TRIBHUVAN UNIVERSITY

INSTITUTE OF ENGINEERING

PULCHOWK CAMPUS

THESIS NO.: 070/MSCS/661

Robust Digital Image Watermarking using Symmetric and Asymmetric Cryptography

By

Pramina Shrestha

A THESIS SUBMITTED TO THE DEPARTMENT OF COMPUTER AND ELECTRONICS ENGINEERING IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE IN COMPUTER SYSTEM AND KNOWLEDGE ENGINEERING

DEPARTMENT OF COMPUTER AND ELECTRONICS ENGINEERING

LALITPUR, NEPAL

February, 2017

Robust Digital Image Watermarking using Symmetric and Asymmetric Cryptography

By
Pramina Shrestha
(070/MSCS/661)

Thesis Supervisor:
Dr. Shashidhar Ram Joshi
Professor

A thesis submitted in partial fulfillment of the requirement for
the degree of Master of Science in Computer System and Knowledge Engineering.

Department of Electronics and Computer Engineering
Institute of Engineering, Central Campus, Pulchowk
Tribhuvan University
Lalitpur, Nepal

February, 2017

COPYRIGHT ©

TRIBHUVAN UNIVERSITY
INSTITUTE OF ENGINEERING
PULCHOWK CAMPUS
DEPARTMENT OF ELECTRONICS AND COMPUTER ENGINEERING

Ananda Niketan, Pulchowk, Lalitpur, P.O. Box 1175, Kathmandu, Nepal.
Tel : 5534070, 5521260 extn. 315, Fax : 977-1-5553946, E-mail : doece@ioe.edu.np

Our Ref :

DEPARTMENTAL ACCEPTANCE

The thesis entitled "Robust Digital Image Watermarking using Symmetric and Asymmetric Cryptography", submitted by Pramina Shrestha in partial fulfillment of the requirement for the award of the degree of "Master of Science in Computer System and Knowledge Engineering" has been accepted as a bona fide record of work independently carried out by her in the department.

Dr. Dibakar Raj Pant

Head of the Department

Department of Electronics and Computer Engineering

Pulchowk Campus

Institute of Engineering

Tribhuvan University

Nepal.

TRIBHUVAN UNIVERSITY
INSTITUTE OF ENGINEERING
PULCHOWK CAMPUS
DEPARTMENT OF ELECTRONICS AND COMPUTER ENGINEERING

Ananda Niketan, Pulchowk, Lalitpur, P.O. Box 1175, Kathmandu, Nepal.
Tel : 5534070, 5521260 extn. 315, Fax : 977-1-5553946, E-mail : doece@ioe.edu.np

Our Ref :

CERTIFICATE OF APPROVAL

The undersigned certify that they have read and recommend to the Department of Electronics and Computer Engineering for acceptance, a thesis entitled "Robust Digital Image Watermarking using Symmetric and Asymmetric Cryptography", submitted by Pramina Shrestha in partial fulfillment of the requirement for the award of the degree of "Master of Science in Computer System and Knowledge Engineering".

Supervisor: Dr. Shashidhar Ram Joshi
Professor
Department of Electronics and Computer Engineering

External Examiner: Mr. Subhash Dhakal
Department of IT, Ministry of Science and Technology

Committee Chairperson: Dr. Subarna Shakya
Professor
Department of Electronics and Computer Engineering

DATE OF APPROVAL: February, 2017

ACKNOWLEDGEMENT

First of all, I would like to express my deep gratitude to Department of Electronics and Computer Engineering for providing the opportunity to carry out thesis work as a partial fulfillment of Master of Science in Computer Systems and Knowledge Engineering.

I would like to express my sincere gratitude to the contribution of my thesis Supervisor **Prof. Dr. Shashidhar Ram Joshi**. I am indebted to him for providing encouragement, outstanding supervision, expert guidance and consistent support throughout the thesis period.

I am also grateful to our head of department **Dr. Dibakar Raj Panta,** MSCSKE Coordinator **Dr. Aman Shakya, Dr. Sanjeeb Prasad Panday, Prof. Dr. Subarna Shakya and Dr. Basanta Joshi** for their encouragement and valuable guidance.

I would like to extend my appreciation to all of my friends for their advice and encouragement during my thesis work.

Finally, I would like to express my heartfelt gratitude to my family for their encouragement and belief in me.

Pramina Shrestha

(070/MSCS/661)

ABSTRACT

As the popularity of digital media is growing, and world is becoming smaller, due to internet and easy access of information, the copyright protection of intellectual properties have become a necessity for prevention of illegal copying and content integrity verification. So, to achieve these requirements, digital watermarking methods have been studied and implemented. Text, images, audios, videos etc. can be used as digital watermarks. Here, in this study, images have been taken as watermark. The different models of watermarking used are related with embedding and extracting image watermark from cover images in transform domain. For this, a varying technique of discrete wavelet transform (DWT) and combination of DWT with advanced encryption standard (AES), asymmetric key algorithm (RSA) and singular value decomposition (SVD) have been implemented for the security and robustness of the embedded watermark. The encrypted watermarked image has gone through many attacks, namely, noise attacks, rotation, crop, mean and median attack. Then the robustness of the extracted watermark has been evaluated by means of image quality criteria MSE, PSNR and NCC. In this thesis work, evaluation of different watermarking methods in transform domain has been carried out.

Keywords:

Digital Watermarking, Transform Domain, Watermark Embedding, Watermark Extraction, Discrete Wavelet Transform, Advanced Encryption Standard, RSA algorithm, Singular Value Decomposition

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

AES	Advanced Encryption Standard
DWT	Discrete Wavelet Transform
HH	Sub band of DWT containing diagonal components
HL	Sub band of DWT containing horizontal components
IDWT	Inverse Discrete Wavelet Transform
LH	Sub band of DWT containing vertical components
LL	Sub band of DWT containing low frequency components
MSE	Mean Square Error
NCC	Normalized Cross Correlation
PSNR	Peak Signal to Noise Ratio
RSA	Rivest, Shamir and Adler Algorithm
SVD	Singular Value Decomposition

CHAPTER 1

INTRODUCTION

1. INTRODUCTION

1.1 BACKGROUND

Digital image processing is an area where many developments have been done and many are ongoing in the field of computer science and engineering. It is important mainly because its methods are used in various fields like for image enhancement, law enforcement, artistic effects, image restoration, medical field, digital watermarking etc.

In this day and age, where normally communication is done through the web, there comes the issue of privacy and security of data. There comes the issue of security because there may be illegal access to the data which we put on the web. To protect the data and provide security there are many different techniques like cryptography, steganography and digital watermarking. Here, we discuss about digital watermarking and cryptography.

A digital watermarking is a kind of marker embedded covertly in a noise-tolerant signal such as audio, video or image data. It is typically used to identify ownership of the copyright of such signal. Watermarking is the process of hiding digital information in a carrier signal. The hidden information can but does not need to contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or for owner identification, content protection, copyright protection etc. It is usually used for tracing copyright infringements and for banknote authentication.

The main difference between watermark and digital watermark is that the digital watermarks are supposed to be invisible or at least does not change the perception of original file whereas watermarks are supposed to be somewhat visible. A signal may carry several different watermarks at the same time. If the signal is copied, then the information is also carried in the copy.

Ideal properties of a digital watermark:

1. A digital watermark should be imperceptible, meaning that it should be perceptually invisible to prevent obstruction of the original image.

2. Watermarks should be robust to filtering, additive noise, compression, cropping and other forms of image manipulations.[3]

The Digital Watermarking methods are as shown below:

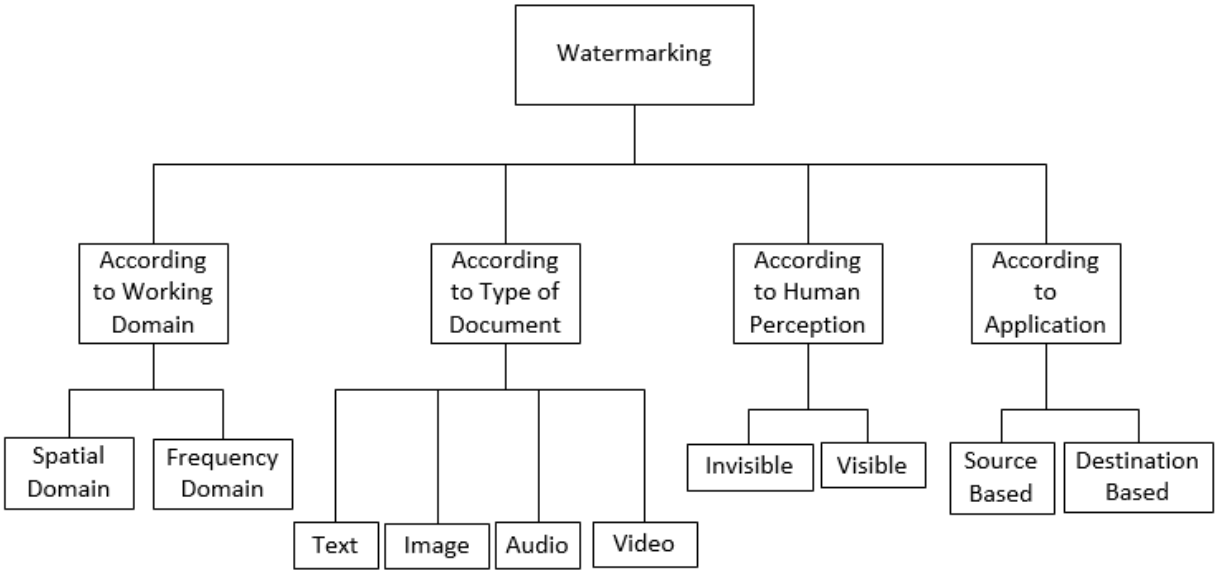


Figure 1.1 : Digital Watermarking methods

As seen from the figure above, Image watermarking can be classified as visible or invisible. A visible watermarking typically contains a visual message or a company logo indicating the ownership of the image. The invisible watermarked image is visually very similar but not necessarily identical to the original unmarked image. There are three categories according to the robustness of watermarking to attacks.

a. Robust Watermarking: The embedded watermark should be resistant to any processing and/or attack that does not seriously affect the quality and value of the host image. It's used for copyright protection and access control.

b. Fragile Watermarking: The watermark should not tolerate any tampering that modifies the complete integrity of the image. It's used for strict image authentication and integrity verification.

c. Semi-fragile Watermarking: The watermark should tolerate occasional noise and common image processing such as lossy compression, but be fragile to any malicious tampering that modifies image content. It's used for soft image authentication and integrity verification.

According to working domain Image watermarking can be classified as:

a. Spatial Domain Watermarking

   In this technique, watermark is embedded by directly amending the pixel values of the host image/video. The pixel based methods are conceptually simple and have low computational intricacies.

b. Transform Domain Watermarking

   In this technique, embedding of watermark is done by altering the transform coefficients of the image. The frequency domain technique first transforms an image into a set of frequency domain coefficients. The watermark is then embedded in the transformed coefficients of the image such that the watermark is invisible and more robust for some image processing operations. Finally, the coefficients are inverse transformed to obtain the watermarked image. Discrete Cosine Transformation (DCT), Discrete Fourier Transformation (DFT) and Discrete Wavelet Transformation (DWT) are the three main methods of data transformation. This technique is complex and watermark cannot be easily recovered at the receiver end as compared to spatial domain technique.

Every digital watermarking technique includes two algorithms – embedding algorithm and detecting algorithm. These two processes are same for all the types of watermarking techniques. Figure below shows the watermark embedding process in which the watermark is embedded in the cover image by using the embedding algorithm. Another figure shows the watermark detection process in which the embedded watermark is recovered by using the detection algorithm.

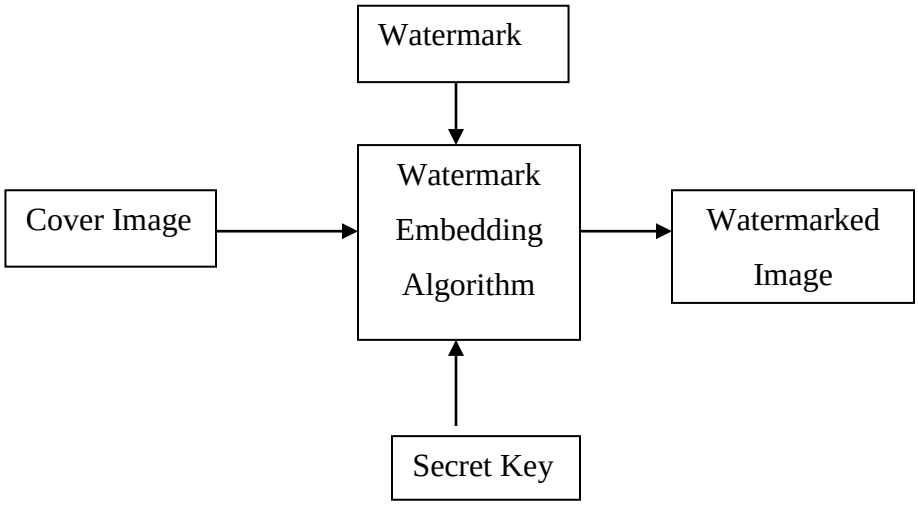


Figure 1.2: Watermark Embedding Process

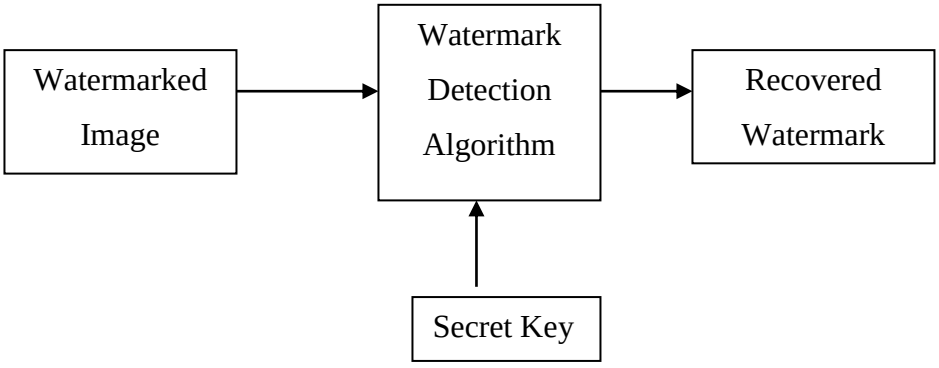


Figure 1.3: Watermark Detection Process

Classification of Attacks:

a. Removal Attacks:

Removal attacks aim at the complete removal of the watermark information from the watermarked data without cracking the security of the watermarking algorithm (e.g., without the key used for watermark embedding). That is, no processing, even prohibitively complex, can recover the watermark information from the attacked data. This category includes denoising, quantization , remodulation, and collusion attacks. Not all of these methods always come close to their goal of complete watermark removal, but they may nevertheless damage the watermark information significantly.

b. Geometric Attacks:

   Geometric attacks do not actually remove the embedded watermark itself, but intend to distort the watermark detector synchronization with the embedded information. The detector could recover the embedded watermark information when perfect synchronization is regained.

c. Cryptographic Attacks:

   Cryptographic attacks aim at cracking the security methods in watermarking schemes and thus finding a way to remove the embedded watermark information or to embed misleading watermarks.

d. Protocol Attacks:

   Protocol attack aims at attacking the entire concept of the watermarking application. One type of protocol attack is based on the concept of invertible watermarks. The idea behind inversion is that the attacker subtracts his own watermark from the watermarked data and claims to be the owner of the watermarked data. This can create ambiguity with respect to the true ownership of the data. Another is copy attack.

