Oblivious Fragile Watermarking Algorithms

Thesis submitted in partial fulfillment of the requirements for the award of degree of

Master of Engineering
in
Computer Science and Engineering

Submitted By
Gagandeep Singh Chauhan
(Roll No. 801632005)

Under the supervision of:
Dr. Geeta Kasana
Assistant Professor

THAPAR INSTITUTE
OF ENGINEERING & TECHNOLOGY
(Deemed to be University)

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT
THAPAR INSTITUTE OF ENGINEERING AND TECHNOLOGY
PATIALA – 147004

June 2018

CERTIFICATE

I hereby certify that the work which is being presented in the thesis entitled, "*Oblivious Fragile Watermarking Algorithms*", in partial fulfillment of the requirements for the award of degree of Master of Engineering in *Computer Science and Engineering* submitted in Computer Science and Engineering Department of Thapar Institute of Engineering and Technology, Patiala, is an authentic record of my own work carried out under the supervision of *Dr. Geeta Kasana* and refers other researcher's work which are duly listed in the reference section.

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

G Shauhan

(Gagandeep Singh Chauhan)

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

Geet

(Dr. Geeta Kasana)
Assistant Professor
Computer Science and Engineering Department

Acknowledgement

I would first like to thank my dissertation advisor **Dr. Geeta Kasana**, Assistant Professor, Computer Science and Engineering Department, Thapar Institute of Engineering and Technology, Patiala. She was always present to help in my dissertation and guide me to right direction whenever needed, not only academically but morally also. I also thank her for her time, patience, her valuable suggestions and advice. I am truly grateful to her for the guidance she provided me throughout the dissertation.

I am also thankful to Dr. Maninder Singh, Professor and Head, Computer Science and Engineering Department, Thapar Institute of Engineering and Technology, Patiala and Dr. Ashutosh Mishra for the support they provided.

I would also like to express my gratitude towards Dr. S. S. Bhatia, Dean of Academic Affairs, Thapar Institute of Engineering and Technology, Patiala for making the provision of infrastructure and facilities such as library, computer labs equipped with internet which were very helpful in the dissertation process.

I am also thankful to entire faculties and staff of Computer Science and Engineering Department all persons associated with the Thapar Institute for the help they provided me during my studies and made my stay here memorable.

Finally, I express my profound gratitude to my family and my friends who always encouraged me during the research and writing process of dissertation.

G Chauhan

(Gagandeep Singh Chauhan)

801632005

Abstract

Dissertation entitled as “Oblivious Fragile Watermarking Algorithms” comprises of two watermarking algorithms for digital images. These algorithms are fragile in nature, and are based on frequency based transforms and blind.

The first watermarking algorithm is based upon entropy of the sub band of an image. The sub band having highest Entropy is selected. The Singular Values of 4×4 blocks of the Sub band are modified to embed the watermark.

The second algorithm is based on *DWT*, *DCT* and *SVD*. In this algorithm, the host image is decomposed into sub bands using the *DWT*. Diagonal sub bands are partitioned into the non-overlapping blocks of equal size. Each block is transformed by *DCT* and further *SVD* is applied and singular values are modified to embed the watermark.

The effectiveness of the proposed algorithms is evaluated by *PSNR* for imperceptibility. Bit Correction Rate, Bit Error Rate, Similarity Index Modulation and Normalized correlation are used to evaluate the comparability between original and extracted watermark.

The main contribution of proposed algorithms is that,they can be used for tempered detection and information security.

Contents

List of Figures

List of Tables

List of Abbreviations

BPNN	Back Propagation Neural Network
BER	Bit Error Rate
CWSA	Chaotic Watermarking Scheme for Authentication
DCT	Discrete Cosine Transform
DFIS	Dynamic Fuzzy Inference System
DWT	Discrete Wavelet Transform
GA	Genetic Algorithm
HVS	Human Visual System
IDWT	Inverse Discrete Wavelet Transform
IWT	Integer Wavelet Domain
JPEG	Joint Photographic Experts Group
MPEG	Moving Pictures Expert Group
MSE	Mean Square Error
NC	Normalized Correlation
OSELM	Online Sequential Extreme Learning Machine
PRNG	Pseudo Random Number Generator
PSNR	Peak Signal to Noise Ratio
RDWT	Redundant Discrete Wavelet Transform
ROI	Region Of Interest
SIM	Similarity Index Modulation
SVD	Singular Value Decomposition

Chapter 1

Introduction

Today, with the advancement in the technology, the illegal use and copying, transferring, manipulating and tampering the digital data it had become important to have a security for these threats which can be provided with the Digital Watermarking.

1.1 History of Digital Watermarking

First time paper watermarks were used in Fabriano, Italy in 1292. They were mostly used for indication of the brand of paper and the mill in which it was produced. After this invention, the watermarks becomes very famous in Italy and then over whole Europe, and initially it was used for the indication of the brand of paper and the mill which produced it. Later watermarks also started to serve as indication for quality of paper, format and its toughness, authentication and to date the paper. By the 18^{th} century watermarks started to be used as a measure of anti-counterfeiting on currencies and other important documents. Even todays watermarks are widely used as security enhancer in currencies around the world. The term "Digital Watermark" was initially used by Charles Osborne and Andrew Tirkel in December 1992. The first successful watermarking of a steganographic spread spectrum watermark was done by Andrew Tirkel, Gerard Rankin and Charles Osborne in 1993.

1.2. Digital Watermarking

The watermark is a configuration of the bits embedded into any digital data like image, video, audio or text file that identities the data's copyright information such as rights, author *etc*. The digital watermarking is generally used to deliver the copyright protection to intellectual properties which are of digital format. The watermarking is very much similar to physical watermarking with difference that here watermarking technique is the one applied on digital files in place of physical objects. In digital watermarking, signals which are low in energy are embedded into another signal. The watermark is the one which carries the low energy signal and it contains some kind of metadata, like rights information or

security about the prime signal. The low energy signals are embedded into the main signal and it is also known as cover signal, as it covers the watermark.

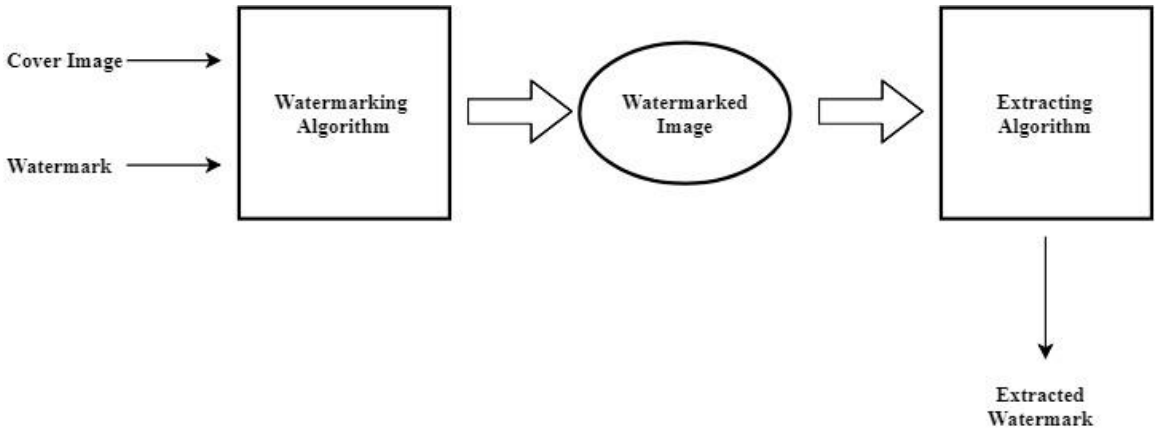


Fig 1.1. Cycle of Digital Image Watermarking

The cover signal is commonly a digital image, a text document, audio, video in digital format. The digital watermarking process consists of a watermarking algorithm and extracting algorithm as shown in Fig 1.1. The watermarking algorithm embeds a watermark into the cover image/host image and the watermarked image is generated which is further followed by an Extracting Algorithm whose job is to extract the watermark which is inserted into the cover image. To check the features such as robustness, fragility *etc.* attacks are executed on the watermarked image and then the watermark is extracted from it.

1.3 Features of Digital Watermarking

The features of the watermarking are the properties which are meant to be present in the watermarking algorithm. Some of the features of Digital Watermarking are described below.

1.3.1 Robustness

It is defined as a property of the watermarking if a watermark is not degraded, displaced or distorted on applying attacks on it like cropping, noise , rotation, quantization, scaling and *JPEG* compression of the content. This property is important in the copyright material which is used for authentication.

1.3.2 Imperceptibility

In digital watermarking the watermark shouldn't be noticeable or visible to the viewer and the quality of the digital data should not be degraded. The only way to view watermark should be applying some kind of extraction algorithm in order to view it.

1.3.3 Security

When a digital watermarking technique is able to prevent any detection and modification of the watermark embedded in the cover image from any unauthorized users then it is said to be secure. Watermark keys are used to ensure that only authorised operators are able to extract or transform the watermark. User having all information of embedding and extracting algorithm and nature of watermark should be able to get access. Watermark information has the unique sign for identification that only the users who are authorised can detect, extract or modify the watermark legally, and be able to provide the copyright protection.

1.3.4 Capacity

This property describes what amount of data or information bits can be inserted in the host image successfully. It describes the potential of embedding more than one watermarks in single digital file. This feature always contest with two other important features, which are, robustness and imperceptibility. A greater capacity could be obtained but at the cost of either robustness, imperceptibility or sometimes both.

1.4 Types of Digital Watermarking

The various type of digital watermarking techniques based upon different properties are discussed and shown in Fig 1.2.

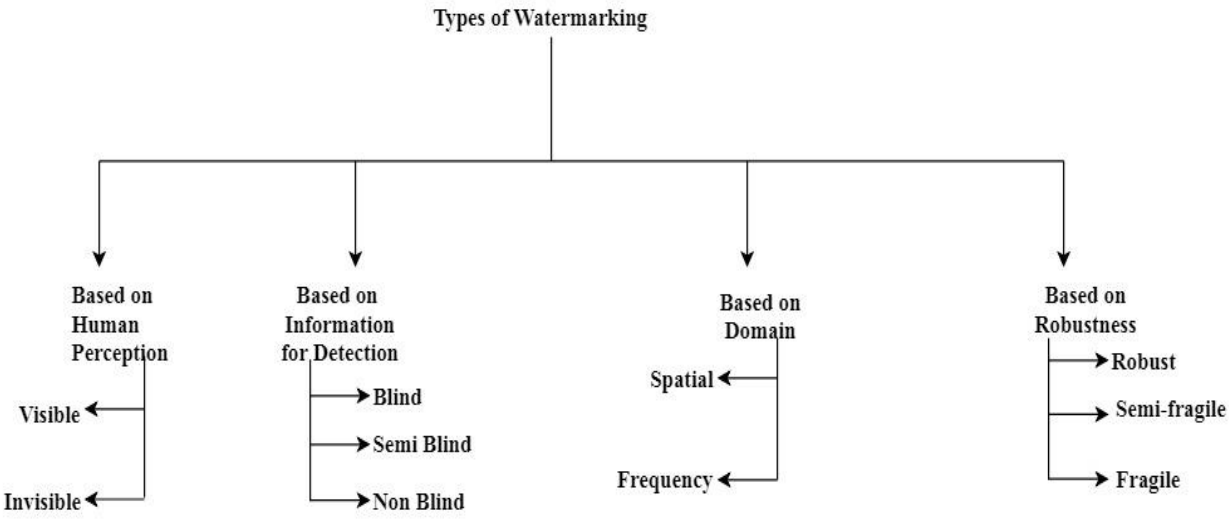


Fig 1.2. Types of Digital Watermarking Techniques

1.4.1 Robust Watermarking

In this Technique watermarks can survive various attacks on them. Watermarks are embedded with such algorithms that they could resist attacks and have minimal damage.

