90-93, 2003.

- [21] R. S. Run, S. J. Horng, J. L. Lai, T. W. Kao and R. Jian Chen, "An Improved SVD-Based Watermarking Technique for Copyright Protection," *Int. Journal on Expert Systems with Applications (ELSEVIER)*, vol. 39, no. 1, pp. 673-689, 2012.
- [22] C. W. Kok, "Fast Algorithm for Computing Discrete Cosine Transform," *IEEE Trans. on Signal Processing*, vol. 45, no. 3, pp. 757-760, 1997.
- [23] C. Lai and C. Tsai "Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition," *IEEE Trans. on Instrumentation and Measurement*, vol. 59, no. 11, pp. 3060-3063, 2010.
- [24] R. Sun, H. Sun and T. Yao, "A SVD and Quantization Based Semi-Fragile Watermarking Technique for Image Authentication," 6th *IEEE Int. Conf. on Signal Processing*, vol. 2, pp. 1592-1595, 2002.
- [25] C. Lai, "An Improved SVD-Based Watermarking Scheme Using Human Visual Characteristics," *Int. Journal on Optics Communications (ELSEVIER)*, vol. 284, no. 4, pp. 938-944, 2011.
- [26] R. Rykaczewski, "Comments on an SVD-Based Watermarking Scheme for Protecting Rightful Ownership," *IEEE Trans. on Multimedia*, vol. 9, no. 2, pp. 421-423, 2007.
- [27] L. Liu and Q. Sun, "Robust Image Watermarking Against Geometrical Attacks," *IET Int. Conf. on Wireless, Mobile and Multimedia Networks*, pp. 1-3, 2006.
- [28] H. Himanshu, S. Rawat, B. Raman, and G. Bhatnagar, "DCT and SVD Based New Watermarking Scheme," 3rd *Int. Conf. on Emerging Trends in Engineering and Technology*, pp. 146 - 151, 2010.
- [29] M. Ding and F. Jing, "Digital Image Encryption Algorithm Based on Improved Arnold Transform," *IEEE Int. Conf. on Information Technology and Applications*, vol. 1, pp. 174 - 176, 2010.
- [30] L. Ling, X. Sun and L. Cai "A Robust Image Watermarking Based on DCT by Arnold Transform and Spread Spectrum," 3rd *IEEE Int. Conf. on Advanced Computer Theory and Engineering*, vol. 1, pp. 198-201, 2010.
- [31] F. Liu and Y. Liu, "A Watermarking Algorithm for Digital Image Based on DCT and SVD," *IEEE Int. Conf. on Image and Signal Processing*, vol. 1, pp. 380 - 383, 2008.

- [32] P. K. Gupta and S. K. Shrivastava, "Improved RST Attacks Resilient Image Watermarking Based on Joint SVD-DCT," IEEE Int. Conf. on Computer and Communication Technology, pp. 46 - 51, 2010.
- [33] L. Quan and A. Aingsong, "A Combination of DCT Based and SVD Based Watermarking Scheme," 7th IEEE Int. Conf. on Signal Processing, 2004. Vol. 1, pp. 873 - 876, 2004.
- [34] Q. Li, C. Yuan and Y. Z. Zhong, "Adaptive DWT SVD Domain Image Watermarking Using Human Visual Model," 9th IEEE Int. Conf. on Advanced Communication Technology, vol. 3, pp. 1947 - 1951, 2007.
- [35] C. C. Lai and C. H. Yeh "A Hybrid Image Watermarking Scheme Based on SVD and DCT," 9th IEEE Int. Conf. on Machine Learning and Cybernetics, vol. 6, pp. 2887-2891, 2010.



List of Candidate's Publications

- [1] T. Rathi, R. P. Maheshwari and M. Tripathy "**Implementation of Multiple Images DCT Watermarking and SVD Robust Watermarking,**" IEEE Int. Conf. on Signal Processing, Computing and Control (ISPCC 2013), 2013. (Under review)
- [2] T. Rathi, R. P. Maheshwari and M. Tripathy "**Comparative Analysis of Different Spatial and Transform Domain based Image Watermarking Techniques,**" 6th IEEE Int. Conf. on Contemporary Computing (IC32013), 2013. (Under review)
- [3] T. Rathi, R. P. Maheshwari and M. Tripathy "**A Combination of DCT and SVD based Algorithm for Resilient Digital Image Watermarking against Geometric Attacks and JPEG Compression,**" IEEE Int. Conf. on "Impact of Engineering on Global Sustainability" 2013. (Communicated)