Applications of Watermarking:

a. Ownership Assertion

b. Fingerprinting

c. Fraud and Tamper detection etc.

Cryptography:

Cryptography is the study of information hiding and retrieval. It is the art of protecting the information by transforming it into unintelligible format in which a message can be hidden from reader and only the intended recipient will be able to convert it into original message. Its main goal is to keep the data safe from unauthorized access. It is used in various aspects in information security such as data confidentiality, data integrity, authentication and non-repudiation.

a. Symmetric Key Algorithm:

Symmetric encryption transforms plaintext into cipher-text using a secret key and an encryption algorithm. Using the same key and a decryption algorithm, the plaintext is recovered from the cipher-text. A symmetric encryption scheme has five components: plaintext, encryption, algorithm, secret key, cipher-text and decryption algorithm. The secret key is shared by both the sender and the receiver and the key must be kept hidden, since if anyone finds the key they would be able to extract the hidden message.

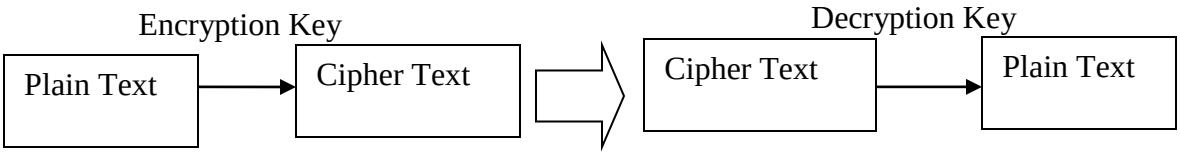


Figure 1.4: Symmetric Encryption

b. Asymmetric Key Algorithm:

Asymmetric cryptography uses public key and private key. Public key is used for encryption and private key is used for decryption of the encrypted data.

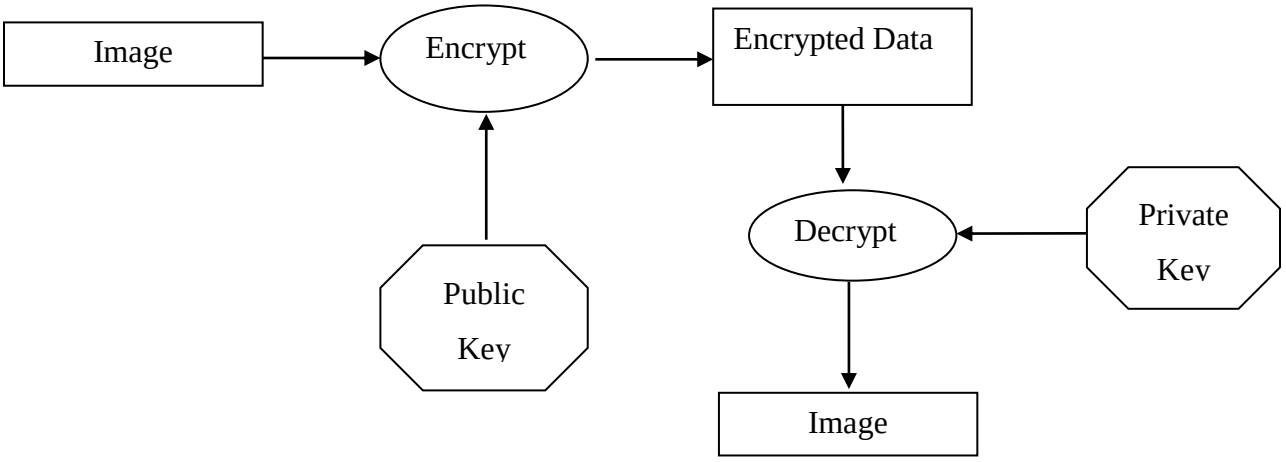


Figure 1.5: Asymmetric Key Encryption and Decryption Process

1.2 PROBLEM DEFINITION

Many images and information can be found in the web these days. To ensure their privacy and to claim copyright of images we can watermark the images. Encryption of the watermarked image can be done to protect it from unauthorized changes and thus help in claiming the authority of the original image which has been watermarked.

1.3 OBJECTIVE

The objectives of this thesis are:

i. To evaluate the existing Transform Domain algorithms for watermarking images and use symmetric and asymmetric algorithms for securing the watermarked image.

ii. To confirm the robustness of the decrypted watermark after different attacks are done on the encrypted watermarked image.

1.4 SCOPE OF THE WORK

The scope of the thesis is on the implementation and comparison of different watermarking techniques. This study examines the watermarking process as the combination of two steps watermark embedding and watermark extraction. The two steps will be covered in detail. The main objective is to understand the different algorithms and approaches that can be used to embed and extract the watermark from the watermarked image in order to ensure its authenticity.

A MATLAB GUI has been implemented to test the watermarking techniques. With the help of the implementation, different methods have been implemented and examined to find the resulting watermark at different conditions of the watermarked image as well as robustness of the extracted watermark has also been checked.

1.5 ORGANIZATION OF REPORT

The report is divided into five chapters. A brief description of each chapter is presented below.

- Chapter 1: This chapter has described a brief introduction to digital watermarking, cryptography and the objectives. The definition of the problem has been included in this chapter.
- Chapter 2: The relevant literature studied and referred in the course of this research work has been included in this chapter.
- Chapter 3: This chapter includes the methodology used in thesis work. It explains how the images are watermarked and how they are extracted.

- Chapter 4: This chapter includes the discussion of the different algorithms used for digital watermarking and their analysis and comparison are given.
- Chapter 5: This chapter gives the conclusion, limitations and recommendations.

CHAPTER 2

LITERATURE REVIEW

2. LITERATURE REVIEW

2.1 RELATED WORK

The field of digital image watermarking and cryptography is a field where many research have already been done and many research are still ongoing. Among the different algorithms developed and implemented some are as follows:

N. Kashyap et.al. have implemented 2 and 3-level discrete wavelet transform and have used the concept of alpha-blending to embed the watermark. Here, multi-bit watermark has been embedded in lower frequency bands and the experimental results demonstrate that the watermarks generated with the proposed algorithm are invisible and the quality of watermarked image and the recovered image are improved.[1],[2] Satendra et.al. have implemented a hybrid digital image watermarking scheme based on discrete wavelet transform and singular value decomposition. To increase and control the strength of the watermark, a scale factor value is used. In this approach, the watermark is not embedded directly on the wavelet coefficients but rather than on the elements of singular values of the cover image with modifying three level Discrete wavelet transform (DWT) HL and LH sub bands. Experimental results are provided in terms of Peak signal to noise ratio (PSNR) and Normalized cross correlation (NCC) to demonstrate the effectiveness of the proposed algorithm against various attacks.[3] A. Joseph et.al. have implemented a robust digital watermarking using discrete wavelet transform and singular value decomposition where the watermarks have been embedded in the HL and LH sub-bands of the host image. This approach withstands many attacks.[4] P. Parashar et.al. did a survey of digital watermarking techniques and have provided the important methods of spatial domain and transform domain.[5] R.V. Ravi et.al. and S. Kumar et. al. have used the concept of discrete wavelet transform and advanced encryption standard for secure image encoding.[6] Joshy et. Al. proposed a multimedia authentication and tamper detection scheme with the security of AES ciphered watermarking and hash function. Two watermarks are embedded in the host image for authentication and tamper detection. One watermark was unique identification code and other hash code of host image which was embedded using two-level discrete wavelet transform. The method was evaluated for robustness under different attack conditions.[7]

K. Singh and S. Dwivedi proposed a concept of digital watermarking using asymmetric key cryptography and spatial domain technique. In order to achieve higher secrecy and efficiency, this combined approach was used. They implemented RSA and spatial domain technique to embed the watermark.[9] Yuva Kumar et. al. have used a technique for secured image steganography using DWT approach. Here, text is encrypted and then embedded in the image using double stegging in DWT domain. [10] Varghese et. al., have implemented a framework of combined enhanced RSA algorithm with watermarking techniques for hiding secret information in digital images. Enhanced RSA cryptosystem used in this paper reduces exponentiation calculation substantially. Enhanced RSA encrypted data and watermark is embedded inside an hue saturation value color image using discrete wavelet transform algorithm.[11]

Dhankar. M. et. al., have done robustness analysis DWT-SVD with AES encryption based image data hiding system for various attacks, a technique for highly secure image data transmission.DWT and SVD based image data embedding over cover image was proposed to achieve higher robustness against various attacks while AES ensures higher efficiency of transmission security.[12] Ajili. S. et. al., presents a watermarking method based on DDWT and SVD with AES algorithm applied on medical image.SVD is applied to higher band of DWT decomposed original image and binary watermark is embedded by using the singular values. AES algorithm is used for enhanced robustness. Serial turbo code was used to control identification and correct the watermark if possible. These have been done on MRI medical images.[13] Lakrissi et. al proposed a method which is based on the combination of encryption algorithms, public-private keys and secret keys and watermarking using AES, RSA and DWT. [15]

CHAPTER 3

METHODOLOGY

3. METHODOLOGY

3.1 WORKING PRINCIPLE

This thesis is focused on the embedding and extraction technique of watermark image on any cover image. The image chosen for watermarking can be a logo or any other image which helps in authenticating the cover image. To ensure the robustness of the watermarked image, transform domain algorithm has been used. And to ensure the security of the watermark or secret image, the watermark image has been encrypted using symmetric algorithm and asymmetric algorithm respectively. This thesis mainly focuses on ensuring the security of the watermark image and making it robust using combination of transform domain technique and encryption algorithms.

3.2 IMPLEMENTED METHOD

3.2.1 Image Pre-Processing

The image input as cover and watermark image is converted to gray scale and then resized to dimension 64*64.

3.2.2 Transform Domain Technique

3.2.2.1 2-Level decomposition using Wavelet Transform

Image is represented as a two dimensional array of coefficients. In order to modify the coefficients of image to transform coefficients, there are different transform methods. Among the transform methods, the method used to decompose the image into lower and higher frequency coefficients is discrete wavelet transform.

Discrete Wavelet Transform (DWT):

Discrete wavelet transform is a multi resolution decomposition of a signal. It hierarchically decomposes an image and maps an image into a set of coefficients. Here, decoding is done in low resolution to high resolution. DWT splits the signal into high and low frequency parts. The high frequency part contains information about the edge components, while the low frequency part is split again into high and low frequency parts. The high frequency components are usually used for watermarking since human eye is less sensitive to changes in edges.

One-level Discrete wavelet transform decomposes an image into lower resolution approximation image(LL),as well as horizontal(HL), vertical(LH) and diagonal(HH) detail components. To compute second-level of DWT, the DWT algorithm is again applied on LL, which further divides the LL part into four sub-bands LL1,HL1,LH1,HH1. This decomposition is shown in the figure below:

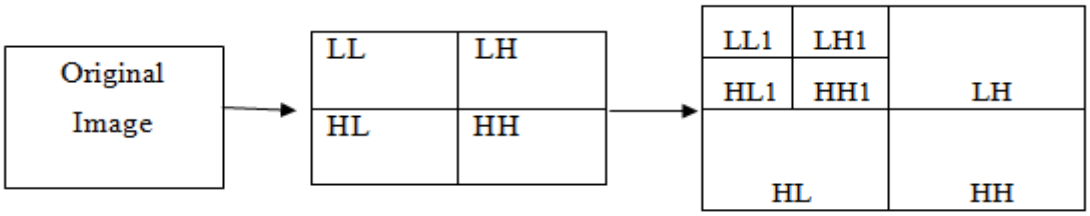


Figure 3.1: 2-level Discrete Wavelet Transform

Explanation:

The DWT of a signal x is calculated by passing it through a series of filters. First the samples are passed through a low pass filter with impulse response g resulting in a convolution of the two:

$$Y[n] = (x * g)[n] = \sum_{k=-\infty \text{ to } \infty} x[k]\, g[n-k] \qquad \textbf{Equation 3.1}$$

The signal is also decomposed simultaneously using a high pass filter h. The output giving the detail coefficients (from the high-pass filter) and approximation coefficients (from the low-pass). For this the filters should be related to each other.

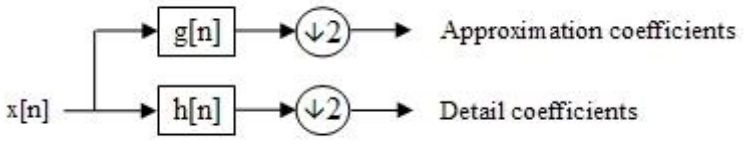


Figure 3.2: Block diagram of filter analysis

However, since half the frequencies of the signal have now been removed, half the samples can now be discarded according to Nyquist's rule. The filter output of the low-pass filter g in the diagram above is then sub-sampled by 2 and further processed by passing it through a new low-pass filter g and a high-pass filter h with half the cut-off frequency of the previous one, i.e.:

$$Y_{low}[n] = \sum_{k=-\infty \text{ to } \infty} x[k]\, g[2n-k] \qquad \text{Equation 3.2}$$

$$Y_{high}[n] = \sum_{k=-\infty \text{ to } \infty} x[k]\, h[2n-k] \qquad \text{Equation 3.3}$$

This decomposition is repeated to further increase the frequency resolution and the approximation coefficients decomposed with high and low pass filters and then down-sampled. This is shown in the figure below:

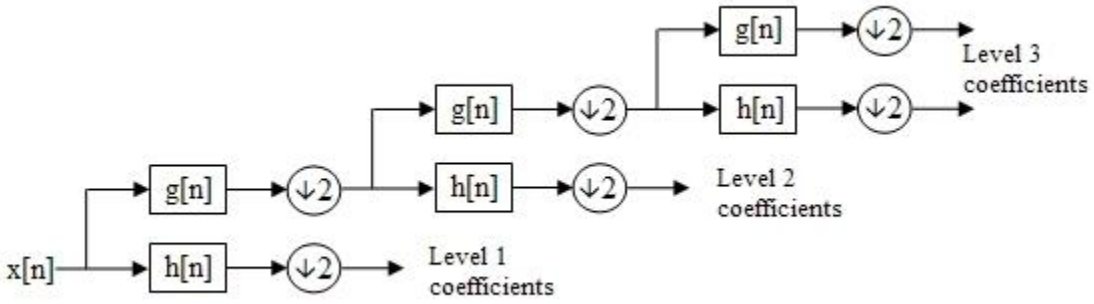


Figure 3.3: A 3-level filter bank

3.2.2.2 Singular Value Decomposition (SVD):

Another transform used is singular value decomposition, which is a linear algebra technique used to solve many mathematical problems. Any image can be considered as a square matrix without loss of generality. So, SVD can be applied to any kind of images.