1.4.2 Fragile and Semi-Fragile Watermarking

In Fragile watermarking, watermarks are very sensitive and get easily distorted upon modification. These are mostly used to find whether data had been tampered or not where as in semi-fragile watermarking the watermarks can handle unintentional attacks such as *JPEG* compression but can survive the intentional attacks like cropping, rotation etc.

1.4.3 Blind and Semi-Blind Watermarking

In blind watermarking also known as public watermarking, during detection or extracting process, host image is not needed where as in semi blind watermarking some part of host image is required.

1.4.4 Non-Blind Watermarking

In non-blind watermarking the host image is needed during the detection and extraction process. This watermarking is also known as private watermarking.

1.4.5 Visible Watermarking

In visible watermarking, watermarks are easily visible or noticeable to human eyes. For example like stamp papers and television channel logo.

1.4.6 Invisible Watermarking

Invisible watermarking is the one's which holds the imperceptibility property. These are not visible to viewers and can be seen only after extraction process.

1.5 Applications

The Digital Watermarking is used as application in various fields of our life and some of which are described below.

1.5.1 Copyright protection

Digital watermarking can be utilised for identification of the ownership and copyright protection. Unique digital watermark can be implanted in the digital file to distinguish the copyright owners.

1.5.2 Copy protection

Digital data can be watermarked to stop the illegal replication without owner's permission. Devices used for replication can then recognise the embedded watermarks and unauthorised replication of the content can be prevented.

1.5.3 Tamper proofing

To make the digital content tamper proof, the digital content is embedded with fragile watermark. In case of any alteration and modification watermark gets destroyed which can be used to detect any tempering.

1.5.4 Broadcast monitoring

The advertisements can be monitored by embedding the digital watermarks in the commercial advertisements, whether the advertisements are being transmitted at the accurate time slots or not. The system searches the embedded watermarks from received

broadcast and identify when and where the advertisement is being broadcasted. The similar methodology could be applied to the sound and video clips.

1.5.5 Tracking

Digital watermarking can be used for tracking the usage of original digital content. Each copy of digital content is uniquely watermarked. These watermarks are then extracted and are used to find the users who illegally replicated the content.

1.5.6 Identity Authentication

Textual Watermark can be embedded in the photo on the *ID* card which contain the information like name and registration number which can be used to provide the authentication to the *ID* card. For example, if the *ID* card is stolen or its photo is replaced then information in watermark could be used to match the information written on card. If they don't match then *ID* card is invalid.

1.5.7 Medical application

The names and data of the patients can be embedded into the X-Rays scans or other documents to provide confidentiality and stop mixing the data with other patients.

1.6 Domains of Digital Watermarking

The watermarking techniques are of two types namely spatial domain and frequency domain which are discussed below.

1.6.1 Spatial Domain Watermarking

Spatial Domain Watermarking is one which straightly embed the unprocessed information into the host image. Spatial domain watermarking is also implemented by using colour separation. By this method, the watermark is embedded in just one of the colour band. This makes the visibility of watermark low such that it is very hard to find it under standard viewing. The spatial techniques are based on modification of pixels of host image.

Least Significant Bit *(LSB)* Watermarking is a fine illustration of spatial domain watermarking. *LSB* Watermarking method installs the watermark in the *LSB* of values of pixels. This strategy is generally does not produce genuine contortion to the picture; in any

case, it isn't highly vigorous against assaults. The insertion of the watermark is done by substituting the *LSB* of the watermark pixel with bits of watermark. The watermark might be dispersed all over the image or might be in the specific regions of the image. These type of procedures are not very much defensive against attacks and the watermark can be effortlessly decimated. This type of approach is exceptionally delicate to clamor and normal flag handling and can't be utilised as a part of functional applications.

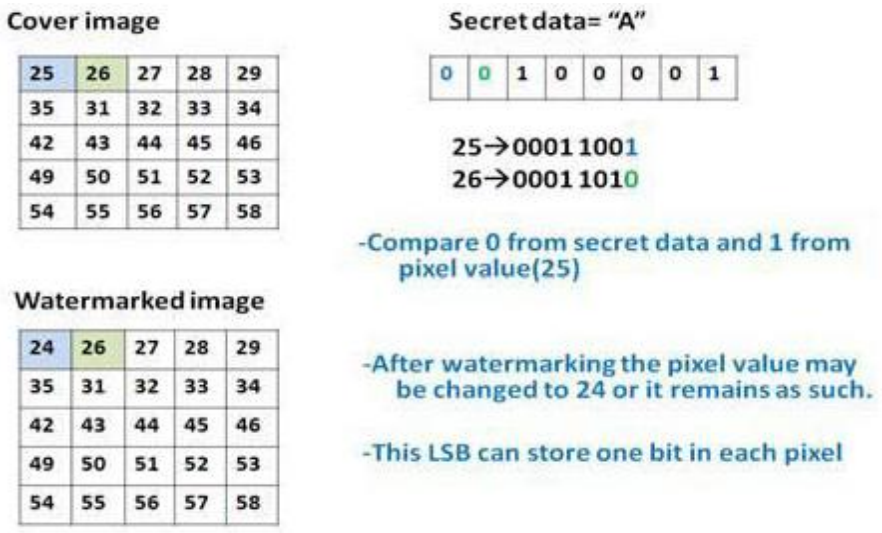


Fig 1.3. Process describing LSB Watermarking

In the event that we have a grayscale bitmap picture, we have each pixel which is of 8-bit size, we put information in the *LSB* of every pixel. In a grayscale picture every pixel is of 1 byte comprise of *8* bits. It represents the 256 colours between 0 which is for the dark to 255 which is for the white. The standard of encoding utilizes the *LSB* of every one of these bytes, the bit on the far right side. On the off chance that information is embedded to just the last two noteworthy bits of each pixel which is not recognizable to the human eyes.

To illustrate the *LSB* based example, the data shown in Fig 1.3. just the *LSB* of every pixel will be utilized for installing data. In the example the pixel value is 25 which is the '00011001' in binary and the watermark bit is 0, the watermarked value of the pixel will be '00011000' which is 24 in decimal. The next pixel value is 26 which is '00011010' in

binary and the watermarked bit is 0. As the *LSB* and the hiding bit both are 0. So it will remain 26.

1.6.2 Frequency Domain Watermarking

Frequency-domain watermarking methods are very frequently used in comparison to spatial domain techniques because they provide more robustness. In frequency domain the watermarks is embedded into the spectral coefficients of the image. Discrete Cosine Transform *(DCT),* Discrete Wavelet Transform *(DWT),* Discrete Fourier Transform *(DFT)* are the most commonly used frequency domain transforms.

1.6.2.1. Discrete Wavelet Transform

DWT is a new wavelet transform and is oftenly applied in digital watermarking and image processing. The transform is based on minor waves, referred to as wavelet, of limited duration and differing frequency. On applying this wavelet transform, the digital image is decomposed into three spatial directions, *i.e*. diagonal, vertical and horizontal. At one level decomposition the four sub bands are *LL*, *LH*, *HL* and *HH* and with further decomposition the two level sub bands are created as shown in Fig 1.4.

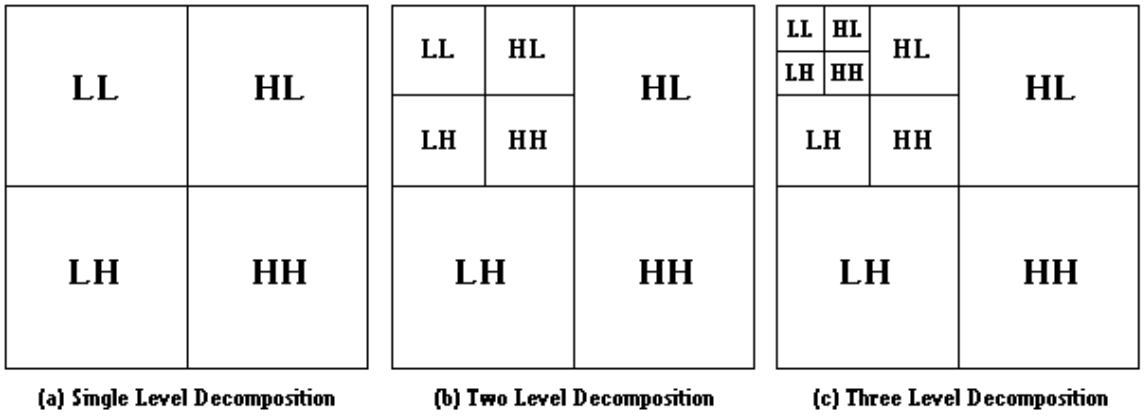


Fig 1.4. Sub Bands of the image after DWT

The *DWT* is presently implemented in diverse range of applications, such as removal of noise in audio, video and audio compression, and simulation of wireless antenna distribution. The main problem of the watermarking technique is to gain a better tradeoff between perceptivity and robustness. Robustness can be provided by enhancing the toughness of the implanted watermark, but it will also grow the visible distortion. However,

DWT is more favoured because it yields both a frequency dispersion of the watermark within the host image and a simultaneous spatial localization. The fundamental aim of *DWT* in digital image processing is to decompose the digital image into sub bands of different spatial domains and with independent frequencies.

1.6.2.2. Discrete Cosine Transform

The *DCT* separates a digital image into various recurrence groups, which makes it considerably less demanding to insert watermarking information into the middle recurrence groups of a digital image. The center recurrence (F_M) groups as shown in Fig 1.5 are picked to such an extent that they maintain a strategic distance from the most visual vital region of the picture having low frequencies (F_L) without over-presenting themselves to recurrence groups having high frequencies (F_H).

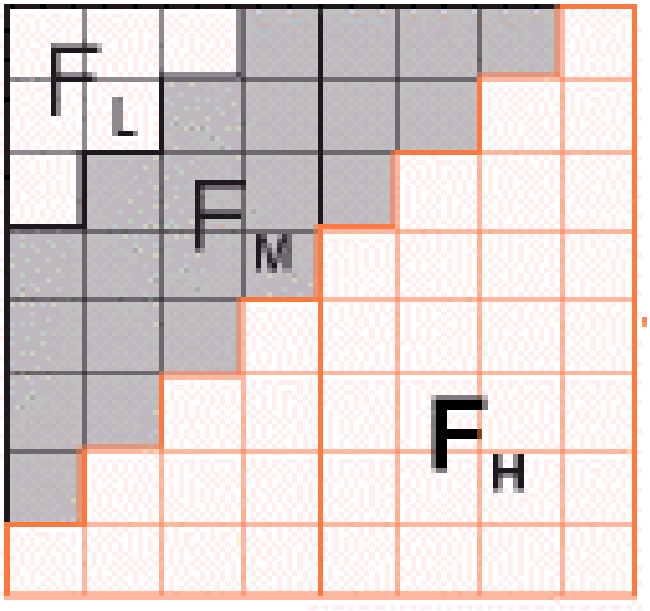


Fig 1.5. Recurrences groups after applying DCT

The DCT is described by the equation:

$$DCT(u,v) = \propto (u) \propto (v) \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y)\, cos\left[\frac{(2x+1)\pi u}{2M}\right] cos\left[\frac{(2y+1)\pi v}{2N}\right] \qquad (1.1)$$

where *(u, v)* and *(x, y)* are the co-ordinates of the image

$(M \times N)$ is the size of the image.

1.6.2.3. Discrete Fourier Transform

Discrete Fourier transform is applied in image processing to decompose image into its corresponding sine and cosine constituents. It transforms spatial domain of image into its frequency domain. Every point signifies a specific frequency carried by the spatial domain image. All the frequencies of the picture are not contained in *DFT* as it is sampled Fourier Transform but only a cluster of samples which are enough to show the spatial domain watermarking. The number of frequency and spatial domain pixels are of same size.

1.6.2.4 Singular Value Decomposition

SVD is linear algebra technique when applied does not change the image significantly. It is applied in various operations of digital image processing like image compression, noise reduction and data hiding.