SVD belongs to orthogonal transform which decomposes the given matrix into three matrices of same size. To decompose the matrix using SVD technique, the matrix need not be square. Let us denote the image as matrix A, then the SVD decomposition of matrix A is given by the equation

$$A = U * S * V^T \qquad \text{Equation 3.4}$$

Here, U and V are unitary matrices such that:

$$U * U^T = I \,,\; V * V^T = I \qquad \text{Equation 3.5}$$

Where, I is an identity matrix.

S is the diagonal matrix having its main diagonal elements all non- negative singular values of A. These positive singular values can be used to embed watermark. The order of singular matrix A is same as original matrix A.[3]

3.2.3 Image Encryption

For further security of the watermarked image, symmetric algorithm i.e., advanced encryption standard and asymmetric algorithm i.e. RSA algorithm have been used.

3.2.3.1 AES Algorithm

AES algorithm is a symmetric algorithm which uses the same key for encryption and decryption of data. It is flexible in supporting any combination of data and key size of 128,192 and 256 bits. However, AES only allows a 128 bit data length that can be divided into four basic operation blocks. These blocks operate on array of bytes and organized as a 4*4 matrix that is called the state. For full encryption, the data is passed through number of rounds Nr (Nr – 10, 12, 14). AES encryption and decryption are shown in the figure below.

These rounds are governed by the following transformations:

SubByte Transformation: A non-linear substitution step where each byte is replaced with another according to a lookup table.

Shiftrows Transformation: A transposition step where each row of the state is shifted cyclically a srtain number of steps.

MixColumns Transformation: It is equivalent to a matrix multiplication of columns of the states. Each column vector is multiplied by a fixed matrix.

Addroundkey Transformation: It is a simple XOR between the working state and the roundkey. Each roundkey consists of block size Nb words from the key schedule.

The cipher transformation is inverted and implemented in reverse order to produce a straightforward inverse cipher for AES algorithm. Invshiftrows, invsubbyte, invmixcolumn and addroundkey are the transformation performed in decryption.

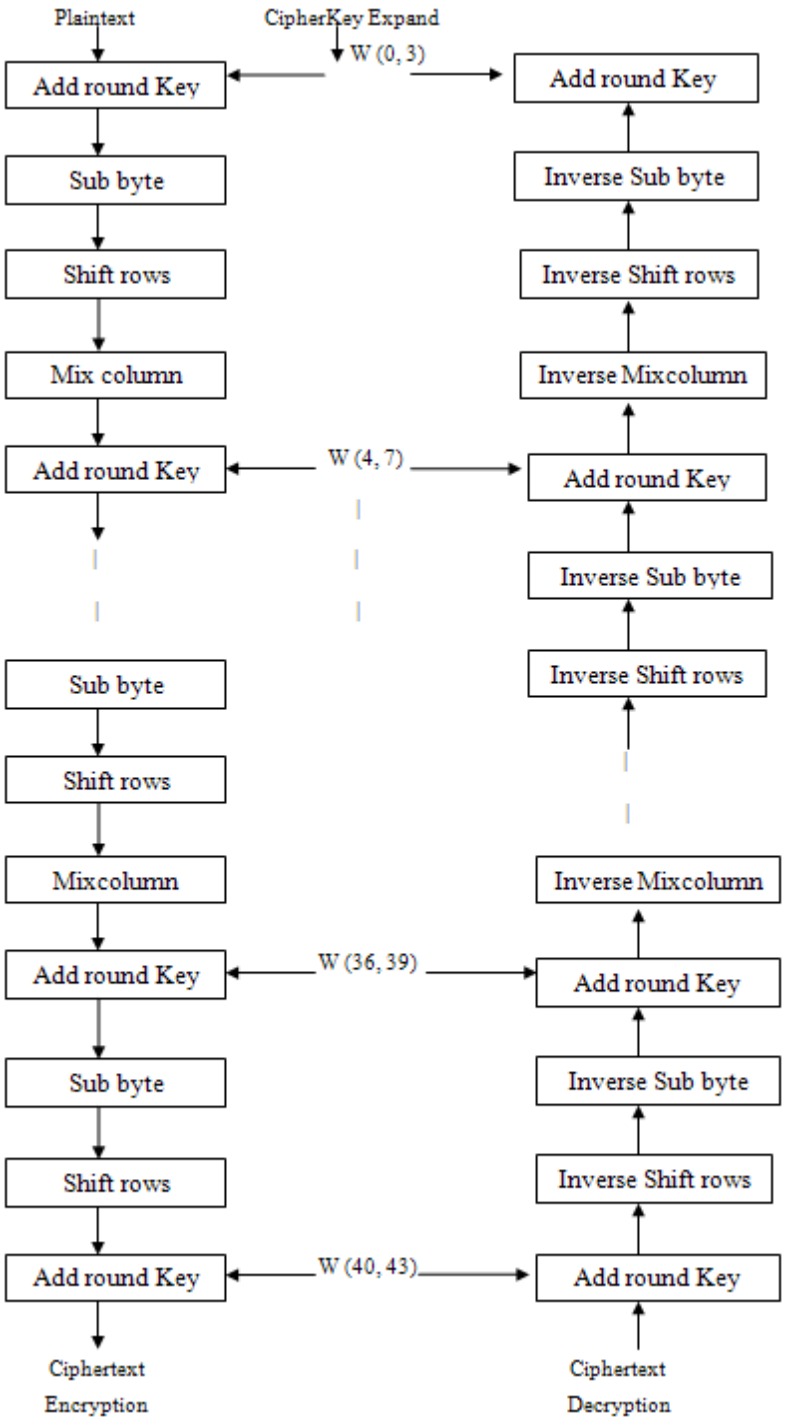


Figure 3.4: AES Encryption and Decryption [6]

3.2.3.2 RSA Algorithm

RSA is an algorithm for public-key cryptography that is based on the presumed difficulty of factoring large integers. The RSA algorithm consists of 3 steps: key generation, encryption and

decryption. A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. The prime factors must be kept secret.

RSA Steps:

1. Choose two distinct prime numbers p and q.
2. Compute n=p*q
3. Compute $\phi(n) = \phi(p)\ \phi(q) = (p-1)\ (q-1)$ where ϕ is euler's totient
4. Choose an integer e such that $1<e<\phi(n)$ and $\gcd(e, \phi(n))=1$ i.e., e and $\phi(n)$ are coprime.
5. Determine d as $d \equiv e-1 \pmod{\varphi(n)}$
6. Public key is (e,n) and Private key is (d,n)
7. Now, message, m is encrypted by the function: c=me mod n

   And encrypted message, c is decrypted by the function: m=cd mod n

3.2.4 Watermark Embedding and Extraction Technique

Alpha-Blending Technique:

The method used for embedding and extracting watermark is Alpha-Blending technique. The embedding process is given by the formula:

WMI=k*(HH1)+q*(WM1) **Equation 3.6**

Where,

HH1 = High frequency approximation of the original cover image

WM1= High frequency approximation of the watermark image

WMI = Watermarked image

k, q = scaling factors

The extraction process of the embedded watermark is given by the formula:

RW=WMI - k*(HH1) **Equation 3.7**

Where,

RW=High frequency approximation of Recovered watermark

LL1 = High frequency approximation of the original cover image

WMI = High frequency approximation of Watermarked image

k = scaling factor

3.2.5 Algorithms

3.2.5.1 DWT-AES

In the algorithms used in [1] LL sub-band has been used for watermark insertion using alpha-blending technique. In the algorithm used in [7], combination of DWT and AES has been used for image security. Combining these two algorithms, image watermarking is done by using alpha-blending technique and image is encrypted by using AES algorithm. In this process, HL band is used for watermark insertion since we are checking the robustness of the extracted watermark.

Watermark Insertion and Encryption:

a. The pre-processed cover and watermark image of size 64*64 is divided into sub-bands LL, HL, LH and HH.
b. LL sub-band is further divided into four sub-bands LL1, HL1, LH1 and HH1.
c. The watermark is then embedded into the HL1 sub-band using alpha-blending insertion technique as in equation 6.
d. Then inverse DWT is done to obtain watermarked image.
e. The watermarked image is then encrypted using AES algorithm to make it secure.

Decryption and Watermark Extraction:

a. The encrypted watermarked image is decrypted.
b. Then 2-level Haar wavelet is applied on the decrypted image to get the HL1 sub-band.
c. Using alpha-blending extraction technique in equation 7, the watermark is extracted.
d. Then inverse DWT is done to obtain watermark.
e. The watermark extracted from the watermarked image subjected to attacks is then checked for robustness in comparison with the original watermark image using similarity measures like MSE, PSNR and NCC.

3.2.5.2 DWT-RSA

In the algorithms used in [10], text has been used as watermark data. This watermark data is encrypted using RSA algorithm inserted using Haar wavelet in 2 dimensional discrete wavelet transform domain. In this process, HL band is used for watermark insertion and instead of encrypting the watermark image, the watermarked image has been encrypted for secure image transmission.

Watermark Insertion and Encryption:

a. The pre-processed cover and watermark image is divided into sub-bands LL, HL, LH and HH.
b. LL sub-band is further divided into four sub-bands LL1, HL1, LH1 and HH1.
c. The watermark is then embedded into the HL1 sub-band using alpha-blending insertion technique as in equation 6.
d. Then inverse DWT is done to obtain watermarked image.
e. Prime numbers p and q were taken as input for calculating the public and private key for RSA algorithm.
f. The watermarked image is then encrypted using public key to make it secure.

Decryption and Watermark Extraction:

a. The encrypted watermarked image is decrypted using private key of RSA algorithm..
b. Then 2-level Haar wavelet is applied on the decrypted image to get the HL1 sub-band.
c. Using alpha-blending extraction technique in equation 7, the watermark is extracted.
d. Then inverse DWT is done to obtain watermark.
e. The watermark extracted from the watermarked image subjected to attacks is then checked for robustness in comparison with the original watermark image using similarity measures like MSE, PSNR and NCC.

3.2.5.3 DWT-SVD-AES

In the algorithm used in [12], the watermark is inserted in DWT-SVD domain and the watermarked image is encrypted using AES algorithm to enhance its security. The algorithm has been implemented here.

Watermark Insertion and Encryption:

a. The pre-processed cover and watermark image is divided into sub-bands LL,HL,LH and HH.
b. Then 2-level DWT decomposition is done on LL image.
c. SVD is applied to HL1 sub-band of the cover and watermark image as:

$$A= U*S^{*}V^{T}$$

d. Singular value of watermark, Swm, is inserted into singular value of cover image, Simg using a scale factor alpha, α as:

$$Sw = Simg + \alpha *Swm$$

Where, α denotes the scale factor

e. Now modified image I of the modified higher frequency coefficient is obtained as:

$$I=U*Sw*VT$$

f. The watermarked image, Aw is then obtained by doing two-level inverse DWT.
g. The watermarked image is then encrypted using symmetric key of 128-bit as input to AES algorithm to make it secure.

Decryption and Watermark Extraction:

a. The encrypted watermarked image is decrypted using symmetric key of AES algorithm.
b. Then 2-level Haar wavelet is applied on the decrypted watermarked image to get the HL1 sub-band.
c. Use 2-level Haar DWT to decompose the watermark image and the original cover image into LL1, LH1, HL1 and HH1.
d. Apply SVD to HL1 band of the watermarked image, original cover image and original watermark image i.e.,

$$A_w=U_w*S_w*V_w^{T}$$

$$A_i= U_i*S_i*V_i^{T}$$

$$A_{wm}= U_{wm}*S_{wm}*V_{wm}^{T}$$

Where A_w denotes watermarked image, A_i denotes cover image and A_{wm} denotes original watermark image.

e. Singular value of the embedded watermark is obtained by:

$$S_{ewm}=(S_w - S_{i)} / \alpha$$

f. Then the DWT HL1 coefficient of the extracted watermark is obtained by:

$$A_{ewm}=U_{wm}*S_{ewm}*V_{wm}^{T}$$

g. Finally, inverse DWT is applied and the embedded watermark is extracted.

h. The watermark extracted from the watermarked image subjected to attacks is then checked for robustness in comparison with the original watermark image using similarity measures like MSE, PSNR and NCC.

3.2.5.4 DWT-SVD-RSA

In the algorithm used in [14], the watermark is inserted in DWT-SVD domain and the watermarked image is encrypted using RSA/AES algorithm to enhance its security. The algorithm has been implemented here.

Watermark Insertion and Encryption:

a. The pre-processed cover and watermark image is divided into sub-bands LL,HL,LH and HH.

b. Then 2-level DWT decomposition is done on LL image.

c. SVD is applied to HL1 sub-band of the cover and watermark image as:

$$A= U*S^{*}V^{T}$$

d. Singular value of watermark, S_{wm}, is inserted into singular value of cover image, S_{img} using a scale factor alpha, α as:

$$S_w = S_{img} + \alpha *S_{wm}$$

Where, α denotes the scale factor

e. Now modified image I of the modified higher frequency coefficient is obtained as:

$$I=U*S_w*V^{T}$$

f. The watermarked image, A_w is then obtained by doing two-level inverse DWT.

g. Prime numbers p and q were taken as input for calculating the public and private key for RSA algorithm.

h. The watermarked image is then encrypted using public key to make it secure.

Decryption and Watermark Extraction:

a. The encrypted watermarked image is decrypted using private key of RSA algorithm..
b. Then 2-level Haar wavelet is applied on the decrypted watermarked image to get the HL1 sub-band.
c. Use 2-level Haar DWT to decompose the watermark image and the original cover image into LL1, LH1, HL1 and HH1.
d. Apply SVD to HL1 band of the watermarked image, original cover image and original watermark image i.e.,

$$A_w = U_w * S_w * V_w^T$$

$$A_i = U_i * S_i * V_i^T$$

$$A_{wm} = U_{wm} * S_{wm} * V_{wm}^T$$

Where A_w denotes watermarked image, A_i denotes cover image and A_{wm} denotes original watermark image.

e. Singular value of the embedded watermark is obtained by:

$$S_{ewm} = (S_w - S_{i)} / \alpha$$

f. Then the DWT HL1 coefficient of the extracted watermark is obtained by:

$$A_{ewm} = U_{wm} * S_{ewm} * V_{wm}^T$$

g. Finally, inverse DWT is applied and the embedded watermark is extracted.
h. The watermark extracted from the watermarked image subjected to attacks is then checked for robustness in comparison with the original watermark image using similarity measures like MSE, PSNR and NCC.

3.3 SIMILARITY ANALYSIS TECHNIQUES

Similarity analysis is one of the important portions of this thesis. Following approaches have been implemented in this thesis for image comparison.

3.3.1 Mean Square Error (MSE)

The mean square error (MSE) of an estimator measure the average of the square of the errors, that is difference between estimator and what is estimated.

In this thesis, MSE is used to compare original image and watermarked image. MSE is calculated using following formula given by equation 3.1

$$MSE = \frac{\sum_{x=1}^{m}\sum_{y=1}^{N}[I_m(x,y)-I'_m(x,y)]^2}{M.N} \qquad \textbf{Equation 3.8}$$

where M, N stands for the size of the image in both horizontal and vertical axes, I_m is the original Cover Image and I_m' is the Watermarked Image i.e., after watermark has been embedded in the Cover Image.

3.3.2 Peak Signal to Noise Ratio (PSNR)

PNSR is defined as the ratio between the maximum possible power of signal and the power of corrupting noise that affects the fidelity of representation. Because many signal have wide dynamic range PNSR is usually expressed in term of logarithmic decibel scale

PSNR is calculated using following formula given by equation 3.2

$$PSNR = 20 * \log[\frac{255}{\sqrt{MSE}}] \qquad \textbf{Equation 3.9}$$

The peak signal-to-noise ratio (PSNR) is used to evaluate the quality of the watermarked image in comparison with the host image.

3.3.3 Normalized Correlation Coefficient (NCC)

After extracting the watermark, the normalized correlation coefficient (NCC) is computed using the original watermark and the extracted watermark to judge the existence of the watermark and to measure the correctness of an extracted watermark. It is defined as:

$$NCC = \frac{\sum_i\sum_j W(i,j)*W'(i*j)}{\sqrt{\sum_i\sum_j W^2(i,j)}\sqrt{\sum_i\sum_j W'^2(i,j)}} \qquad \textbf{Equation 3.10}$$

Where, W(i,j) and W'(i,j) are pixel values at the (i,j) locations of the original watermark and the extracted watermark image respectively.

CHAPTER 4

RESULTS AND DISCUSSION

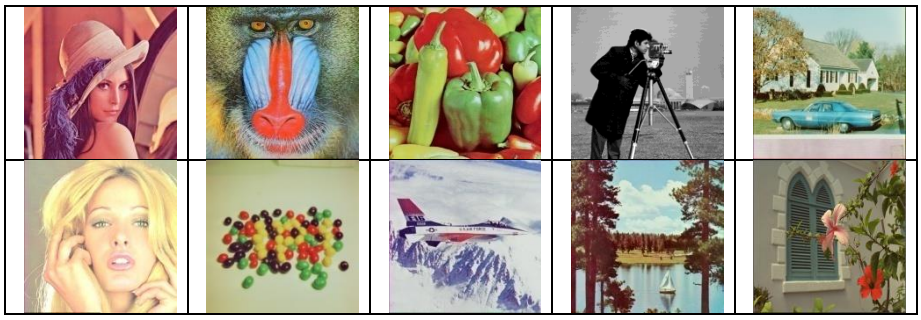
4. RESULTS AND DISCUSSIONS

4.1 DATASET

For carrying out the watermarking operation we need cover and watermark images. The cover images have been taken from The USC-SIPI Image Database, Kodak Lossless True Color Image Suite and Image Processing Place. The watermark images have been taken from Flickr Logos.

In this study, different cover and watermark images have been used to implement the various watermarking algorithms. The images are of types tiff, png and jpg. Some of the cover and watermark sample images used to carry out this study are:

Cover Images:



Watermark Images:

Figure 4.1: Cover and Watermark Images

The experiments are done by embedding and extracting watermark in cover images. The watermark is embedded in the DWT transform domain using alpha-blending technique and in DWT-SVD domain by using the singular values of SVD. The watermarking and encryption of the images are done using the algorithms mentioned in section 3.2.6. The obtained results from

different algorithm are then compared and analyzed. The details of all these procedures are described below.

4.2 ANALYSIS

Best value of factors k and q for alpha-blending technique:

The best value of k and q that gives better result while embedding and extracting watermark in cover image has been calculated as follows:

Table 4.1: PSNR and MSE for watermarked image keeping q constant and varying k and extracted watermark keeping k constant and varying q, when embedded in HH1 sub band.

		DWT Embed		Remarks			DWT Extract	
k	**Q**	**MSE**	**PSNR**		**K**	**q**	**MSE**	**PSNR**
1.5	0.001	3.73E-04	77.6196		0.001	1.5	2.40E-03	56.9284
1	0.001	9.79E-10	206.113	Best Result	0.001	1	2.40E-03	56.935
1	0.001	5.97E-07	141.9878		0.001	1	2.40E-03	56.935
0.9	0.001	1.49E-05	109.8093		0.001	0.9	2.40E-03	56.9373
0.9	0.001	3.35E-05	101.6999		0.001	0.9	2.40E-03	56.9386
0.8	0.001	7.21E-05	94.04		0.001	0.8	2.40E-03	56.9407
0.6	0.001	2.38E-04	82.083		0.001	0.6	2.40E-03	56.9484
0.2	0.001	9.54E-04	68.2199		0.001	0.2	2.40E-03	56.9303

To implement this technique we have used grayscale images of Lena as cover image and Babboon as watermark. The dimension of the image is 256*256 and is grayscale. For embedding of watermark in the original image, the value of scaling factor k is varied from 0.2 to 1.5 by keeping value of q constant and best result is obtained at k=1 and q=0.001 as seen from the table above. For extracting the watermarked image, the value of scaling factor q is varied from 0.2 to 1.5 by keeping value of k constant and best result is obtained at q=1 and k=0.001 as seen from the table above.

Now, Keeping the obtained values of the constants k and q as k=1, q=0.001, watermark was embedded in all the sub-bands of 2-level DWT, LL1, LH1, HL1 and HH1, one by one, to find in which band the watermark is imperceptible when embedded in the cover image and also to find how robust the extracted watermark is, in normal as well as in attacked condition.. The result obtained is as follows:

Cover Image: Lena (256*256)
Watermark Image: Babboon (256 * 256)

Table 4.2: Comparison to find which sub-band is most suitable for extracting robust watermark and imperceptible watermarked image

	DWT-HH1			DWT-LH1			DWT-HL1			DWT-LL1		
Attacks	**MSE**	**PSNR**	**NCC**	**MSE**	**PSNR**	**NCC**	**MSE**	**PSNR**	**NCC**	**MSE**	**PSNR**	**NCC**
	5.04E-10	212.7519		1.05E-09	2.05E+02		9.79E-10	206.1129		0.2709	11.7262	
No	7.88E-04	68.2577	0.9982	0.0016	60.875	0.9962	2.40E-03	56.935	0.9966	0.0508	26.5835	0.893
Noise												
0.01	0.0025	56.7883	0.9946	0.0018	59.8655	0.9962	0.0026	56.4507	0.9966	0.0383	29.4226	0.783
0.05	0.0032	54.3878	0.9946	0.0025	56.6141	0.9962	0.0032	54.2496	0.9965	0.0373	29.6782	0.7899
0.1	0.0041	51.8278	0.9947	0.0034	53.6167	0.9961	0.0039	52.2971	0.9964	0.0375	29.626	0.7949
0.5	0.0108	42.0873	0.9945	0.0095	43.3545	0.9962	0.0097	43.1916	0.9965	0.0333	30.8044	0.8569
Rotation												
5	0.0023	57.4763	0.9947	0.0019	59.2558	0.9964	0.0028	55.5871	0.9965	0.0603	24.8719	0.857
45	0.0025	56.7889	0.9946	0.0019	59.288	0.9963	0.0021	58.4549	0.9967	**0.098**	20.0242	0.7574
90	0.0023	57.4615	0.9946	0.0025	56.5134	0.9963	0.0015	61.6026	0.9966	0.0495	26.8426	0.8954
180	0.0023	57.581	0.9947	0.0016	60.8892	0.9962	0.0024	57.0176	0.9966	0.051	26.5497	0.8928
Crop	0.0022	57.9313	0.9947	0.0016	61.1087	0.9963	0.0021	58.4313	0.9966	0.0911	20.7523	0.9086

When checking the similarity measure between two images, whether it may be cover image and watermarked image or watermark image and extracted watermark, the value of MSE should be low and the value of PSNR should be above 45dB, to be considered as good image quality.

For robustness, the extracted watermark and the original watermark image have been compared using NCC parameter. The value of NCC equals to 1 means the extracted watermark is similar to the original watermark image. From the table above, we can see that the value of NCC for the extracted watermark embedded in LH, HL and HH sub-bands are more robust than the watermark extracted from LL sub-band.

So, from the analysis of the table above, we can see that embedding and extraction of watermark in the higher frequency bands gives better result that embedding in lower frequency band.

Best value of factor α for singular value decomposition:

From the above discussion, we know that embedding watermark in higher frequency bands give better imperceptibility and the extracted watermark image is more robust. So, it is best to embed the watermark in the middle frequency bands HL and LH. Here, the watermark has been

embedded in the HL sub-band and experiment has been carried out to find the best value of the factor α while doing DWT-SVD technique for watermark embedding and extraction. The result is as follows:

Cover Image: Lena (256*256)
Watermark Image: Babboon (256 * 256)

Table 4.3: Comparison to find the best value of α for extracting robust watermark and imperceptible watermarked image using DWT-SVD algorithm

DWT-SVD						
	α=0.1			α=0.5		
Attacks	**MSE**	**PSNR**	**NCC**	**MSE**	**PSNR**	**NCC**
Watermarked Image	9.79E-06	98.223		2.45E-04	84.2436	
No	1.22E-05	97.2672	1	1.50E-06	106.3593	1
Noise						
0.01	5.04E-04	81.1077	0.9982	1.11E-05	97.6609	1
0.05	0.0097	68.2593	0.9674	1.89E-04	85.3669	0.9993
0.1	0.0283	63.6071	0.9117	5.96E-04	80.3815	0.9979
Rotation						
5	6.47E-04	80.024	0.9977	2.97E-04	83.4071	0.9989
45	0.0058	70.5154	0.9797	0.0013	77.1302	0.9955
90	0.033	62.9447	0.892	0.0037	72.4681	0.987
Crop	0.0053	70.8861	0.9813	0.001	78.1115	0.9964

Analysis:

So, from the above analysis, it was found that the watermark image embedded in higher frequency gives imperceptible watermarked image and the watermark extracted is more robust as can be seen by comparing the similarity measures: MSE, PSNR and NCC values of Table 4.2. So, the middle frequency band HL of Haar wavelet transform was used for embedding watermark. Then Singular value decomposition was applied in the HL band of Haar wavelet transform for embedding and extraction of watermark. The best value of α for watermark insertion and extraction using SVD was found to be 0.5 as seen from Table 4.3.

We can say that DWT-SVD gives better result than using only DWT for watermark insertion and extraction.

Attacks:

Different types of attacks have been used for robustness analysis. There are different types of attacks that can be used, some of them have been implemented here. They are: Noise attacks like: Salt and Pepper Noise, Gaussian Noise and Speckle noise, Rotation, Crop, Mean and Median.

Implementation:

A GUI has been created in MATLAB to carry out the implementation of the algorithms DWT-AES, DWT-RSA, DWT-SVD-AES and DWT-SVD-RSA. Here, the attacks that have been implemented to test the robustness of the extracted watermark are: Salt and Pepper noise attack (0.05), Rotation attack (45 degree),Crop attack, Gaussian noise.(0.05), Speckle Noise(0.05), mean and median attacks.

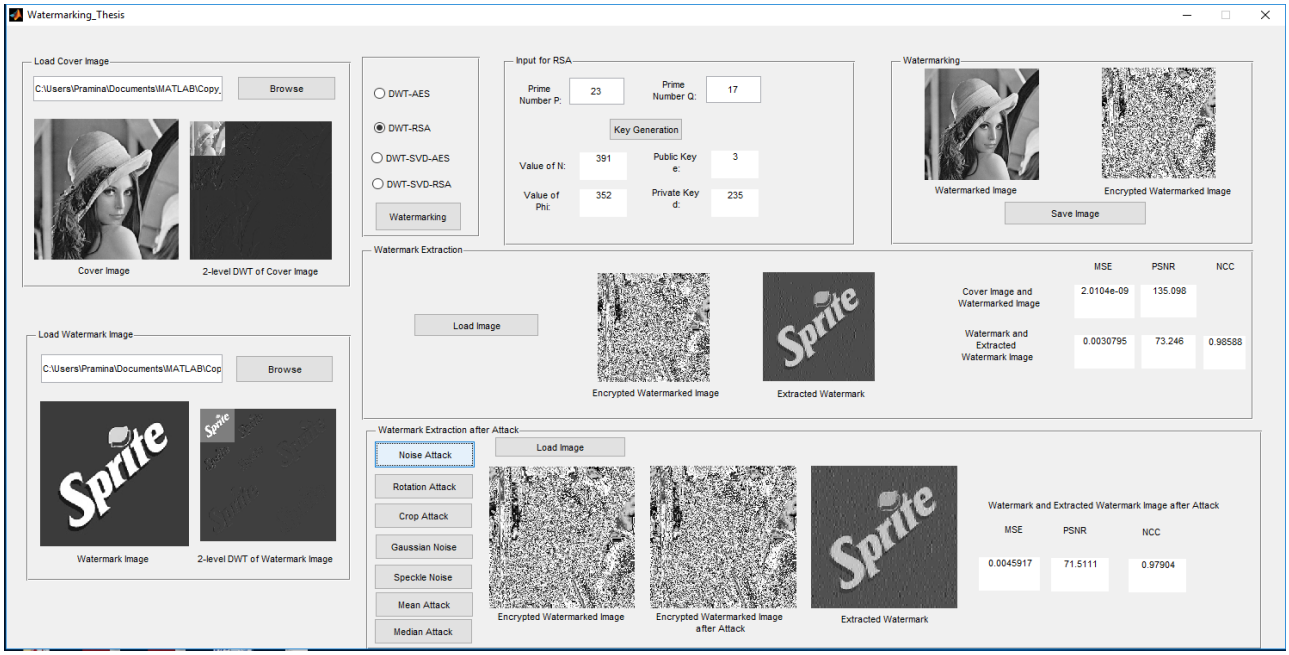


Figure 4.2: MATLAB GUI Implementation

4.3 EXPERIMENTAL ANALYSIS AND RESULTS

Several experiments were carried out to compare and analyze the performance of different watermarking algorithms. For each experiment, performance parameters have been measured and plotted to compare with other methods. As the encryption time is dependent on the size of the image used, for faster analysis, the cover and watermark images have been resized to 64*64. The key used for AES algorithm is 128-bit and for RSA algorithm the prime numbers used is (23,17) giving public key (3,391) and private key(235,391).