For an image *I* of *N*×*N* size, the *SVD* is represented by the three matrices

$$[u\ s\ v] = svd(I)$$

$$u = \begin{bmatrix} u_{1,1} & \cdots & u_{1,n} \\ \vdots & \ddots & \vdots \\ u_{n,1} & \cdots & u_{n,n} \end{bmatrix}$$

$$s = \begin{bmatrix} \lambda_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda_n \end{bmatrix}$$

$$v = \begin{bmatrix} v_{1,1} & \cdots & v_{1,n} \\ \vdots & \ddots & \vdots \\ v_{n,1} & \cdots & v_{n,n} \end{bmatrix}$$

The matrices *u* and *v* are the orthogonal matrices and contains smaller singular values where as matrix *s* contains the larger singular values. With decomposing the image into the *u*, *s* and *v* matrices it could be used in the embedding process by modifying its singular values. This Method had got very much attention due its simple implementation.

1.6.2.5 Arnold Transform

Arnold Transform is an effective way of encrypting the image. It has been widely used for shuffling the watermark image. It was proposed by the Arnold [Huang (2004)] and it is defined by the equation as:

$$\begin{pmatrix} m' \\ n' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} m \\ n \end{pmatrix} (mod\ N) \tag{1.2}$$

where $(m, n)$are coordinates of the original watermark.

$(m'n')$ are the coordinates of the shuffled watermark.

$(mod\ N)$ is a modulo operator and *N* is the size of the watermark.

1.7 Image Quality Metrics

The Image Quality Metrics are the parameters which are used to analyze the changes in its quality after embedding, extracting and attacking process.

1.7.1. Peak Signal-to-Noise Ratio

PSNR determines the peak signal-to-noise ratio, in decibels, among the two images. This ratio is frequently used as an image quality metric among the host and the watermarked image. Higher the rate of *PSNR* is, better the imperceptibility of the watermarked image is.

$$PSNR = 10 \log_{10} \frac{\left(2^b - 1\right)^2}{MSE} \tag{1.3}$$

where *b* is bit depth of an image.

Mean Square Error *(MSE*) is also an image quality metric used for comparison between the image quality. *MSE* shows the cumulative squared error between the watermarked and the host image, and quantity of the peak error is *PSNR*.

MSE is evaluated as the root mean square of difference of the corresponding pixel values of the host image and watermarked image. Minimum the Mean Squared error is, better the watermarking is. The Mean Squared error can expressed as

$$MSE = \frac{\sum[I_1(i,j) - I_2(i,j)]}{M \times N} \quad (1.4)$$

where $I_1(i,j)$ is cover image pixel at *(i, ,j)* location

$I_2(i,j)$ is watermarked image pixel at *(i, j)* location

$M \times N$ is rows and columns of the image.

1.7.2. Bit Error Rate

Bit error rate is defined as the number of the bit changed during extraction to the bits that were embedded in cover image.

$$BER = \frac{\sum I_1(i,j) \oplus I_2(i,j)}{(M \times N)} \quad (1.5)$$

where $I_1(i,j)$ is original watermark image pixel at *(i, j)* location.

$I_2(i,j)$ is extracted watermark image pixel at *(i, j)* location.

$M \times N$ is rows and column of the image.

1.7.3. Bit Correction Rate

BCR implies greater resemblance between the host watermark and the extracted watermark. It is defined as the ratio of the bit remained unchanged during extraction to the bits that were embedded in cover image and is usually calculated as

$$BCR = 100 - BER \quad (1.6)$$

1.7.4. Normalized Correlation

This parameter is used to evaluate the quality among the original and the extracted watermark. The Expression for the Normal Correlation is

$$NC = \frac{\sum(x-\bar{x})\times(y-\bar{y})}{\sqrt{\sum(x-\bar{x})^2\times\sum(y-\bar{y})^2}} \quad (1.7)$$

where x is the pixel of watermark,

$\bar{x}$ is the mean of the watermark,

y is pixel of extracted watermark,

$\bar{y}$ is the mean of extracted watermark.

1.7.5. Similarity Index Modulation

This index is used to measure the similarity between the host and the watermarked image and it is expressed by:

$$SIM = \frac{\sum_i \sum_j I_1(i,j) \times I_2(i,j)}{\sum_i \sum_j [I(i,j)]^2} \quad (1.8)$$

where $I_1(i,j)$ is the original watermark where as the $I_2(i,j)$ is the extracted watermark.

1.8. Watermarking Attacks

The various watermarking attacks based on classification are described below.

1.8.1. Noise Attacks: (also known as "waveform attacks" and "simple attacks") are attacks that tries to dismantle the inserted watermark by distorting the entire watermarked information without identifying the part of the watermarked image where watermark is embedded. Examples include addition of noise (gaussian, salt & pepper), addition of an offset, compression (*JPEG, MPEG*), Digital to analog and analog to digital conversion and cropping and filtering.

1.8.2. Detection-disabling attacks: These attacks are done in order to make the recovery of the watermark impossible by the geometric detector. Its examples includes rotation, cropping, pixel permutations, geometric distortion like zooming, insertion and removal of pixels or its clusters.

1.8.3. Ambiguity attacks: These are attacks which tries to counterfeit by generating forged watermarked data or forged original data. The inversion attack is an example which discredits the control of the original watermark by inserting one or more watermarks make it unclear which was the original watermark.

1.8.4. Removal attacks: These attacks first processes the whole data of the watermarked image and then tries to divides the watermarked data into cover image data and the watermark. Examples includes certain filter operations, denoising, collusion attacks, or compression attacks like (e.g., 3-D models or using texture models).

1.9 Dissertation Outline

Thesis have been divided into six chapters. Chapter 1 contains the introduction and basic concepts related to the image watermarking. The Chapter 2 contains the literature Review of the content related to the watermarking. In Chapter 3 problem definition is given and in Chapter 4 proposed fragile watermarking algorithms are explained. In Chapter 5 results and descriptions of Chapter 4 algorithms are described. Finally Conclusion and Future work has been described in Chapter 6.

Chapter 2

Literature Review

This Chapter includes the research papers which includes the existing watermarking techniques which were used to develop the proposed algorithm. Here mainly the brief idea of the each paper is given. The most of the papers discussed here includes watermarking techniques based on *SVD*.

Ganic *et al.* (2004) had presented a hybrid non-blind algorithm based on *DWT* and *SVD*. The cover image was decomposed into four sub bands which were *LL*, *LH*, *HL*, and *HH*, then *SVD* was applied to each of the sub band, and then the singular values of the host image were modified with the watermark's singular values. Modification in the frequencies made a watermarking system which was robust to a many type of attacks. Their hybrid algorithm was compared with a pure *SVD*-based method, and showed that it was robust to attacks and more reliable.

Shieh *et al.* (2005) proposed a robust watermarking system for embedding grayscale watermarks into host images. The lossless objective were attained by inserting the singular values computed from *SVD* of the cover image into the watermark. The image quality parameters proves that the proposed method ensures the extracted watermark has the mean *PSNR* value of 24.91 *dB* and the worst *PSNR* values of 19.96 *dB*, respectively. With addition to the assurance of the standard of image quality of extracted watermark, chaos permutation is also applied to the referenced watermark to further increase the strength. The proposed method provided better robustness from various watermarking attacks and is more efficient in comparison to other grayscale watermarking algorithm.

A digital watermarking method based on *SVD* using *GA* had been presented by **Aslantas** (2008). During the embedding process, the singular values of the cover image were remodeled by multiple scaling factors. Modifications were optimized using genetic algorithm and the highest of the possible robustness were obtained without losing the transparency.

Saha *et al.* (2010) had presented an overview of few possible attacks which may causes threat to currently used watermarking techniques. They had determined the attacks which oftenly targets several of the well-known fragile and semi-fragile watermarking techniques.

An algorithm for finding the simultaneous *SVD* had been proposed by **Maehara** and **Murota** (2011) on the basis of schemes of Maehara–Murota and Murota–Kanno–Kojima–Kojima for simultaneous block-diagonalization of square matrices under orthogonal (or unitary) similarity. They called this the simultaneous *SVD* motivated by the fact that the simultaneous *SVD* is uniquely determined by the unique case where N = 1, a matrix is provided and it reduced to the normal *SVD* with the help of the theory of bi-module and algebra.

Dogan *et al.* (2011) has proposed a scheme for watermarking with *SVD*. The proposed algorithm is based on improved *SVD* has been improved for colour image in the paper. *SVD* had been used for hiding information on digital image files which falls under in the frequency domain. In *SVD* centered watermarking technique, the watermark is inserted by changing the *LSB* of the singular value matrix.

A digital image watermarking algorithm by using a tiny genetic algorithm and *SVD* and having robustness is proposed by **Lai** (2011). The non-symmetric and one-way properties of *SVD* makes watermarking techniques easy for implementation. The singular values produced vary very small under several operations of image processing and attacks are very stable. In the proposed algorithm, embedding the watermark image, the singular elements of a host image are amended by numerous scale factors. The Tiny-GA was used to find the correct values in order to raise the robustness of the algorithm and the imperceptibility standard of the watermarked image as the values of scale factors were used to find the strength of watermark.

Ramamurthy and **Varadarajan** (2012) had compared two novel principles for embedding watermark into the original image using quantisation based on *DFIS* and *BPNN*. The host image was decomposed up to three levels using *DWT* and quantization. The bitmap was chosen as a watermark. The *DFIS* was used to create the watermark weighting function for embedding and extracting the imperceptible watermark in one method while in the other

method the *BPNN* was implemented to embedding and extracting the watermark. The suggested watermarking algorithms were imperceptible and robust to normal attacks.

Jose *et al.* (2012) had proposed a Hybrid digital watermarking process based on *DCT – DWT - SVD*. The host image was re-arranged before applying the *DCT*. The *DCT* coefficients of the re-arranged image were decomposed into sub bands by applying *DWT*. The singular quantities of the central sub bands were determined and then watermark was embedded.

Su *et al.* (2013) has proposed an algorithm based on *SVD* which is blind in nature. By examining the orthogonal matrix of u after applying *SVD*, it is determined that there is a huge correlation between the elements of the second row of first column and the third row of first column. This similarity for image watermarking was utilized for this work. Firstly, the non-overlapping block having the size 4 × 4, of each sub band in colour original image is determined by using *SVD*. Then the value from the second row of the first column element and third row of the first column one of u matrix was slightly reorganized for embedding the colour watermark, and the modified relation was utilized for extracting the watermark. Without depending up on the original cover image and cover watermark image, the implanted watermark was easily extracted.

Su *et al.* (2013) had proposed an image watermarking process based upon the upgraded compensation of *SVD* for implanting the watermark image into the cover image. First, the bits of watermark were inserted into 4 × 4 block by reorganizing the elements of second row of the first column and third row of the first column of u matrix after applying *SVD*. Then, the block which was embedded in cover image, was compensated by the improved optimisation operation for getting greater *PSNR* and higher threshold *T*. By using the relation between the changed elements of *u* matrix, the watermark was extracted from the watermarked image after performing various attacks without depending on the original data.

Ghazy *et al.* (2014) had compared between the proposed algorithm for implanting encrypted watermarks and the traditional method of Liu. A diffusion based encrypting method and permutation based encrypting method were also compared as the watermark

encryption algorithms. Quality parameters had shown that the proposed algorithm is better than traditional method of Liu for watermarking operations even after attacks.

DWT with Haar filter for embedding a binary watermark image in picked coefficient blocks had been proposed by **AL-Nabhani** *et al.* (2015) and then a *PNN* was used for extracting the watermark image. For evaluation of the proficiency of the quality and the algorithm for extracting the watermark images, commonly used image quality metrics, such as *NC* and *PSNR* were used. Observations shows the better invisibility of the extracted watermark image with *PSNR* of 68.27 *dB* and the *NC* at 0.9779. Results are showing that the proposed watermarking technique yields robustness and better imperceptibility to common attacks such as median filter, cropping, rotation, *JPEG* compression and Gaussian noise.

Caragata *et al.* (2015) has proposed a new algorithm that is based on the cryptanalysis of the *CWSA* algorithm. The proposed algorithm is robust from cryptanalysis, less perceptible, faster and also preserves the advantages of *CWSA*. It uses two chaotic maps: a chaotic generator which comprises of two perturbed recursive filters with a nonlinear function, which is Skew Tent map and the piecewise linear chaotic map.

Singular-value-based semi-fragile watermarking system had been proposed by **Qi** and **Xin** (2015) mainly to be used for image content authentication. In this method, watermark dependent on content was created by a *SVD* based sequence and watermark independent of content was created by a private-key-based sequence. For embedding the quantisation process was used and for extraction the parity of the quantization was used. Experiments results are showing the method to be better in providing the authentication.

Makbol *et al* (2015) had suggested as a method to achieve digital protection by reorganizing several elements in *u* matrix on the low sub-band obtained by *SVD*. Before this DWT was applied. Parameters are showing the method to be more efficient.

Keshavarzian *et al.* (2016) has proposed a blind and robust watermarking algorithm based on Region of Interest using the Arnold Transform. In proposed algorithm first a watermark is produced from the original image and then the embedding process is used with Arnold scrambling. In proposed algorithm, the Region of Interest of the original image is used for

production of another image which is further used as watermark. In next step First level of DWT is implemented on the watermark and for embedding, approximation coefficients are used as data. In the sub band having low frequency of the chosen block of the cover image in the wavelet domain each approximation coefficient is embedded. Arnold Transform is implemented on the approximation coefficients of the watermark before embedding, even to the blocks of cover image also.

A system for an invisible and secure watermarking is proposed by **Saikrishna N** and **Resmipriya M G** (2016). The host image was classified into white and black textured areas by the determined location of embedding through initially entered key. The watermark image is then transformed by applying Arnold scrambling. *DWT* technique is used for inserting the transformed watermark into the regions having white textures. For extracting the watermark same key is entered which was already entered during embedding.

Sai *et al.* (2016) described the relative work of Truncated *DWT-SVD* and *DCT-SVD*. In the paper two distinct approaches had been proposed to determine the feature vector for image retrieval method based on content. *DWT* is used for the decomposed image measured for grayscale image, *YCbCr* color image and *RGB* and *SVD* feature for successively truncated *DCT* image. Truncated *DCT*, *DWT* decomposition and *SVD* features of the image determined up to fifth level for comparison of the performance. Proposed technique includes the using of *SVD* of coefficients of *DWT* and *DCT* of the image having low frequency for computing the multidimensional features vector. Bray Curtis distance and Euclidean Distance were measured between the query image and database image.

Sharma *et al.* (2016) discussed basic concepts of digital watermarking and its properties, general watermark embedding and extraction process, important attacks on watermark system, important transform and machine learning techniques and some transforms and spatial domain based watermarking method using machine learning.

Durgesh Singh and **Sanjay K. Singh** (2016) had proposed a watermarking algorithm for copyright protection based on *DCT*, *DWT* and *SVD* with Arnold Cat Map encryption. *DCT* coefficients of *MSB* and *LSB* values were inserted into the central singular values of each block having dimensions of 4×4 of the cover image's sub band after applying one level

DWT. Proposed scheme is able to solve problem of unauthorised reading and false-positive detection and is robust.

Haddada *et al.* (2017) proposed a watermarking technique that safeguards the security of the biometric data of the person and the computational complication of the proposed technique. The better visual standards of the watermarked image and reduced storage space had been maintained. The biometric used are fingerprint and face, which are developed ones in biometric watermarking algorithms and among the most frequently deployed. The same watermarking method is implemented two time in sequence. First, the minutia of the fingerprint is watermarked in face of a person. Then, the formerly watermarked face image is embedded into the cover image of fingerprint as additional data. The interesting performances in individuals' verification had been shown by the watermarked image. By various tests performed, robustness to several signal processing attacks had been demonstrated by the proposed algorithm.

Kumar *et al.* (2017) provided a way of digital watermarking system by the use of homomorphic encryption methods by using biometric image as watermark. It provided authenticity and data confidentiality also. The biometric image was embedded in to the benchmark images. Robustness of the embedded watermarks in the host images are demonstrated through image quality metrics such as Correlation coefficient, noise test and *PSNR*. The biometric images were acquired by eliminating watermarked images with the benchmark images.

Loukhaoukha *et al.* (2017) are using the *SVD* and redundant discrete wavelet transform (*RDWT*) and are describing two ambiguity attacks on the method that fails when it is used in the application having robust features like transaction tracking, owner identification and proof of ownership.

Panda *et al*. (2017) proposed an optimised *DWT-SVD* based watermarking algorithm using *GA*. The singular values of the watermark picture were added along with a proper scaling factor in order to alter the singular value section of the cover image. In order to provide the greater values and robustness without decreasing the transparency of the watermark scaling factor was optimised by *GA* with *PSNR* used as the fitness criteria. Further analysis were implemented by using the *NC* as a fitness function to determine the results in robustness.

A digital watermarking scheme with *SVD* and Online Sequential Extreme Learning Machine (*OSELM*) in the Integer Wavelet Domain (*IWT*) domain had been proposed by **Dabas** *et al.* (2017) for the copyright protection. It is blind in nature. *SVD* had been implemented on the coefficient blocks during the embedding process in order to get the singular values in the *IWT* domain. For embedding the watermark in the original image singular values were modulated. For learning the correlation between the original coefficient and the watermarked coefficient an *OSELM* was trained. During the extraction process, host image was not needed during extraction process as the trained *OSELM* was used for extracting the embedded watermark blindly. The watermarked image was manipulated using watermarking attacks like rotation, noise, blurring, and cropping and sharpening. Image Quality metrics showed that the proposed watermarking algorithm was more robust to various watermarking attacks. The watermark extracted was very analogous to embedded watermark and worthy for ownership verification.

Ma *et al*. (2018) had surveyed the currently used algorithm and applications for the integration of infrared images and the visible images. They had proposed the fusion of these two kinds of images, which combined the benefits of detailed texture data in visible images and thermal radiation data in infrared images.

Solorio *et al* (2018) had proposed an algorithm in which two series of reference bits of the five most significant bit-planes of the image were generated. Some authentication bits and reference bits were then assigned to the three least significant bit-planes (*LSBP*s) of the image. The verified bits were used by the receiver to localize the changed pixel-blocks. An iterative restoration mechanism was executed to determine the genuine value of the watermarked pixels.

Peng *et al* (2018) proposed a method where hiding of secret information was done, which is reversible in nature with two indistinguishable cover images and the classified data was watermarked in one cover image. The distortion data was hidden in the, another host image. For determining authenticity, comparison between the extracted information from the image and the original authenticated data is done to find whether the image was tampered or not. Image quality parameters shows that the recommended scheme improved the effectiveness of tamper detection as well as quality of image.

Sangeetha *et al.* (2018) had proposed a method for digital image watermarking method by using the entropy of original images and texture of the watermarks. The evaluation of the Entropy is done by the coefficients determined by applying *DWT* of the host image were used. The sub band with the greatest entropy were chosen for implanting the texture of watermark. Watermark was texturised by using the Arnold Scrambling and texture was randomly selected. Texture was embedded instead of watermark itself to increase the level of security. The experimental results were showing the method to be effectively extracting the watermark.

.

Chapter 3

Problem Formulation

In the world where the data is in abundance and its security is becoming a real problem. The digital data present in the form of images and audio is always under the threat of being stolen or misused.

In the age of Internet where one siting in one corner of world can launch a wave of cyber-attack. It is important to know whether data available to us is authenticated and the original or not, it is tampered or not.

3.1 Gaps

In the light of the Literature Review conducted on the existing watermarking algorithms following gaps have been found:

- Most of the *SVD* based algorithms are non-blind in nature.
- Mostly algorithms are having the false positive problem.

3.2 Objectives

On the basis of the identified gaps, following objectives are defined:

- To design false positive detection free watermarking algorithm.
- To design a blind watermarking algorithm.

Chapter 4

Oblivious Fragile Watermarking Algorithms

4.1 Introduction:

In this chapter two blind algorithms for grayscale images have been proposed out of which one is only in wavelet domain with *SVD* and other is *DWT, DCT* and *SVD* based.

The first algorithm is, Entropy based blind watermarking algorithm using DWT and $S\,VD$. A binary watermark is hidden into the singular value of the non-overlapping blocks of DWT sub-band having maximum entropy. After applying DWT to the host image, further sub-band having maximum entropy is decomposed into 4×4 sized non overlapping blocks. SVD is then applied on each 4×4 block and then watermark is embedded into one of the singular value of each block. Singular value should be chosen so that imperceptibility as well as good quality of extracted watermark is feasible in the proposed algorithm.

Where, as in second algorithm, Watermarking using *DWT, DCT* and *SVD* had been proposed. DWT is implemented on the host image and then it is decomposed into 4×4 sized non overlapping blocks. Then *DCT* and *SVD* is implemented on the blocks and a watermark is embedded into the singular value of the non-overlapping blocks.

4.2 Entropy based Watermarking Algorithm using DWT and SVD

The property of the SVD domain is to modify the host image by some watermark. Singular values of the coefficients of the matrix in each block. In order to use the characteristics of the *SVD* domain to embed a watermark into a host image, it is normally identified that bigger the singular value utilized for watermark embedding, lesser the Impact of watermark on host image. The number of designated singular values are similar as the amount of pixels in watermark image but good quality of extracted watermark. These factors support the idea behind developing a SVD based watermarking algorithm.

4.2.1 Embedding Method:

Embedding method of the proposed algorithm is shown in Fig 4.1 and steps are explained below:

Step 1: Decompose the host image H into four sub-bands, HL, LH, HH and LL using DWT and $Haar$ wavelet.

$$[LL, LH, HL, HH] = DWT(H, 'haar')$$

Step 2: Find out the entropy of each band. Choose the band for embedding having maximum entropy.

$$X_{sub} = Max\_entropy(LL, LH, HL, HH)$$

$$where\ X_{sub}\ is\ the\ sub\ band\ with\ maximum\ entropy$$

Step 3: Divide the selective band having maximum entropy into non-overlapping blocks of dimension 4×4.

Step 4: Apply the SVD on each non-overlapping blocks of each sub-band.

$$[u, s, v] = svd(B_i)$$

$$where\ , i\ is\ the\ corresponding\ block$$

Step 5: Read the watermark W and shuffle it using Arnold transform.

Step 6: Modify the singular values for embedding the watermark bit W by performing following steps:

- If watermark bit is '1' and the largest singular value is odd then there will be no variation in the singular value otherwise increment the singular value by one.
- If watermark bit is '0' and largest singular value is even then there will be no variation in the singular value otherwise increment the singular value by one.

Step 7: Apply inverse SVD on every block and then join all blocks to restore the sub band.

Step 8: Apply inverse wavelet $IDWT$ to obtain watermarked image W'.

$$W' = IDWT(X_{sub}, HL, LH, HH, 'haar')$$

(assuming LL is having maximum entropy)

To increase watermarking security, a pseudo random number generator (*PRNG*) is adopted to select the block from where watermark bit start embedding.