Example 1

Table 4.4: Comparison of similarity measure of Watermarked Image with the Cover Image using different algorithms

Algorithms	Cover Image	Watermark Image	Watermarked Image	MSE	PSNR(dB)
DWT-AES				5.5760e-09	130.6675
DWT-RSA				5.5760e-09	130.6675
DWT-SVD-AES				0.0014	76.6881
DWT-SVD-RSA				0.0014	76.6881

From the Table 4.4, comparing the similarity measures mean square error(MSE) and peak signal to noise ratio(PSNR), we can see that after embedding the watermark image in the cover image,

the obtained watermarked image is imperceptible using DWT-AES and DWT-RSA algorithms than DWT-SVD-AES and DWT-SVD-RSA algorithms. The lower the value of MSE, the higher the value of PSNR. PSNR gives the imperceptibility measure between the watermarked image and the original cover image.

Table 4.5: Comparison of similarity measure of Extracted Watermark with the Original Watermark using different algorithms

Algorithms	Watermarked Image	Encrypted Watermarked image	Extracted Watermark	MSE	PSNR(dB)	NCC
DWT-AES				0.0082	68.9948	0.9615
DWT-RSA				0.0056	70.6751	0.9737
DWT-SVD-AES				1.8469e-06	105.4665	1
DWT-SVD-RSA				1.8469e-06	105.4665	1

We can check the robustness measure of the extracted watermark from the above table. Comparing the similarity measures mean square error (MSE), peak signal to noise ratio (PSNR) and normalized cross correlation(NCC), we can see that after embedding the watermark image in the cover image, the obtained watermarked image is more robust using DWT-SVD-AES and DWT-SVD-RSA algorithms than DWT-AES and DWT-RSA algorithms. Lower the value of MSE, higher the value of PSNR. NCC gives the robustness measure between the extracted

watermark image and the original watermark image. NCC value is measured between 0 and 1 value. NCC value nearing 1 means the extracted watermark is of good quality and could withstand the attacks done on the image. And the value nearing 0 means, the extracted watermark could not withstand the attacks and it's quality is not good. Here, the watermark is extracted from the watermarked image which is not subjected to any attacks and the NCC value for DWT-SVD-AES and DWT-SVD-RSA algorithms is equal to 1. Whereas, for DWT-AES and DWT-RSA algorithms, it's nearly equal to 0.97. So both algorithms in DWT only and DWT-SVD domain give good results in case of the watermark extracted from the encrypted watermarked image not subjected to any attacks.

Extracted Watermark from Encrypted Watermarked Image subjected to various attacks:

Attacks	DWT-AES	DWT-RSA	DWT-SVD-AES	DWT-SVD-RSA
Salt and Pepper Noise(Density=0.05)				
Rotation(Angle in degree= 45)				
Crop				
Gaussian Noise (Variance=0.05)				
Speckle Noise (Variance=0.05)				
Mean				
Median				

Figure 4.3: Extracted Watermarks at different attack conditions using different algorithms

Figure 4.3 shows the extracted watermark images from encrypted watermarked image under various attack conditions.

Table 4.6: Comparison of similarity measures of Extracted Watermark with the Original Watermark at different attack conditions using different algorithms

Attacks	DWT-AES			DWT-RSA			DWT-SVD-AES			DWT-SVD-RSA		
	MSE	PSNR(dB)	NCC	MSE	PSNR(dB)	NCC	MSE	PSNR(dB)	NCC	MSE	PSNR(dB)	NCC
Salt and Pepper Noise(Density=0.05)	0.0092	68.5135	0.9571	0.0069	69.7675	0.9677	3.10E-03	73.2811	0.9856	0.012	67.3512	0.9439
Rotation(Angle in degree= 45)	0.0111	67.6609	0.9482	0.0076	69.3065	0.9641	0.0021	74.9642	0.9902	0.0083	68.9351	0.9608
Crop	0.0109	67.7603	0.9493	0.0058	70.468	0.9725	0.0021	74.8142	0.9899	0.0251	64.1317	0.8855
Gaussian Noise (Variance=0.05)	0.0114	67.5788	0.9471	0.007	69.7091	0.9672	0.0029	73.5391	0.9864	0.008	69.0879	0.9622
Speckle Noise(Variance=0.05)	0.0116	67.4994	0.9462	0.0056	70.6822	0.9738	0.0027	73.8259	0.9873	0.0181	65.5447	0.9159
Mean	0.012	67.3253	0.9441	0.0056	70.6672	0.9737	0.0011	77.6792	0.9948	0.0327	62.9842	0.8537
Median	0.0116	67.4772	0.9459	0.0056	70.6387	0.9735	0.0019	75.2394	0.9908	0.0295	63.43	0.8669

Table 4.6 gives the comparison of the different similarity measures, MSE,PSNR and NCC obtained while extracting the watermark images as shown in Figure 4.3.

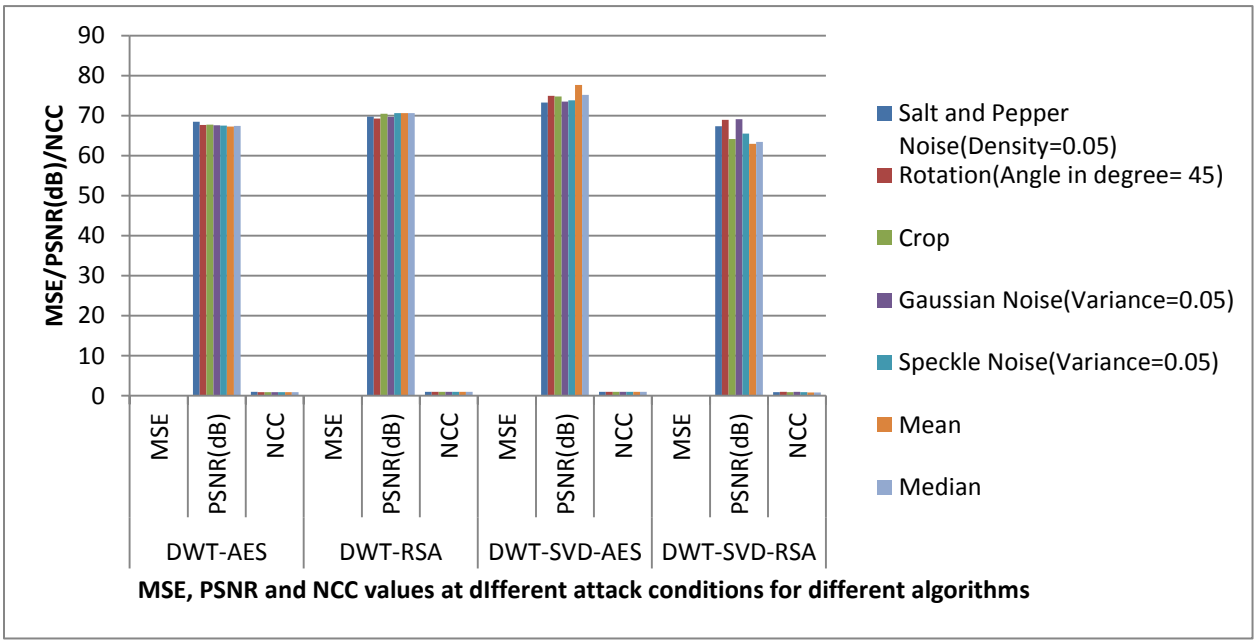
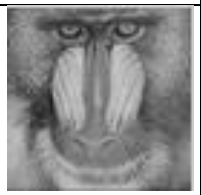
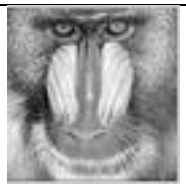
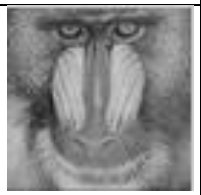
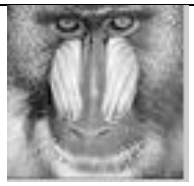
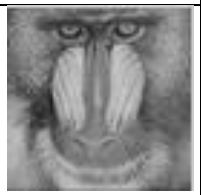
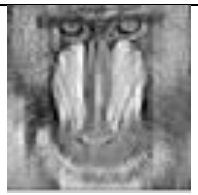
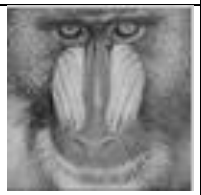
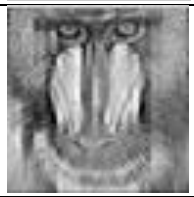


Figure 4.4: Bar Diagram for the results of Table 4.6

Figure 4.4 is the bar diagram representing the values of Table 4.6. We can see from the bar diagram that, the extracted watermark from the encrypted watermarked image subjected to various attacks, is robust and of good quality when DWT-SVD-AES algorithm is used. The PSNR value is in the range of 73 dB and value of NCC is nearly equal to 1. In the case of watermark embedded using alpha-blending in DWT domain, DWT-RSA algorithm is giving better result than DWT-AES algorithm as seen from the diagram above.

Example 2:

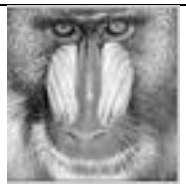
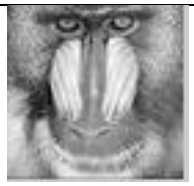
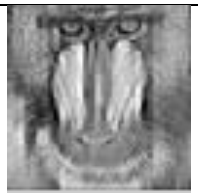
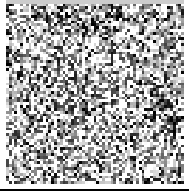
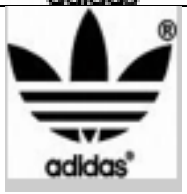
Table 4.7: Comparison of similarity measure of Watermarked Image with the Cover Image using different algorithms

Algorithms	Cover Image	Watermark Image	Watermarked Image	MSE	PSNR(dB)
DWT-AES				9.4693e-09	128.3676
DWT-RSA				9.4693e-09	128.3676
DWT-SVD-AES				0.0024	74.3882
DWT-SVD-RSA				0.0024	74.3882

From the Table 4.7, comparing the similarity measures MSE and PSNR, we can see that after embedding the watermark image in the cover image, the obtained watermarked image is imperceptible using DWT transform algorithm than DWT-SVD transform algorithms. PSNR gives the imperceptibility measure between the watermarked image and the original cover image.

Here, the PSNR value for DWT transform algorithms is 128.3 dB whereas for DWT-SVD is 74.3 dB.

Table 4.8: Comparison of similarity measure of Extracted Watermark with the Original Watermark using different algorithms

Algorithms	Watermarked Image	Encrypted Watermarked image	Extracted Watermark	MSE	PSNR(dB)	NCC
DWT-AES				0.0108	67.8050	0.9837
DWT-RSA				0.0094	68.4099	0.9858
DWT-SVD-AES				5.1496e-06	101.0131	1
DWT-SVD-RSA				5.1496e-06	101.0131	1

From the Table 4.8, we can see that after embedding the watermark image in the cover image, the obtained watermarked image is robust using DWT-SVD-AES and DWT-SVD-RSA algorithms than DWT-AES and DWT-RSA algorithms. NCC gives the robustness measure between the extracted watermark image and the original watermark image and using DWT-SVD algorithm the NCC value obtained is equal to 1. Using DWT algorithm also, the obtained value of NCC is equal to 0.98. So both algorithms in DWT only and DWT-SVD domain give good results in case of the watermark extracted from the encrypted watermarked image not subjected to any attacks.

Extracted Watermark from Encrypted Watermarked Image subjected to various attacks:

Attacks	DWT-AES	DWT-RSA	DWT-SVD-AES	DWT-SVD-RSA
Salt and Pepper Noise(Density=0.05)				
Rotation(Angle in degree= 45)				
Crop				
Gaussian Noise (Variance=0.04)				
Speckle Noise (Variance=0.03')				
Mean				
Median				

Figure 4.5: Extracted Watermarks at different attack conditions using different algorithms

Figure 4.5 shows the extracted watermark images from encrypted watermarked image under various attack conditions.

Table 4.9: Comparison of similarity measures of Extracted Watermark with the Original Watermark at different attack conditions using different algorithms

Attacks	DWT-AES			DWT-RSA			DWT-SVD-AES			DWT-SVD-RSA		
	MSE	PSNR(dB)	NCC	MSE	PSNR(dB)	NCC	MSE	PSNR(dB)	NCC	MSE	PSNR(dB)	NCC
Salt and Pepper Noise(Density=0.05)	0.0122	67.2832	0.9817	0.0112	67.6347	0.9831	3.00E-03	73.3029	0.9954	0.0123	67.2444	0.9815
Rotation(Angle in degree= 45)	0.0156	66.2132	0.9766	0.0121	67.2975	0.9817	0.0014	76.5454	0.9978	0.0087	68.7569	0.9869
Crop	0.0158	66.1417	0.9762	0.0097	68.258	0.9853	0.0037	72.5015	0.9945	0.0193	65.2738	0.9709
Gaussian Noise(Variance=0.04)	0.0162	66.0316	0.9756	0.0097	68.2588	0.9853	0.0033	72.9542	0.995	0.0096	68.2885	0.9854
Speckle Noise(Variance=0.03)	0.017	65.8346	0.9745	0.0094	68.3812	0.9857	0.0032	73.1277	0.9952	0.0094	68.3775	0.9857
Mean	0.0163	66.0095	0.9755	0.0095	68.3675	0.9857	9.40E-04	78.3996	0.9986	0.0283	63.6138	0.9576
Median	0.0174	65.7204	0.9738	0.0095	68.3506	0.9856	0.0027	73.7478	0.9959	0.026	63.9791	0.961

Table 4.9 gives the comparison of the different similarity measures, MSE, PSNR and NCC obtained while extracting the watermark images as shown in Figure 4.5.

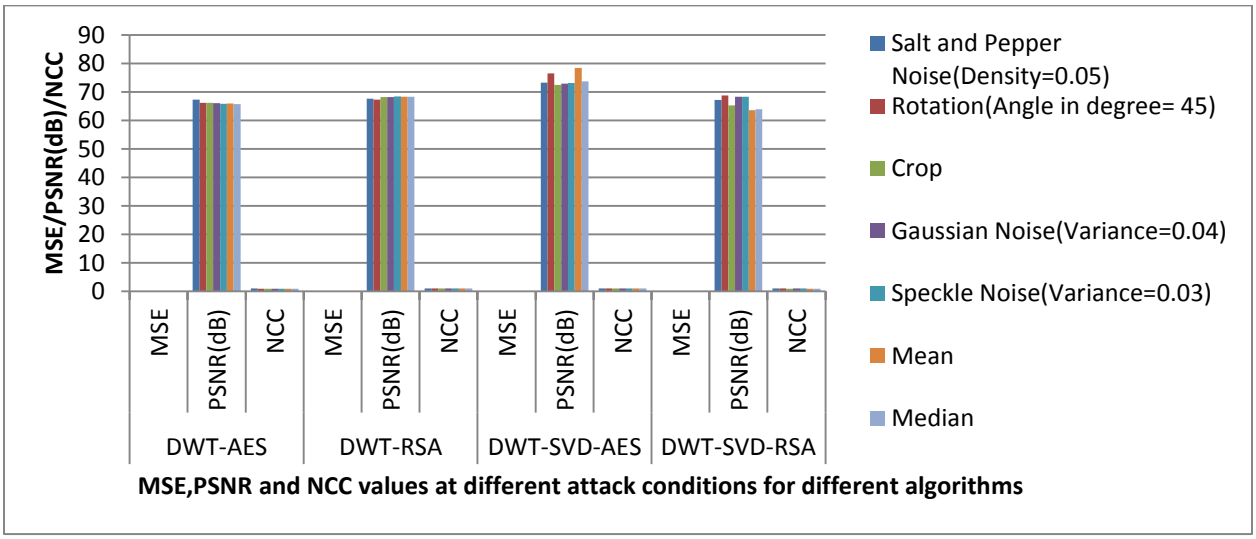


Figure 4.6: Bar Diagram for the results of Table 4.9

Figure 4.6 is the bar diagram representing the values of Table 4.9. We can see from the bar diagram that, the extracted watermark from the encrypted watermarked image subjected to various attacks, is robust and of good quality when DWT-SVD-AES algorithm is used. The PSNR value is in the range of 73 dB and value of NCC is nearly equal to 1. In the case of

watermark embedded using alpha-blending in DWT domain, DWT-RSA algorithm is giving better result than DWT-AES algorithm as seen from the diagram above.

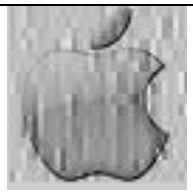
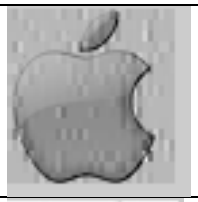
Example 3

Table 4.10: Comparison of similarity measure of Watermarked Image with the Cover Image using different algorithms

Algorithms	Cover Image	Watermark Image	Watermarked Image	MSE	PSNR(dB)
DWT-AES				1.3099e-09	136.9585
DWT-RSA				1.3099e-09	136.9585
DWT-SVD-AES				3.2747e-04	82.9791
DWT-SVD-RSA				3.2747e-04	82.9791

From the Table 4.10, comparing the similarity measures MSE and PSNR, we can see that after embedding the watermark image in the cover image, the obtained watermarked image is more imperceptible using DWT transform algorithm than DWT-SVD transform algorithms. PSNR gives the imperceptibility measure between the watermarked image and the original cover image. Here, the PSNR value for DWT transform algorithms is 136 dB whereas for DWT-SVD is 82.9 dB.

Table 4.11: Comparison of similarity measure of Extracted Watermark with the Original Watermark using different algorithms

Algorithms	Watermarked Image	Encrypted Watermarked image	Extracted Watermark	MSE	PSNR(dB)	NCC
DWT-AES				0.0049	71.2556	0.9940
DWT-RSA				0.0024	74.3688	0.9971
DWT-SVD-AES				4.5093e-06	101.5897	1
DWT-SVD-RSA				4.5093e-06	101.5897	1

From the Table 4.11, we can see that after embedding the watermark image in the cover image, the obtained watermarked image is robust using both the algorithms in DWT domain and DWT-SVD domain. NCC gives the robustness measure between the extracted watermark image and the original watermark image and using DWT-SVD algorithm the NCC value obtained is equal to 1. Using DWT algorithm also, the obtained value of NCC is equal to 0.99. So both algorithms in DWT only and DWT-SVD domain give good results in case of the watermark extracted from the encrypted watermarked image not subjected to any attacks.

Extracted Watermark from Encrypted Watermarked Image subjected to various attacks:

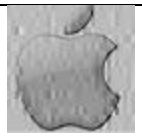
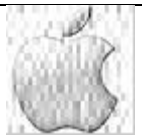
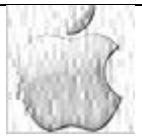
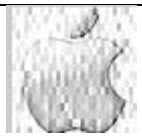
Attacks	DWT-AES	DWT-RSA	DWT-SVD-AES	DWT-SVD-RSA
Salt and Pepper Noise(Density=0.05)				
Rotation(Angle in degree= 45)				
Crop				
Gaussian Noise (Variance=0.03)				
Speckle Noise (Variance=0.04)				
Mean				
Median				

Figure 4.7: Extracted Watermarks at different attack conditions using different algorithms

Figure 4.7 shows the extracted watermark images from encrypted watermarked image under various attack conditions.

Table 4.12: Comparison of similarity measures of Extracted Watermark with the Original Watermark at different attack conditions using different algorithms

Attacks	DWT-AES			DWT-RSA			DWT-SVD-AES			DWT-SVD-RSA		
	MSE	PSNR(dB)	NCC	MSE	PSNR(dB)	NCC	MSE	PSNR(dB)	NCC	MSE	PSNR(dB)	NCC
Salt and Pepper Noise(Density=0.05)	0.0051	71.0209	0.9937	0.003	73.365	0.9963	6.83E-04	79.7864	0.9992	0.005	71.1524	0.9938
Rotation(Angle in degree= 45)	0.0079	69.1613	0.9903	0.0045	71.5943	0.9944	3.88E-04	82.2471	0.9995	0.0029	73.4378	0.9964
Crop	0.0054	70.7781	0.9933	0.0018	75.5037	0.9977	0.0014	76.7512	0.9983	0.0098	68.2131	0.9879
Gaussian Noise(Variance=0.03)	0.0074	69.4218	0.9909	0.002	75.0241	0.9975	7.85E-04	79.1797	0.999	0.0045	71.5749	0.9944
Speckle Noise(Variance=0.04)	0.0063	70.1703	0.9923	0.002	75.1207	0.9975	0.0011	77.6824	0.9986	0.0068	69.7849	0.9916
Mean	0.0102	68.0588	0.9875	0.0016	75.9903	0.998	7.56E-04	79.347	0.9991	0.0128	67.0684	0.9843
Median	0.006	70.3149	0.9926	0.0017	75.9133	0.9979	6.21E-04	80.1981	0.9992	0.0122	67.2622	0.985

Table 4.12 gives the comparison of the different similarity measures, MSE, PSNR and NCC obtained while extracting the watermark images as shown in Figure 4.7.

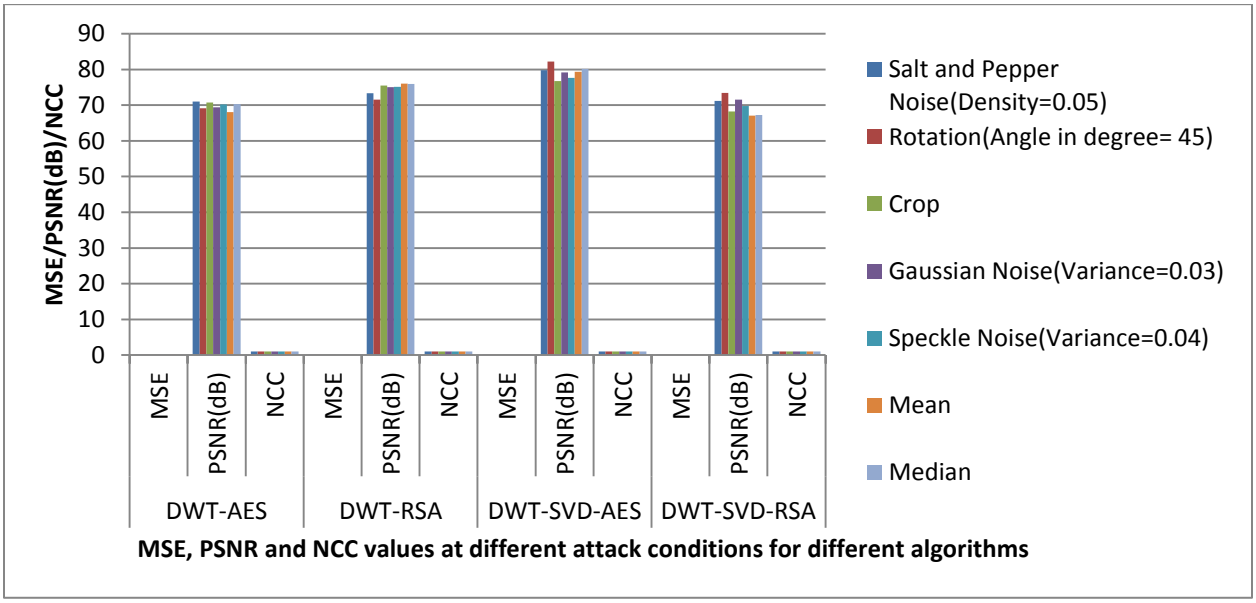


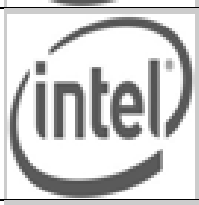
Figure 4.8: Bar Diagram for the results of Table 4.12

Figure 4.8 is the bar diagram representing the values of Table 4.12. We can see from the bar diagram that, the extracted watermark from the encrypted watermarked image subjected to various attacks, is robust and of good quality when DWT-SVD-AES algorithm is used. The PSNR value is in the range of 73 dB and value of NCC is nearly equal to 1. In the case of

watermark embedded using alpha-blending in DWT domain, DWT-RSA algorithm is giving marginally better result than DWT-AES algorithm as seen from the diagram above.

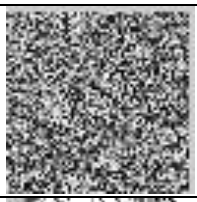
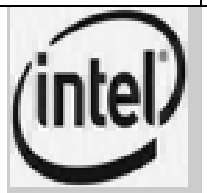
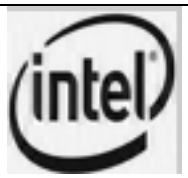
Example 4

Table 4.13: Comparison of similarity measure of Watermarked Image with the Cover Image using different algorithms

Algorithms	Cover Image	Watermark Image	Watermarked Image	MSE	PSNR(dB)
DWT-AES				9.9084e-09	128.1707
DWT-RSA				9.9084e-09	128.1707
DWT-SVD-AES				0.0025	74.1913
DWT-SVD-RSA				0.0025	74.1913

From the Table 4.13, comparing the similarity measures MSE and PSNR, we can see that after embedding the watermark image in the cover image, the obtained watermarked image is more imperceptible using DWT transform algorithm than DWT-SVD transform algorithms. PSNR gives the imperceptibility measure between the watermarked image and the original cover image. Here, the PSNR value for DWT transform algorithms is 128 dB whereas for DWT-SVD is 74 dB.

Table 4.14: Comparison of similarity measure of Extracted Watermark with the Original Watermark using different algorithms

Algorithms	Watermarked Image	Encrypted Watermarked image	Extracted Watermark	MSE	PSNR(dB)	NCC
DWT-AES				0.0113	67.5990	0.9845
DWT-RSA				0.0118	67.4138	0.9838
DWT-SVD-AES				3.9675e-04	82.1457	0.9995
DWT-SVD-RSA				3.9675e-04	82.1457	0.9995

From the Table 4.14, we can see that after embedding the watermark image in the cover image, the obtained watermarked image is robust using both the algorithms in DWT domain and DWT-SVD domain. NCC gives the robustness measure between the extracted watermark image and the original watermark image and using DWT-SVD algorithm the NCC value obtained is equal to 1. Using DWT algorithm also, the obtained value of NCC is equal to 0.98. So both algorithms in DWT only and DWT-SVD domain give good results in case of the watermark extracted from the encrypted watermarked image not subjected to any attacks.

Extracted Watermark from Encrypted Watermarked Image subjected to various attacks:

Attacks	DWT-AES	DWT-RSA	DWT-SVD-AES	DWT-SVD-RSA
Salt and Pepper Noise(Density=0.05)				
Rotation(Angle in degree= 90)				
Crop				
Gaussian Noise (Variance=0.02)				
Speckle Noise (Variance=0.01)				
Mean				
Median				

Figure 4.9: Extracted Watermarks at different attack conditions using different algorithms

Figure 4.9 shows the extracted watermark images from encrypted watermarked image under various attack conditions.