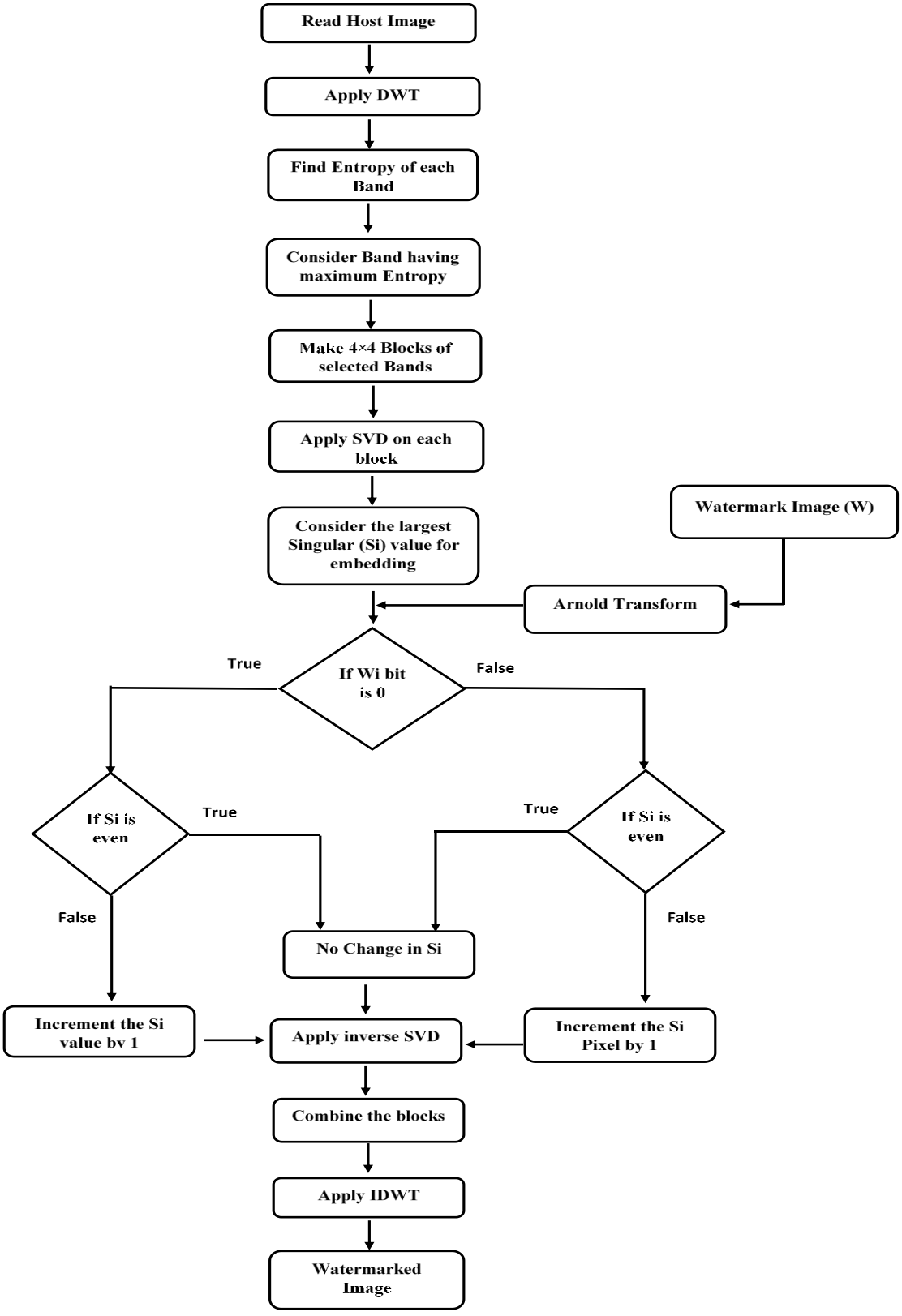


Fig 4.1 Flowchart Depicting Embedding method of Entropy based Algorithm using DWT and SVD

4.2.2 Extraction Method:

Extraction method of the proposed algorithm is shown in Fig 4.2 and steps are discussed below:

Step1: Apply DWT on the watermarked image W' to form sub bands

$$[LL, LH, HL, HH] = DWT(W', 'haar')$$

Step 2: Find the entropy of each sub-band and select the sub-band having maximum entropy.

$$Max\_entropy(LL, HL, LH, HH)$$

Step 3: Divide the selected sub-bands into 4×4 blocks.

Step 4: Apply SVD to every block by

$$[u, s, v] = svd(B_i)$$

Step 5: Largest singular value of every block is obtained.

- If singular value is even then watermark bit =0
- If singular value is odd then watermark bit =1

Step 6: Apply Anti Arnold on extracted watermark.

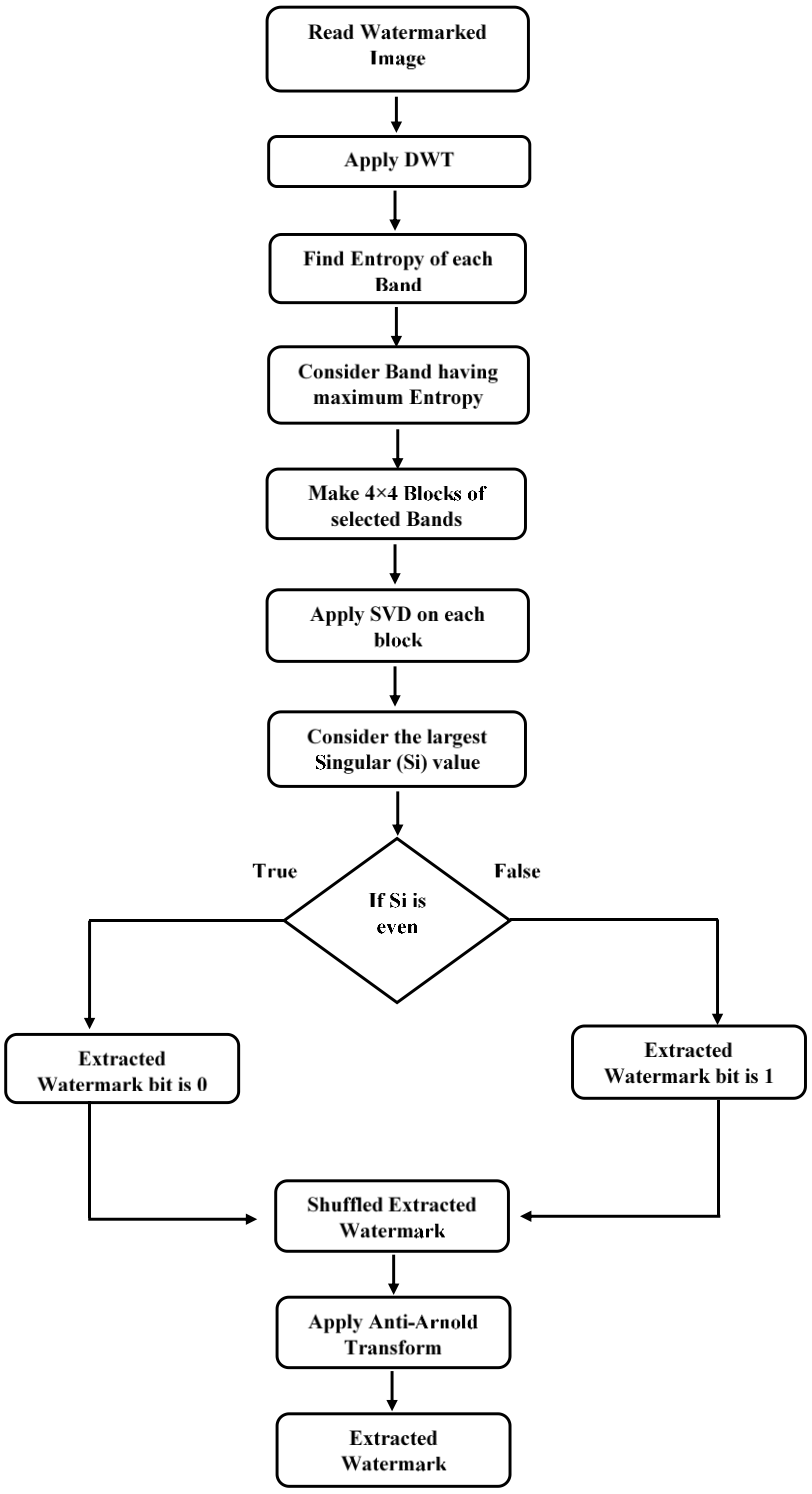


Fig 4.2 Flowchart depicting Extraction method of Entropy based Algorithm using DWT and SVD

4.3. Algorithm based on DWT, DCT and SVD

The algorithm proposed with using the concepts of the *DWT*, *DCT* and *SVD*. The algorithm will be having Embedding and the Extraction method which are explained with Steps and detailed flowchart

4.3.1. Embedding method

Embedding method of the proposed algorithm is shown in Fig 4.3 and steps are explained below:

Step 1: Consider the host image and apply single level DWT on the host image to divide it into four sub bands LL, LH, HL and HH.

$$[LL, LH, HL, HH] = DWT(H, 'haar')$$

Step 2: Divide the sub band LL into non-overlapping block of 4×4 elements.

Step 3: Apply DCT on each block of sub band

$$DCT(B_i)$$

Step 4: Execute *SVD* operation on each and every blocks of the Sub band.

$$[u_i\ s_i\ v_i] = svd(B_i)$$

Step 5: Read the watermark and apply Arnold Transform on it.

Step 6: Modify the singular value Si of the block bi with the watermark data by the following steps

- If watermark bit is '1' and the largest singular value is odd then there will be no variation in the singular value otherwise increment the singular value by one.
- If watermark bit is '0' and integer part of the singular value is even then there will be no variation in the singular value otherwise increment the singular value by one.

Step 7: Perform inverse *SVD* on ach and every blocks, and merge the modified Sub band.

Step 8: Implement inverse of *DCT* to each block.

Step 9: Apply single-level inverse Haar $IDWT$ to obtain the watermarked image

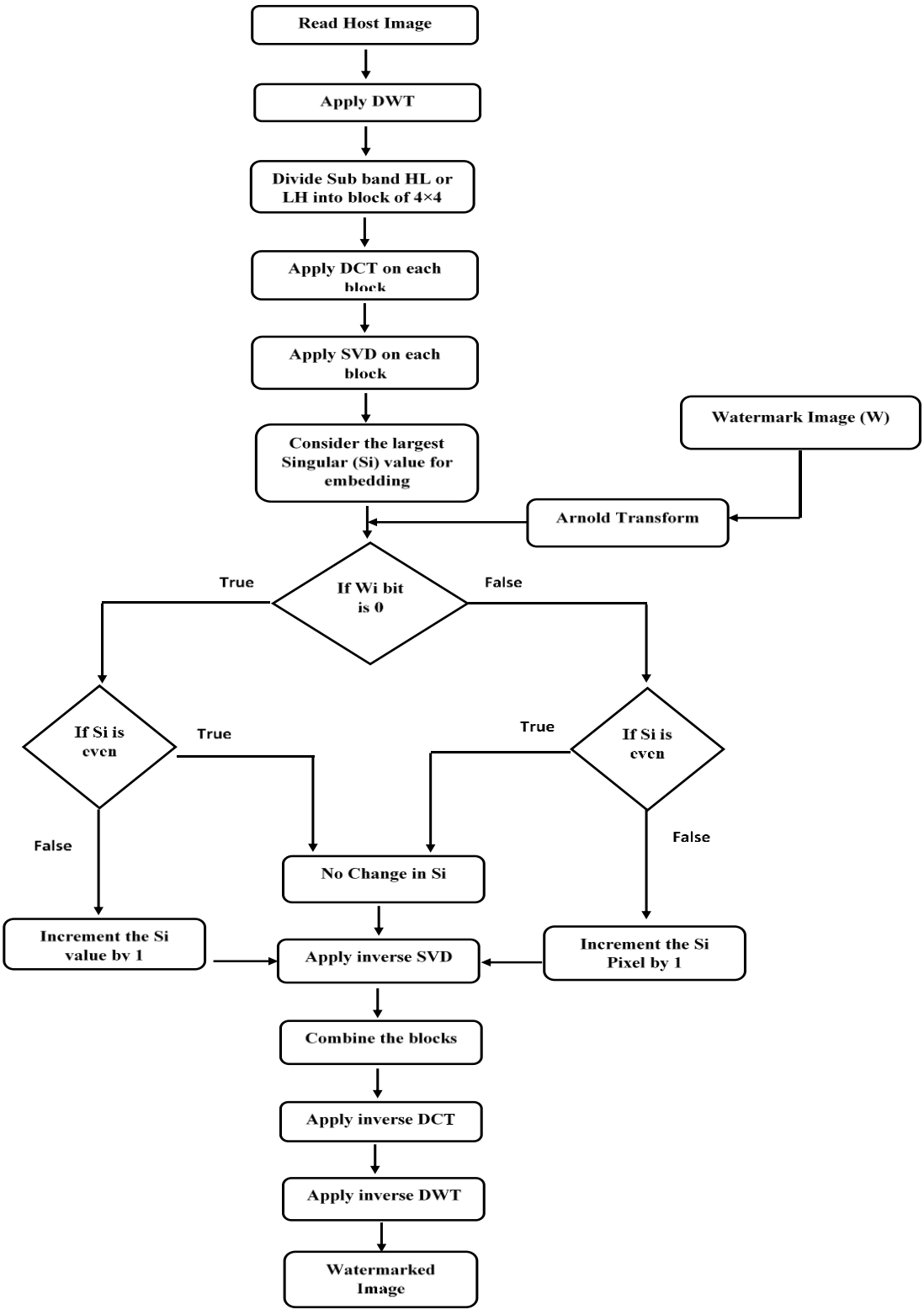


Fig 4.3. Flowchart depicting Embedding method of Algorithm based on DWT, DCT and SVD

4.3.2 Extraction method

Extraction method of the proposed algorithm is shown in Fig 4.4 and steps are discussed below:

Step 1: Consider the host image and apply single level DWT on the host image to divide it into four sub bands LL, LH, HL and HH.

$$[LL, LH, HL, HH] = DWT(W', 'haar')$$

Step 2: Divide the sub band HL or LH into non-overlapping block of 4×4 elements.