Table 4.15: Comparison of similarity measures of Extracted Watermark with the Original Watermark at different attack conditions using different algorithms

Attacks	DWT-AES			DWT-RSA			DWT-SVD-AES			DWT-SVD-RSA		
	MSE	PSNR(dB)	NCC	MSE	PSNR(dB)	NCC	MSE	PSNR(dB)	NCC	MSE	PSNR(dB)	NCC
Salt and Pepper Noise (Density=0.05)	0.0131	66.9619	0.9821	0.0132	66.9313	0.9819	6.00E-03	70.3139	0.9917	0.0044	71.6638	0.9939
Rotation (Angle in degree= 90)	0.0157	66.1701	0.9785	0.0117	67.4632	0.984	0.0062	70.2014	0.9915	0.0041	71.9574	0.9943
Crop	0.014	66.6593	0.9808	0.011	67.7007	0.9849	0.0059	70.4259	0.9919	0.0054	70.7848	0.9926
Gaussian Noise (Variance=0.02)	0.0164	65.9732	0.9775	0.0114	67.562	0.9844	0.0059	70.399	0.9919	0.0035	72.7099	0.9952
Speckle Noise (Variance=0.01)	0.0162	66.0378	0.9779	0.0114	67.5576	0.9844	0.0059	70.3966	0.9919	0.0048	71.3484	0.9935
Mean	0.0173	65.7514	0.9764	0.0109	67.7717	0.9851	0.0052	70.9337	0.9928	0.0051	71.0507	0.993
Median	0.0144	66.5618	0.9804	0.0109	67.7548	0.9851	0.0055	70.7448	0.9925	0.0049	71.2073	0.9933

Table 4.15 gives the comparison of the different similarity measures, MSE, PSNR and NCC obtained while extracting the watermark images as shown in Figure 4.9.

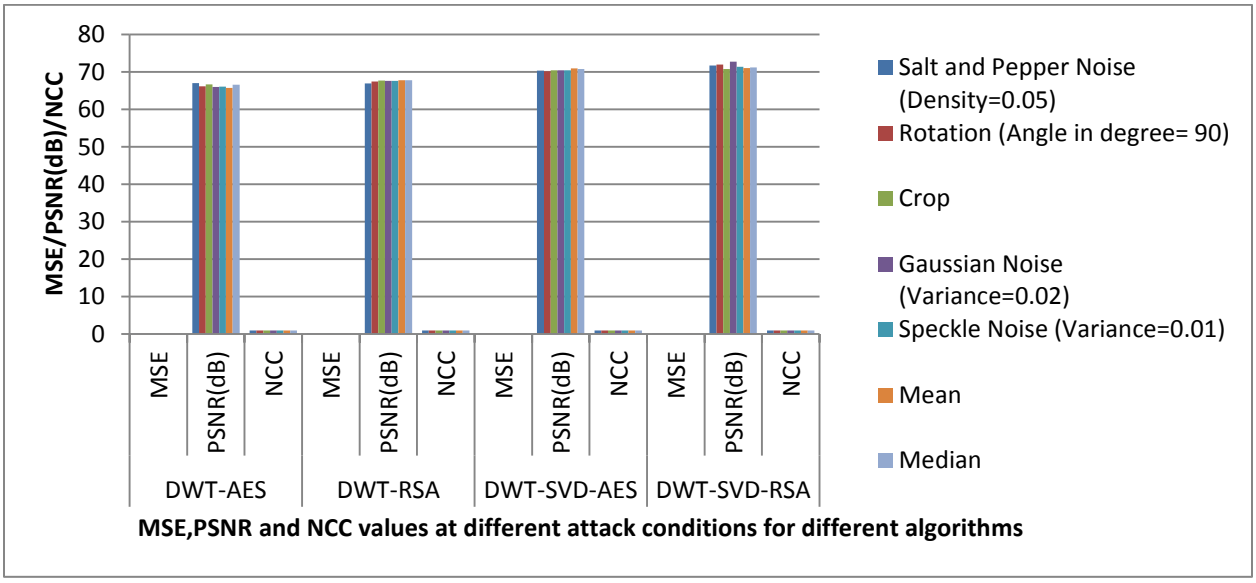


Figure 4.10: Bar Diagram for the results of Table 4.15

Figure 4.10 is the bar diagram representing the values of Table 4.15. We can see from the bar diagram that, the extracted watermark from the encrypted watermarked image subjected to various attacks, is robust and of good quality when DWT-SVD-AES and DWT-SVD-RSA algorithms are used. The PSNR value is in the range of 70 dB and value of NCC is nearly equal

to 1. In the case of watermark embedded using alpha-blending in DWT domain, DWT-RSA and DWT-AES algorithms are giving similar results.

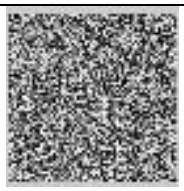
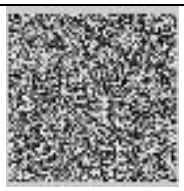
Example 5

Table 4.16: Comparison of similarity measure of Watermarked Image with the Cover Image using different algorithms

Algorithms	Cover Image	Watermark Image	Watermarked Image	MSE	PSNR(dB)
DWT-AES				6.4620e-09	130.0272
DWT-RSA				6.4620e-09	130.0272
DWT-SVD-AES				0.0016	76.0478
DWT-SVD-RSA				0.0016	76.0478

From the Table 4.16, comparing the similarity measures MSE and PSNR, we can see that after embedding the watermark image in the cover image, the obtained watermarked image is more imperceptible using DWT transform algorithm than DWT-SVD transform algorithms. PSNR gives the imperceptibility measure between the watermarked image and the original cover image. Here, the PSNR value for DWT transform algorithms is 130 dB whereas for DWT-SVD is 76 dB.

Table 4.17: Comparison of similarity measure of Extracted Watermark with the Original Watermark using different algorithms

Algorithms	Watermarked Image	Encrypted Watermarked image	Extracted Watermark	MSE	PSNR(dB)	NCC
DWT-AES				0.0088	68.7024	0.9817
DWT-RSA				0.0066	69.9563	0.9863
DWT-SVD-AES				1.8375e-05	95.4885	1
DWT-SVD-RSA				1.8375e-05	95.4885	1

From the Table 4.17, we can see that after embedding the watermark image in the cover image, the obtained watermarked image is robust using both the algorithms in DWT domain and DWT-SVD domain. NCC gives the robustness measure between the extracted watermark image and the original watermark image and using DWT-SVD algorithm the NCC value obtained is equal to 1. Using DWT algorithm also, the obtained value of NCC is equal to 0.98. So both algorithms in DWT only and DWT-SVD domain give good results in case of the watermark extracted from the encrypted watermarked image not subjected to any attacks.

Extracted Watermark from Encrypted Watermarked Image subjected to various attacks

Attacks	DWT-AES	DWT-RSA	DWT-SVD-AES	DWT-SVD-RSA
Salt and Pepper Noise(Density=0.05)				
Rotation(Angle in degree= 45)				
Crop				
Gaussian Noise (Variance=0.01)				
Speckle Noise (Variance=0.02)				
Mean				
Median				

Figure 4.11: Extracted Watermarks at different attack conditions using different algorithms

Figure 4.11 shows the extracted watermark images from encrypted watermarked image under various attack conditions.

Table 4.18: Comparison of similarity measures of Extracted Watermark with the Original Watermark at different attack conditions using different algorithms

Attacks	DWT-AES			DWT-RSA			DWT-SVD-AES			DWT-SVD-RSA		
	MSE	PSNR(dB)	NCC	MSE	PSNR(dB)	NCC	MSE	PSNR(dB)	NCC	MSE	PSNR(dB)	NCC
Salt and Pepper Noise (Density=0.05)	0.0097	68.2839	0.9799	0.007	69.6517	0.9853	2.20E-03	74.6549	0.9954	0.0087	68.7466	0.9819
Rotation (Angle in degree= 45)	0.0119	67.3816	0.9754	0.0091	68.5327	0.981	0.001	78.0714	0.9979	0.0062	70.2148	0.9871
Crop	0.0105	67.9227	0.9782	0.007	69.6865	0.9854	0.0027	73.8652	0.9944	0.0144	66.5611	0.9702
Gaussian Noise (Variance=0.01)	0.0115	67.5167	0.9761	0.0066	69.9139	0.9862	0.0019	75.4539	0.9961	0.0096	68.3151	0.98
Speckle Noise (Variance=0.02)	0.0107	67.8399	0.9778	0.0066	69.9505	0.9863	0.0023	74.4329	0.9951	0.0119	67.377	0.9753
Mean	0.0138	66.7199	0.9714	0.0065	70.0276	0.9865	0.0013	77.0531	0.9973	0.0168	65.8876	0.9652
Median	0.0125	67.1525	0.9741	0.0065	70.0098	0.9865	0.002	75.0602	0.9958	0.016	66.0922	0.9668

Table 4.18 gives the comparison of the different similarity measures, MSE, PSNR and NCC obtained while extracting the watermark images as shown in Figure 4.11.

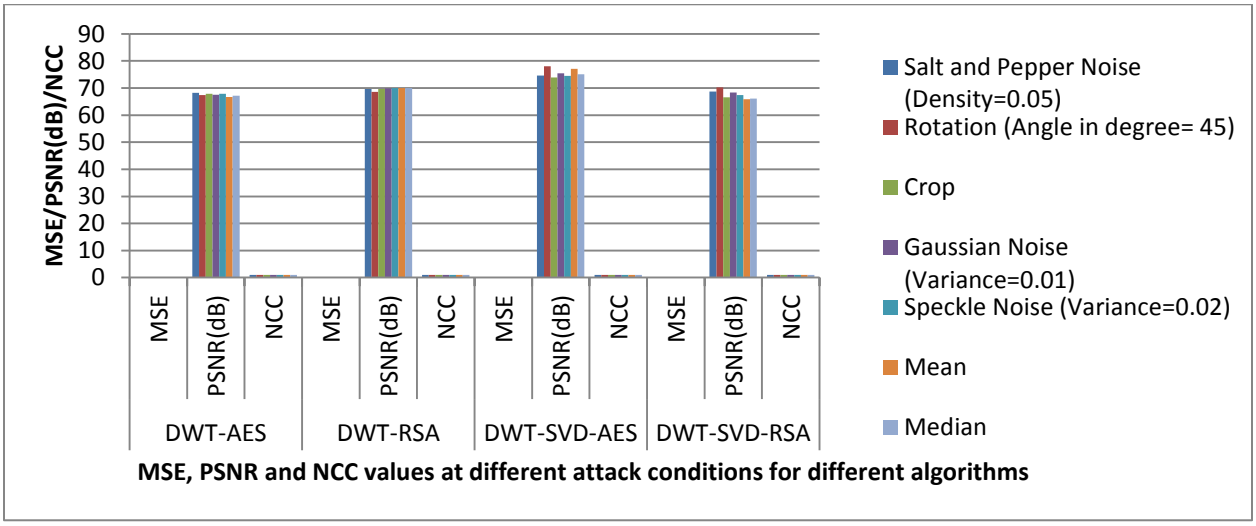


Figure 4.12: Bar Diagram for the results of Table 4.18

Figure 4.12 is the bar diagram representing the values of Table 4.18. We can see from the bar diagram that, the extracted watermark from the encrypted watermarked image subjected to various attacks, is robust and of good quality when DWT-SVD-AES algorithm is used. The PSNR value is in the range of 75 dB and value of NCC is nearly equal to 1. In the case of watermark embedded using alpha-blending in DWT domain, DWT-RSA is giving marginally better result than DWT-AES algorithm.

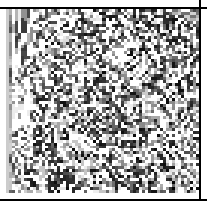
Example 6

Table 4.19: Comparison of similarity measure of Watermarked Image with the Cover Image using different algorithms

Algorithms	Cover Image	Watermark Image	Watermarked Image	MSE	PSNR(dB)
DWT-AES				6.2124e-09	130.1982
DWT-RSA				6.2124e-09	130.1982
DWT-SVD-AES				0.0016	76.2188
DWT-SVD-RSA				0.0016	76.2188

From the Table 4.19, comparing the similarity measures MSE and PSNR, we can see that after embedding the watermark image in the cover image, the obtained watermarked image is more imperceptible using DWT transform algorithm than DWT-SVD transform algorithms. PSNR gives the imperceptibility measure between the watermarked image and the original cover image. Here, the PSNR value for DWT transform algorithms is 130 dB whereas for DWT-SVD is 76 dB.

Table 4.20: Comparison of similarity measure of Extracted Watermark with the Original Watermark using different algorithms

Algorithms	Watermarked Image	Encrypted Watermarked image	Extracted Watermark	MSE	PSNR(dB)	NCC
DWT-AES				0.0073	69.4999	0.9904
DWT-RSA				0.0063	70.1476	0.9918
DWT-SVD-AES				8.8906e-05	88.6415	0.9999
DWT-SVD-RSA				8.8906e-05	88.6415	0.9999

From the Table 4.20, we can see that after embedding the watermark image in the cover image, the obtained watermarked image is more robust using DWT-SVD-AES and DWT-SVD-RSA algorithms than DWT-AES and DWT-RSA algorithms. NCC gives the robustness measure between the extracted watermark image and the original watermark image and using DWT-SVD algorithm the NCC value obtained is equal to 0.99. Using DWT algorithm also, the obtained value of NCC is equal to 0.99. So both algorithms in DWT only and DWT-SVD domain give good results in case of the watermark extracted from the encrypted watermarked image not subjected to any attacks.

Extracted Watermark from Encrypted Watermarked Image subjected to various attacks:

Attacks	DWT-AES	DWT-RSA	DWT-SVD-AES	DWT-SVD-RSA
Salt and Pepper Noise(Density=0.05)				
Rotation(Angle in degree= 45)				
Crop				
Gaussian Noise (Variance=0.06)				
Speckle Noise (Variance=0.05)				
Mean				
Median				

Figure 4.13: Extracted Watermarks at different attack conditions using different algorithms

Figure 4.13 shows the extracted watermark images from encrypted watermarked image under various attack conditions.

Table 4.21: Comparison of similarity measures of Extracted Watermark with the Original Watermark at different attack conditions using different algorithms

Attacks	DWT-AES			DWT-RSA			DWT-SVD-AES			DWT-SVD-RSA		
	MSE	PSNR(dB)	NCC	MSE	PSNR(dB)	NCC	MSE	PSNR(dB)	NCC	MSE	PSNR(dB)	NCC
Salt and Pepper Noise (Density=0.05)	0.01	68.128	0.9869	0.007	69.6776	0.9908	2.00E-03	75.0739	0.9974	0.0083	68.9262	0.9891
Rotation (Angle in degree= 45)	0.0143	66.5674	0.9813	0.0086	68.8054	0.9888	0.0012	77.3679	0.9984	0.0048	71.3541	0.9938
Crop	0.0122	67.2823	0.9841	0.0064	70.0921	0.9917	0.0016	76.1375	0.9979	0.0148	66.4262	0.9806
Gaussian Noise (Variance=0.06)	0.012	67.351	0.9844	0.0062	70.1948	0.9919	0.0018	75.538	0.9976	0.0041	71.9758	0.9946
Speckle Noise (Variance=0.05)	0.011	67.7326	0.9857	0.0063	70.1308	0.9917	0.0018	75.4999	0.9976	0.0148	66.4165	0.9806
Mean	0.0138	66.7252	0.982	0.0062	70.1983	0.9919	0.0017	75.8273	0.9978	0.0195	65.2262	0.9745
Median	0.0112	67.6291	0.9853	0.0063	70.1192	0.9917	0.0017	75.8311	0.9978	0.0179	65.6067	0.9767

Table 4.21 gives the comparison of the different similarity measures, MSE, PSNR and NCC obtained while extracting the watermark images as shown in Figure 4.13.