Step 3: Apply DCT on each block of sub band

$$DCT(B_i)$$

Step 4: Implement SVD on all blocks of the Sub band.

$$[u_i\ s_i\ v_i] = svd(B_i)$$

Step 5: largest singular value of each block is obtained.

- If singular value is even then watermark bit =0
- If singular value is odd then watermark bit =1

using above steps shuffled watermark is extracted.

Step 6: Apply the Anti-Arnold Transform on shuffled watermark to get extracted watermark.

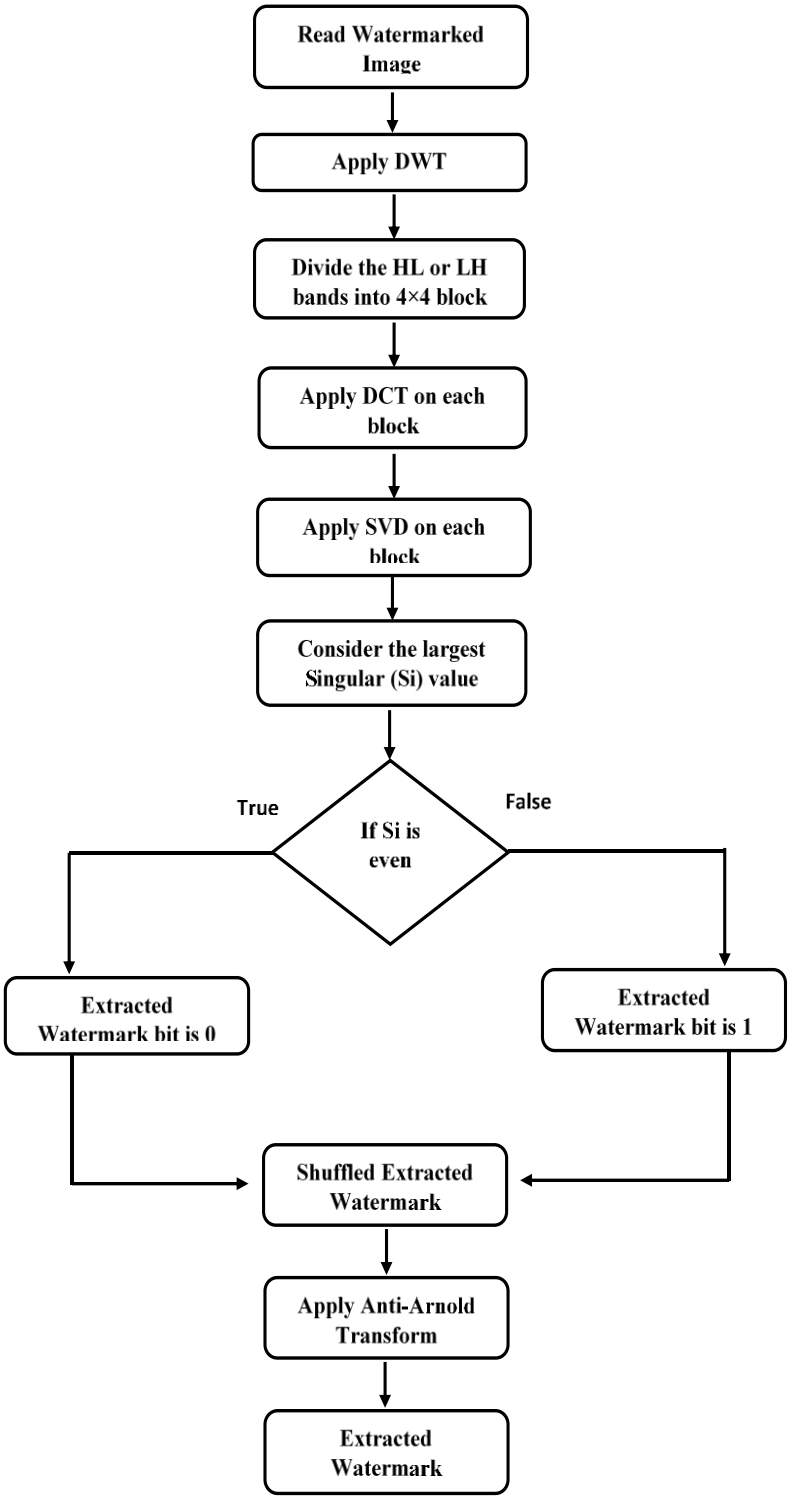


Fig 4.4. Flowchart depicting Extracting method of Algorithm based on DWT, DCT and SVD

Chapter 5

Experimental Results

In this chapter, we have discussed results of two blind watermarking algorithms which are mentioned in Chapter 4.

Proposed watermarking algorithms are implemented in MATLAB. To analyse the performance of the proposed algorithms, few images like Baboon, Boat, Lena, Girlface, Crowd and Zelda are considered as host image for experiment. All these images are of size 512 × 512 and some of these are shown in Fig 5.2. The considered watermarks are logo and copyright of size 32 × 32 are shown in Fig 5.1 (a) and (b)

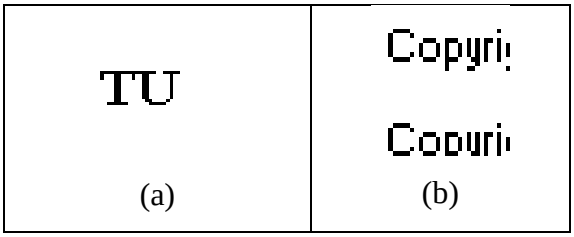
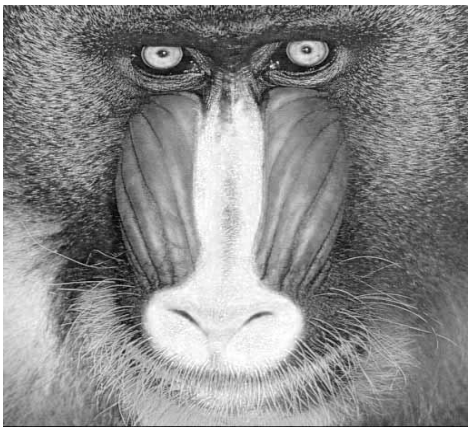


Fig 5.1 Watermarks (a)logo image (b)copyright image

5.1 Entropy based Algorithm using DWT and SVD

Using this algorithm, watermarked images are formed, which are shown in Fig 5.3. If we compare the watermarked image with their host image, the visual quality of both are similar *i.e* they maintains the imperceptibility.

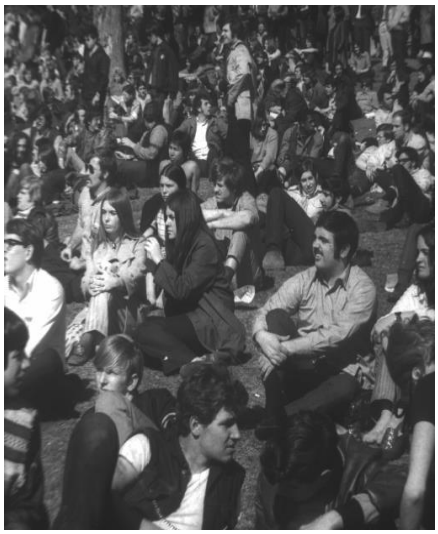


(a) Baboon

(b)Boat

(c) Lena

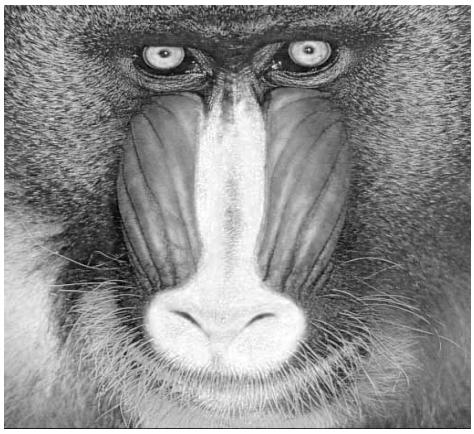
(d)Girlface



(e) Crowd

(f) Zelda

Fig 5.2 Host images



(a) Baboon

(b)Boat

(c) Lena

(d) Girlface

(e) Crowd

(f) Zelda

Fig 5.3: Watermarked Images by Entropy based Algorithm using DWT and SVD

The entropy of each sub band of host images and *PSNR* between host and watermarked images after embedding 32 ×32 copyright watermark is shown in table 5.1

Table 5.1: Entropy of the Sub-bands of the host images and *PSNR* (*dB*) between host and watermarked images after embedding 32 ×32 copyright watermark.

	Baboon		Boat		Lena	
Images Subband	Entropy	PSNR	Entropy	PSNR	Entropy	PSNR
LL	0	4.737	0	5.361	0	4.829
HL	1.1516	25.163	1.253	33.638	1.255	33.449
LH	1.1569	75.147	1.217	30.328	1.232	33.285
HH	1.336	29.743	1.275	75.189	1.421	75.156

	Girlface		Crowd		Zelda	
Images Subband	Entropy	PSNR	Entropy	PSNR	Entropy	PSNR
LL	0.138	6.478	0	8.247	0	5.464
HL	1.308	33.481	1.323	32.837	1.337	37.105
LH	1.385	73.386	1.316	33.634	1.260	33.880
HH	1.435	35.044	1.404	74.893	1.367	72.462

From Table 5.1 we conclude that, diagonal sub bands of *DWT* have maximum entropy and *PSNR* is also indication to high imperceptibility.

In order to show the goodness of algorithm, Tables 5.2 and 5.3 contains the *PSNR* between host and watermarked images, *NC, BCR, BER, SIM* between original watermarks and extracted watermarks, and the watermark extracted from different watermarked images obtained is shown .

Table 5.2: $PSNR$ (*in dB*) between host and watermarked image, *NC*, $BCR(in\ \%)$, $BER(in\ \%), SIM$ between original copyright watermark and extracted watermark, and watermark extracted from different watermarked images.

	Baboon	Boat	Lena	Girlface	Crowd	Zelda
PSNR	75.147	75.189	75.156	73.386	74.893	72.462
NC	1	1	1	1	1	1
BCR	100	100	100	100	100	100

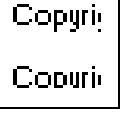
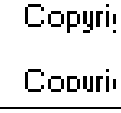
BER	0	0	0	0	0	0
SIM	1	1	1	1	1	1
Extracted Watermark						

Table 5.3: $PSNR$ (*in dB*) between host and watermarked image, *NC*, $BCR(in\ \%)$, $BER(in\ \%), SIM$ between original logo watermark and extracted watermark, and watermark extracted from different watermarked images.

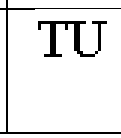
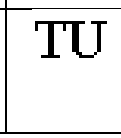
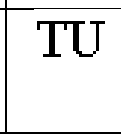
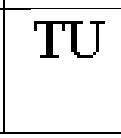
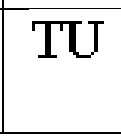
	Baboon	Boat	Lena	Girlface	Crowd	Zelda
PSNR in dB	74.387	74.547	74.493	72.687	74.310	71.797
NC	1	1	1	1	1	1
BCR	100	100	100	100	100	100
BER	0	0	0	0	0	0
SIM	1	1	1	1	1	1
Extracted Watermark						

Table 5.2 and 5.3 summarizes the performance of the entropy based proposed algorithm after embedding watermark of size 32×32. The $PSNR$ between host image and watermark image is about $70\ dB$ it maintains the imperceptibility, visual quality of watermarked image is better whereas *NC* and *SIM* between original and extracted watermark is '1' , BCR is 100 and BER is 0 % which depicts the extracted watermark image quality is exactly similar to the original watermark.

In order to use characteristics of *SVD* domain to embed a watermark in host image, different singular values are used for determining image quality metrics. As we apply the *SVD* on 4×4 block, four non-zero singular values. Tables 5.4 to 5.7 shows which nonzero singular values gives better imperceptibility and extraction of watermark after embedding.

Table 5.4: $PSNR\ (dB)$ between watermarked and host image, NC, $BCR\ in\ (\%), BER\ in\ (\%)$ and SIM between original and extracted watermark without any attack embedded in $S(1,1)$ and image of extracted watermark.

	Baboon	Boat	Lena	Girlface	Crowd	Zelda
PSNR	75.147	75.189	75.156	73.386	74.893	72.462
NC	1	1	1	1	1	1
BCR	100	100	100	100	100	100
BER	0	0	0	0	0	0
SIM	1	1	1	1	1	1
Extracted Watermark						

Table 5.5: $PSNR\ (dB)$ between watermarked and host image, NC, $BCR\ in\ (\%), BER\ in\ (\%)$ and SIM between original and extracted watermark without any attack embedded in $S(2,2)$ and image of extracted watermark.

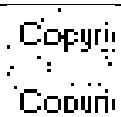
	Baboon	Boat	Lena	Girlface	Crowd	Zelda
PSNR	75.274	75.181	75.438	73.270	75.634	72.445
NC	1	0.983	0.916	0.909	0.901	0.934
BCR	100	99.609	97.949	97.753	97.656	98.437
BER	0	0.390	2.050	2.246	2.343	1.562
SIM	1	1	1	1	1	1
Extracted Watermark						

Table 5.6: $PSNR\ (dB)$ between watermarked and host image, NC, $BCR\ in\ (\%), BER\ in\ (\%)$ and SIM between original and extracted watermark without any attack embedded in $S(3,3)$ and image of extracted watermark.

	Baboon	Boat	Lena	Girlface	Crowd	Zelda
PSNR	75.040	75.215	74.958	73.905	74.949	72.487
NC	0.987	0.971	0.758	0.8302	0.834	0.897
BCR	99.707	99.316	92.773	95.605	95.507	97.363
BER	0.293	0.683	7.226	4.394	4.492	2.636

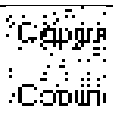
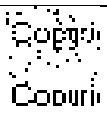
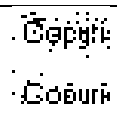
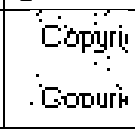
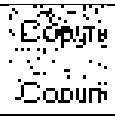
SIM	1	1	1	1	1	1
Extracted Watermark						

Table 5.7: $PSNR\ (dB)$ between watermarked and host image $NC, BCR\ in\ (\%), BER\ in\ (\%)$ and SIM between original and extracted watermark without any attack embedded in $S(4,4)$ and image of extracted watermark.

	Baboon	Boat	Lena	Girlface	Crowd	Zelda
PSNR	74.765	74.592	73.315	71.871	73.568	71.246
NC	0.970	0.949	0.449	0.739	0.513	0.819
BCR	99.316	98.828	71.679	92.089	77.050	95.312
BER	0.683	1.171	28.320	7.910	22.949	4.687
SIM	1	1	1	1	1	1
Extracted Watermark						

After observing the *PSNR* values for different images in the given tables we observed that data embedded into highest singular value gives better *PSNR i.e* imperceptibility maintained and *BCR* having value above 90 and very low *BER*, it infer that quality of extracted watermark is comparable to original watermark.

To show the fragility of the watermarking algorithm, different attacks on the watermarked image have been applied. After applying these attacks the values of *NC*, *BCR* and *BER* between original and extracted watermark are tabulated in Table 5.8

Table 5.8: *NC, BCR* and *BER* between original and extracted watermark after attack on watermarked image.

Image	Attacks	NC	BCR	BER
Baboon	Averaging Filtering	0.057	51.85	48.14
	JPEG Compression	0.017	13.28	86.71
	Salt & Pepper	0.012	13.183	86.816
Boat	Averaging Filtering	0.015	14.74	85.25
	JPEG Compression	0.025	13.08	86.91
	Salt & Pepper	0.0242	13.476	86.523

Lena	Averaging Filtering	0.04	18.06	81.93
	JPEG Compression	0.01	13.08	86.91
	Salt & Pepper	0.012	13.183	86.816
Girlface	Averaging Filtering	0.027	35.05	64.94
	JPEG Compression	-0.050	16.21	83.78
	Salt & Pepper	0.010	16.406	83.593
Crowd	Averaging Filtering	-0.017	17.96	82.03
	JPEG Compression	-0.01	13.08	86.91
	Salt & Pepper	0.012	13.183	86.816
Zelda	Averaging Filtering	-0.004	14.06	85.91
	JPEG Compression	-0.004	13.08	86.91
	Salt & Pepper	0.017	13.085	86.914

From Table 5.8, we can conclude that after attacking the watermarked image by average filtering and salt n pepper noise the *NC* values are very less and *BCR* value is also below 50 %, which shows the watermarking scheme can be used for fragile watermarking.

In Table 5.9 the *PSNR* between host and watermarked image after embedding copyright watermark of different sizes are tabulated.

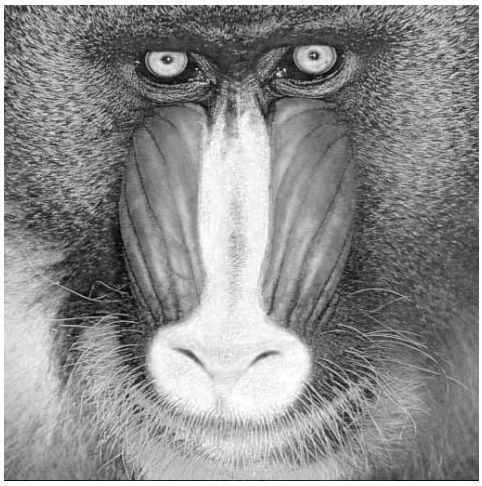
Table 5.9: *PSNR* (*dB*) for 32×32 , 56×56 *and* 64×64 copyright watermarks.

Image\size	**32×32**	**56×56**	**64×64**
Baboon	75.147	70.239	69.150
Boat	75.189	70.398	69.244
Lena	75.156	70.272	69.135
Girlface	73.386	68.544	67.371
Crowd	74.893	70.331	69.319
Zelda	72.462	67.730	66.568

From Table 5.9 we can conclude that on embedding different sizes of watermark, the *PSNR* is greater than or near to 70 *dB.*

5.2 Algorithm based on DWT, DCT and SVD

By implementing this proposed algorithm, watermarked images are formed, which are shown in Fig 5.4. If we compare the visualization of the watermarked image with their host images, then we notice that they both look similar, *i.e* they maintained the imperceptibility.

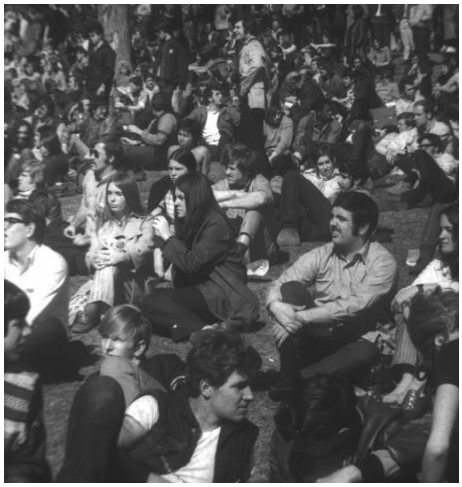


(a) Baboon

(b)Boat

(c) Lena

(d)Girlface



(e) Crowd

(f) Zelda

Fig 5.4 Watermarked Images from Algorithm based on DWT, DCT and SVD

In order to show the goodness of algorithm, Tables 5.10, 5.11,5.12 and 5.13 contains the *PSNR* between host and watermarked images, *NC, BCR, BER, SIM* between original and extracted watermark, and the extracted watermark image from different watermarked images obtained is shown .

Table 5.10: *PSNR* (*in dB*) between host and watermarked image, *NC, BCR (in %), BER (in %)* and *SIM* between 32×32 original and extracted watermark, and watermark extracted from different watermarked images.

	Baboon	Boat	Lena	Girlface	Crowd	Zelda
PSNR	74.952	75.114	75.030	73.412	75.061	72.258
NC	1	1	1	1	1	1
BCR	100	100	100	100	100	100
BER	0	0	0	0	0	0
SIM	1	1	1	1	1	1
Extracted Watermark						

Table 5.11: *PSNR (dB*) between host and watermarked image, *NC, BCR (in %), BER (in %)* and *SIM* between 56×56 original and extracted watermark, and watermark extracted from different watermarked images.

	Baboon	Boat	Lena	Girlface	Crowd	Zelda
PSNR	70.385	70.290	70.340	68.619	70.309	67.713
NC	1	1	1	1	1	1
BCR	100	100	100	100	100	100
BER	0	0	0	0	0	0
SIM	1	1	1	1	1	1
Extracted Watermark						

Table 5.12: *PSNR* (*dB*) between host and watermarked image, *NC, BCR (in %), BER (in %)* and *SIM* between 64×64 original and extracted watermark, and watermark extracted from different watermarked images.

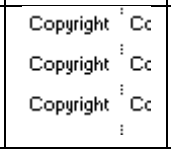
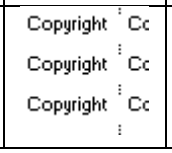
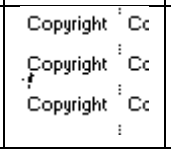
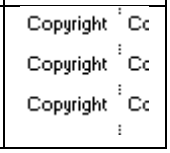
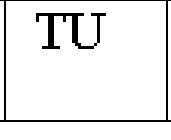
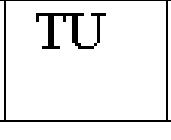
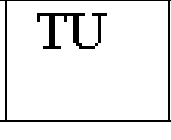
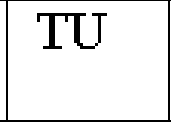
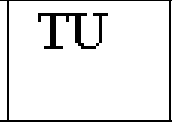
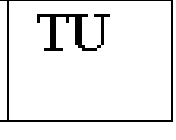
	Baboon	Boat	Lena	Girlface	Crowd	Zelda
PSNR	69.175	69.154	69.219	67.460	69.122	66.504
NC	1	1	1	1	1	1
BCR	100	100	100	100	100	100
BER	0	0	0	0	0	0
SIM	1	1	1	1	1	1
Extracted Watermark						

Table 5.13: *PSNR* (*dB*) between host and watermarked image, *NC, BCR (in %), BER (in %)* and *SIM* between original and extracted logo watermark, and watermark extracted from different watermarked images.

	Baboon	Boat	Lena	Girlface	Crowd	Zelda
PSNR	74.496	74.205	74.448	72.737	74.415	71.712
NC	1	1	1	1	1	1
BCR	100	100	100	100	100	100
BER	0	0	0	0	0	0
SIM	1	1	1	1	1	1
Extracted Watermark						

From table 5.10 to 5.13 shows that the *NC* and *BCR* are having values 1 and 100 respectively and the *PSNR* having value about 75 *dB*. After analyzing the result values we can observe that applying *DCT* on 4×4 block before *SVD*, gives better *PSNR* and other parameters.

To show the fragility of the watermarking algorithm, different attacks on the watermarked image have been applied. After applying these attacks the values of *NC, BCR* and *BER* between original and extracted watermark are tabulated in Table 5.14

Table 5.14: *NC, BCR* and *BER* between original and extracted watermark after attack on watermarked image.

Image	Attacks	NC	BCR	BER
Baboon	Average Filtering	-0.034	49.902	50.097
	JPEG Compression	-0.017	86.718	13.281
	Salt & Pepper	0.003	86.914	13.085
Boat	Average Filtering	0.003	48.828	51.171
	JPEG Compression	-0.018	86.914	13.085
	Salt & Pepper	0.005	86.914	13.085
Lena	Averaging Filtering	-0.011	47.363	52.636
	JPEG Compression	-0.021	86.914	13.085
	Salt & Pepper	0.004	86.914	13.085
Girlface	Averaging Filtering	0.017	50.585	49.414
	JPEG Compression	0.026	82.519	17.480
	Salt & Pepper	0.005	84.960	15.039
Crowd	Averaging Filtering	-0.007	49.609	50.390
	JPEG Compression	0.01	86.914	13.085
	Salt & Pepper	0.002	86.914	13.085
Zelda	Averaging Filtering	-0.067	47.363	52.636
	JPEG Compression	-0.017	86.914	13.085
	Salt & Pepper	0.002	86.914	13.085

From Table 5.14, we can conclude that after attacking the watermarked image by average filtering and salt n pepper noise the *NC* values are very less, which shows the watermarking scheme can be used for fragile watermarking.

In Table 5.15 the *PSNR* between host and watermarked image after embedding copyright watermark of different sizes are tabulated.

Table 5.15: *PSNR* (in *dB*) for *32×32, 56×56 64×64* copyright watermarks.

Size of watermark Image	**32×32**	**56×56**	**64×64**
Baboon	74.952	70.385	69.175
Boat	75.114	70.290	69.154
Lena	75.030	70.340	69.219
Girlface	73.412	68.619	67.460
Crowd	75.061	70.309	69.122
Zelda	72.258	67.713	66.504

From table 5.15 we conclude that after embedding large size of watermark, it maintains the imperceptibility.

The comparison of proposed algorithms with existing techniques with respect to *PSNR*, blindness and false positive are shown in tables 5.16 and 5.17.

Table 5.16: Comparison of the *PSNR* (in *dB*) between existing techniques with proposed algorithms

	Jose *et al.*(2012)	Sangeetha *et al.*(2018)	Mishra *et al*. (2014)	Proposed Entropy based algorithm	Proposed *DCT* based algorithm
Airplane	-	28.66762	-	-	-
Baboon	-	28.58936	53.0487	75.147	74.952
Boat	-	28.65913	54.0508	75.189	75.114
Barbara	51.7341	28.61679	-	-	-
Crowd	-	-	-	74.893	75.061
Cameraman	-	-	53.5651	-	-
Girlface	-	-	-	73.386	73.412
Goldhill	-	28.66259	-	-	-
Lena	51.5564	-	53.3062	75.156	75.030
Pepper	51.7925	-	52.09	-	-
Zelda	-	28.66974	-	72.462	72.258

Table 5.17: Comparison of the False-Positive and Blindness with existing techniques.

	Watermark Type	Type of Transform	Embedding Sub Band	Encryption	False-Positive Problem	Blindness
Mishra *et al.* 2014	Binary	DWT+SVD	LL3	No	Yes	No
Rastegar *et al.* 2011	Binary	FRAT+SVD +DWT	LL3, LH3	No	Yes	No
Proposed Entropy based Algorithm	Binary	DWT+SVD	Based on Entropy	Yes	No	Yes
Proposed *DCT* based Algorithm	Binary	DWT+DCT+ SVD	LL	Yes	No	Yes

From Tables 5.16 and 5.17 we concluded that the values of the *PSNR* between the host images and watermarked images, are higher in both of the proposed algorithms which are about 74 *dB i.e* they maintained the imperceptibility, and the proposed algorithms are blind and also free from False-Positive Problem.

Chapter 6

Conclusion and Future Scope

6.1. Conclusion

In this work, transform based blind watermarking algorithms for digital images have been proposed. Grayscale images have been considered for the experimental results. In first algorithm, after its implementation the average *PSNR* was up to 74.372 *dB* with *NC* and *BCR* with values 1 and 100 % respectively. Watermarks of sizes 32×32, 56×56 and 64×64 are considered. In the second proposed algorithm, image quality metrics evaluated were showing the average *PSNR* up to 74.827*dB* with *NC* and *BCR* with values 1 and 100 % respectively.

After analyzing the all image quality metrics we have concluded the both our proposed algorithms are providing the better imperceptibility and are also free from false-positive problem. Further, both of our algorithms also include blindness feature as the host image is not required.

6.2 Future Scope

The proposed algorithms are very much fragile but are not able to provide the robustness where the user may need this feature. So the work on the robustness of the techniques can be done in the near future.

References

AL-Nabhani Y., **Jalab H. A.**, **Wahid A., Noor R. M.**, "Robust watermarking algorithm for digital images using discrete wavelet and probabilistic neural network", Journal of King Saud University – Computer and Information Sciences, pp. 393-401, September 2015.

Aslantas V., "A singular-value decomposition-based image watermarking using genetic algorithm", Int. J. Electron. Commun. (AEÜ) 62, pp. 386 – 394, 2008.

Caragata D., Assad S. E., Luduena M., "An improved fragile watermarking algorithm for JPEG images", International Journal of Electronics and Communications (AEÜ), pp. 1783-1794, December 2015.

Dabas N., Singh R. P., Kher G., Chaudhary V., "A Novel SVD and Online Sequential Extreme Learning Machine Based Watermark Method for Copyright Protection", 8th International Conference on Computing Communication and Networking Technologies, , IIT Delhi, Delhi, India, pp. 1-5, July 2017.

Dogan S., Tuncer T., Avci E., Gulten A., "A robust color image watermarking with Singular Value Decomposition method", Advances in Engineering Software, Advances in Engineering Software 42, pp. 336–346, April 2011.

Durgesh Singh, S. K. Singh, "DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection" Multimed Tools Appl, Springer Science+Business Media New York 2016, Issue 76, pp. 13001-13024, July 2016.

Ganic E., **Eskicioglu A. M.**, "Robust Embedding of visual Watermarks using DWT-SVD", Department of Computer and Information Science, CUNY Brooklyn College, pp. 1-13, 2004.

Ghazy R. A., Amoon M., Abdallahd H. A., El-Fishawyb N. A., Hadhoude M. M., Dessoukya M. I., Alshebeilif S.A., El-Samie F. E. A., "Block based embedding of encrypted watermarks using singular value decomposition" , Optik 125, pp. 6299-6304, 2014.

Haddada L.R., Dorizzic B., Amara N. E. B., "A combined watermarking approach for securing biometric data", Signal Processing: Image Communication, Issue 55, pp. 23-31, March 2017.

Huang, J., C. Yang, ″Image Digital Watermarking Algorithm using Multiresolution Wavelet Transform″, In Proc. of IEEE Systems, Man and Cybernetics Conference, pp. 2977- 2982, 2004.

Jose S., Roy R. C., Shashidharan S., "Robust Image Watermarking based on DCT-DWT-SVD Method" , International Journal of Computer Applications, Volume 58, Issue 21, pp. 12-16, November 2012.

Keshavarziana R., Aghagolzadeh A., "ROI based robust and secure image watermarking using DWT and Arnold map", International Journal of Electronics and Communications (AEÜ), pp. 278-288, 2016.

Kumar G. D., Teja D. P., Reddy S. S., Sasikaladevi N., "An Efficient Watermarking Technique for Biometric Images", 7th International Conference On Advances In Computing & Communications, ICACC 2017, August 22-24, 2017, Cochin, India. Procedia Computer Science 115, pp. 423–430, 2017.

Lai C. C., "A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm", Digital Signal Processing 21, pp. 522–527, January 2011.

Loukhaoukha K., Refaey A., Zebbiche K., "Ambiguity attacks on robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition", Journal of Electrical Systems and Information Technology 4 (2017), pp. 359–368, January 2017.

Ma J., Ma Y., Li C., "Infrared and visible image fusion methods and applications: A survey", Information Fusion 45, pp. 153–178, February 2018.

Maehara T., Murota K., "Linear Algebra and its Applications", Linear Algebra and its Applications 435, pp. 106-116, February 2011.

Makbol N. M., Khoo B. E., Rassem T.H., "Block-based discrete wavelet transform singular value decomposition image watermarking scheme using human visual system characteristics" , IET Image Processing, Volume 10, Issue 1, pp. 34–52, July 2015.

Mishra A., Agarwal C., Sharma A., Bedi P., "Optimized gray-scale image watermarking using DWT–SVD and Firefly Algorithm" Expert Systems with Applications, Issue 41, pp. 7858–7867, June 2014.

Panda J., Nair A.S., Uppal A., Agrawal B., "Genetic Algorithm based optimized Color Image watermarking technique using SVD and DWT", 7th International Advance Computing Conference, Institute of Electrical and Electronics Engineers, pp. 579-583, 2017.

Peng Y., Niu X., Fu L., Yin Z., "Image authentication scheme based on reversible fragile watermarking with two images" , Journal of Information Security and Applications, Issue 40, pp. 236-246, May 2018.

Qi X, Xin X., "A singular-value-based semi-fragile watermarking scheme for image content authentication with tamper localization" , Journal of Visual Communication and Image Representation, Issue 30, pp. 312-327, May 2015.

Ramamurthy N., Varadarajan S., "Robust Digital Image Watermarking Scheme with Neural Network and Fuzzy Logic Network" International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 9, pp. 555-562, September 2012.

Rastegar S., Namazi F, Yaghmaie K, Aliabadian A., "Hybrid watermarking algorithm based on singular value decomposition and radon transform". AEU-International Journal on Electronics Communication, Volume 7, Issue 65, pp. 658–663, 2011.

Saha S., Bhattacharyya D., Bandyopadhyay S.K., "Security on Fragile and Semi-fragile Watermarks Authentication", International Journal of Computer Applications, Volume 3, Issue 4, pp. 23-27, June 2010.

Sai N. S. T., Patil R., Sangle S., Nemade B., "Truncated DCT and Decomposed DWT SVD features for Image Retrieval", 7th International Conference on Communication, Computing and Virtualization 2016. Procedia Computer Science 79, pp. 570-588, 2016.

Saikrishna N., Resmipriya M. G., "An Invisible Logo Watermarking using Arnold Transform", 6th International Conference On Advances In Computing & Communications, ICACC 2016, 6-8 September 2016, Cochin, India. pp. 808-815, 2016.

Solorio S. Y., Calderon F., Lic C.T., Nandi A. K., "Fast fragile watermark embedding and iterative mechanism with high self-restoration performance" Digital Signal Processing, Issue 73, pp. 83-92, 2018.

Sangeetha N., Anita X., "Entropy based texture watermarking using discrete wavelet transform" , Optik, Issue 160, pp. 380-388, Jan 2018.

Shieh J.M., Lou D.C., Chang M.C., "A semi-blind digital watermarking scheme based on singular value decomposition", Computer Standards & Interfaces 28, pp. 428– 440, April 2005.

Sharma S., Singh A. K., Kumar P., "Digital Image Watermarking using Machine Learning Techniques: A Technical Review", Advances in Engineering and Technology, pp. 83-87, 2016.

Su Q., Niu Y., Zou H., Liu X., "A blind dual color images watermarking based on singular value decomposition", Applied Mathematics and Computation 219, pp. 8455–8466, 2013.

Su Q., Niu Y., Zhao Y., Pang S., Liu X., "A dual color images watermarking scheme based on the optimized compensation of singular value decomposition", International Journal of Electronics and Communications (AEÜ) 67, pp. 652– 664, 2013.