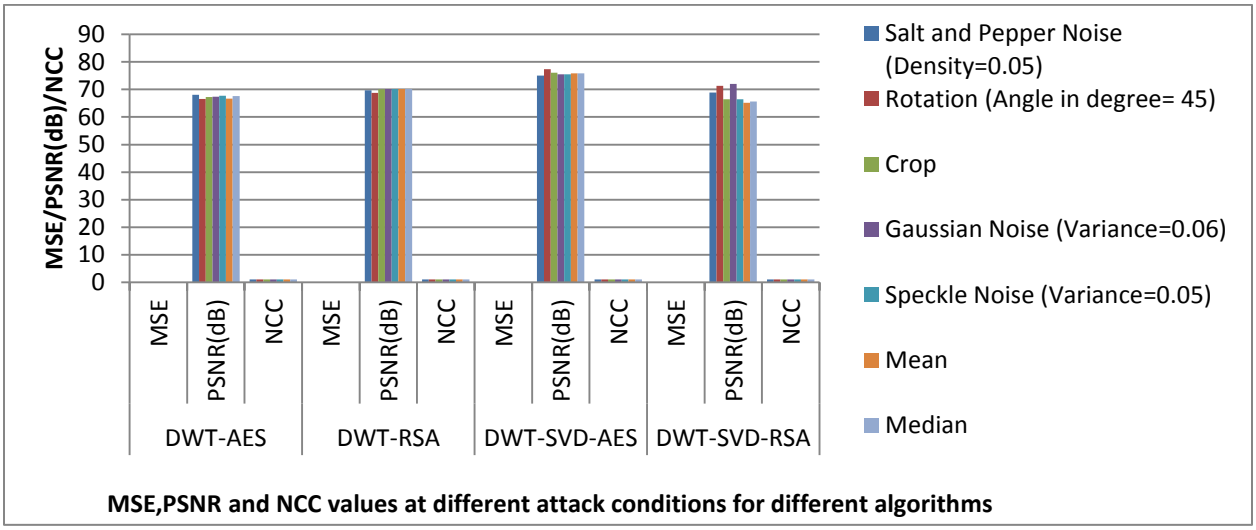
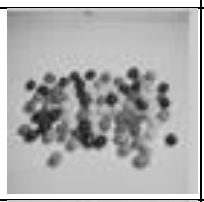
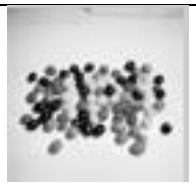
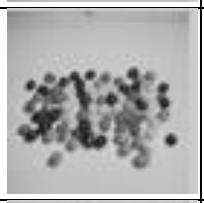
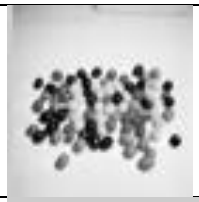
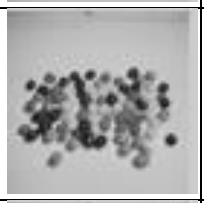
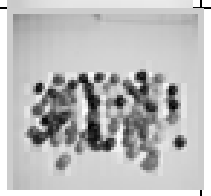
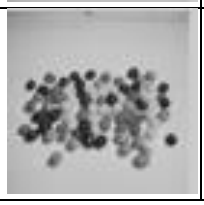
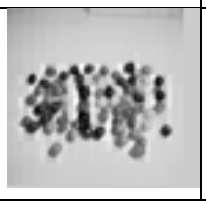


Figure 4.14: Bar Diagram for the results of Table 4.21

Figure 4.14 is the bar diagram representing the values of Table 4.21. We can see from the bar diagram that, the extracted watermark from the encrypted watermarked image subjected to various attacks, is robust and of good quality when DWT-SVD-AES and DWT-SVD-RSA algorithms are used. The PSNR value is in the range of 75 dB and value of NCC is nearly equal to 1. In the case of watermark embedded using alpha-blending in DWT domain, DWT-RSA and DWT-AES algorithms are giving similar results.

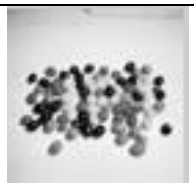
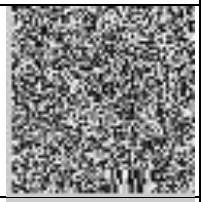
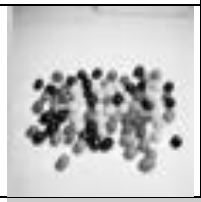
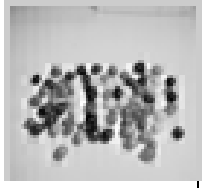
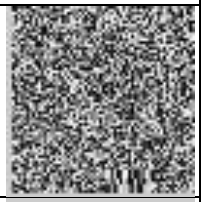
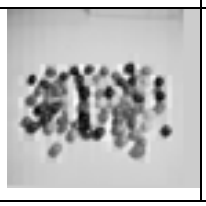
Example 7

Table 4.22: Comparison of similarity measure of Watermarked Image with the Cover Image using different algorithms

Algorithms	Cover Image	Watermark Image	Watermarked Image	MSE	PSNR(dB)
DWT-AES				6.5924e-09	129.9404
DWT-RSA				6.5924e-09	129.9404
DWT-SVD-AES				0.0016	75.9610
DWT-SVD-RSA				0.0016	75.9610

From the Table 4.22, comparing the similarity measures MSE and PSNR, we can see that after embedding the watermark image in the cover image, the obtained watermarked image is more imperceptible using DWT transform algorithm than DWT-SVD transform algorithms. PSNR gives the imperceptibility measure between the watermarked image and the original cover image. Here, the PSNR value for DWT transform algorithms is 129 dB whereas for DWT-SVD is 75 dB.

Table 4.23: Comparison of similarity measure of Extracted Watermark with the Original Watermark using different algorithms

Algorithms	Watermarked Image	Encrypted Watermarked image	Extracted Watermark	MSE	PSNR(dB)	NCC
DWT-AES				0.0109	67.7445	0.9432
DWT-RSA				0.0068	69.8369	0.9647
DWT-SVD-AES				2.2566e-06	104.5964	1
DWT-SVD-RSA				2.2566e-06	104.5964	1

From the Table 4.23, we can see that after embedding the watermark image in the cover image, the obtained watermarked image is more robust using DWT-SVD-AES and DWT-SVD-RSA algorithms than DWT-AES and DWT-RSA algorithms. NCC gives the robustness measure between the extracted watermark image and the original watermark image and using DWT-SVD algorithm the NCC value obtained is equal to 1. Using DWT algorithm also, the obtained value of NCC is equal to 0.96. So both algorithms in DWT only and DWT-SVD domain give good results in case of the watermark extracted from the encrypted watermarked image not subjected to any attacks.

Extracted Watermark from Encrypted Watermarked Image subjected to various attacks:

Attacks	DWT-AES	DWT-RSA	DWT-SVD-AES	DWT-SVD-RSA
Salt and Pepper Noise(Density=0.05)				
Rotation(Angle in degree= 45)				
Crop				
Gaussian Noise (Variance=0.05)				
Speckle Noise (Variance=0.05)				
Mean				
Median				

Figure 4.15: Extracted Watermarks at different attack conditions using different algorithms

Figure 4.15 shows the extracted watermark images from encrypted watermarked image under various attack conditions.

Table 4.24: Comparison of similarity measures of Extracted Watermark with the Original Watermark at different attack conditions using different algorithms

Attacks	DWT-AES			DWT-RSA			DWT-SVD-AES			DWT-SVD-RSA		
	MSE	PSNR(dB)	NCC	MSE	PSNR(dB)	NCC	MSE	PSNR(dB)	NCC	MSE	PSNR(dB)	NCC
Salt and Pepper Noise(Density=0.05)	0.011	67.71	0.943	0.008	69.35	0.961	6.50E-03	70.034	0.966	0.016	66.03	0.916
Rotation(Angle in degree= 45)	0.014	66.799	0.93	0.008	68.997	0.957	0.0044	71.68	0.977	0.013	66.951	0.932
Crop	0.011	67.606	0.942	0.007	69.689	0.964	0.0063	70.12	0.967	0.024	64.273	0.877
Gaussian Noise (Variance=0.05)	0.011	67.905	0.946	0.008	69.046	0.958	0.0064	70.094	0.967	0.012	67.273	0.937
Speckle Noise(Variance=0.05)	0.013	67.142	0.935	0.007	69.8	0.964	0.0054	70.845	0.972	0.021	64.848	0.891
Mean	0.014	66.607	0.927	0.007	69.941	0.966	0.0055	70.731	0.971	0.029	63.554	0.856
Median	0.013	67.177	0.936	0.007	69.925	0.965	0.0069	69.758	0.964	0.027	63.856	0.865

Table 4.24 gives the comparison of the different similarity measures, MSE, PSNR and NCC obtained while extracting the watermark images as shown in Figure 4.15.

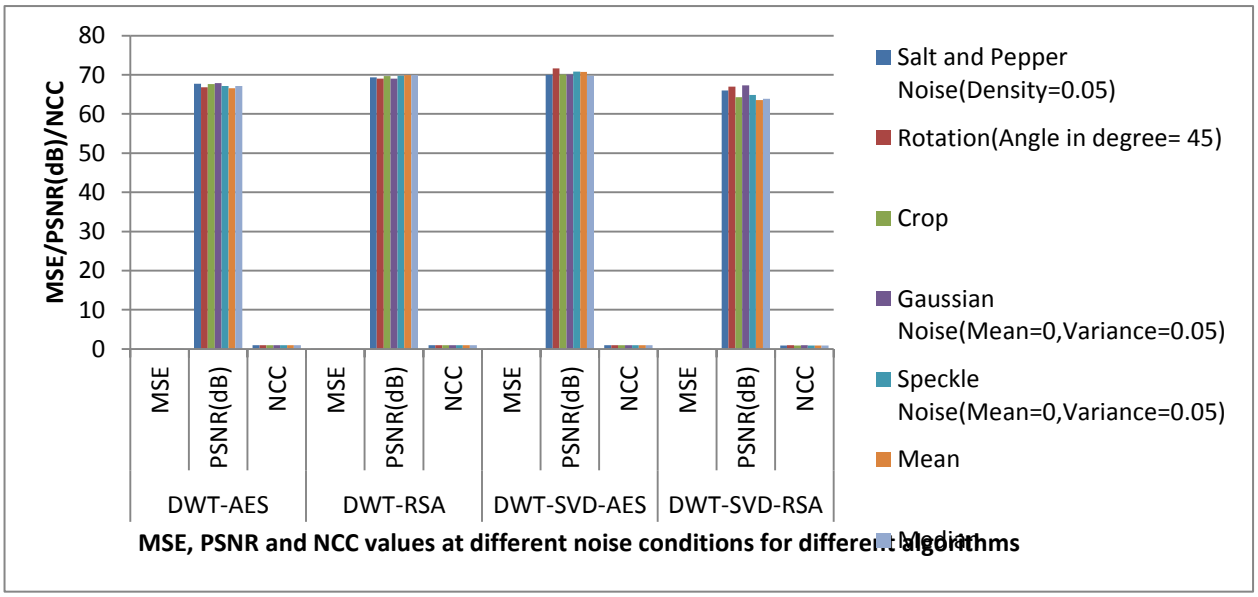


Figure 4.16: Bar Diagram for the results of Table 4.24

Figure 4.16 is the bar diagram representing the values of Table 4.24. We can see from the bar diagram that, the extracted watermark from the encrypted watermarked image subjected to various attacks, is robust and of good quality when DWT-SVD-AES and DWT-RSA algorithms are used. The PSNR value is in the range of 70 dB and 69 dB respectively.

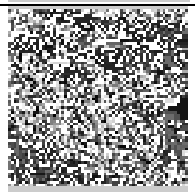
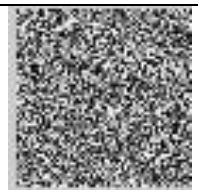
Example 8

Table 4.25: Comparison of similarity measure of Watermarked Image with the Cover Image using different algorithms

Algorithms	Cover Image	Watermark Image	Watermarked Image	MSE	PSNR(dB)
DWT-AES				9.3109e-09	128.4409
DWT-RSA				9.3109e-09	128.4409
DWT-SVD-AES				0.0023	74.4615
DWT-SVD-RSA				0.0023	74.4615

From the Table 4.25, comparing the similarity measures MSE and PSNR, we can see that after embedding the watermark image in the cover image, the obtained watermarked image is more imperceptible using DWT transform algorithm than DWT-SVD transform algorithms. PSNR gives the imperceptibility measure between the watermarked image and the original cover image. Here, the PSNR value for DWT transform algorithms is 128 dB whereas for DWT-SVD is 74 dB.

Table 4.26: Comparison of similarity measure of Extracted Watermark with the Original Watermark using different algorithms

Algorithms	Watermarked Image	Encrypted Watermarked image	Extracted Watermark	MSE	PSNR(dB)	NCC
DWT-AES				0.0108	67.7798	0.9817
DWT-RSA				0.0096	68.3244	0.9838
DWT-SVD-AES				3.5038e-05	92.6854	0.9999
DWT-SVD-RSA				3.5038e-05	92.6854	0.9999

From the Table 4.26, we can see that after embedding the watermark image in the cover image, the obtained watermarked image is more robust using DWT-SVD-AES and DWT-SVD-RSA algorithms than DWT-AES and DWT-RSA algorithms. NCC gives the robustness measure between the extracted watermark image and the original watermark image and using DWT-SVD algorithm the NCC value obtained is equal to 0.99. Using DWT algorithm also, the obtained value of NCC is equal to 0.98. So both algorithms in DWT only and DWT-SVD domain give good results in case of the watermark extracted from the encrypted watermarked image not subjected to any attacks.

Extracted Watermark from Encrypted Watermarked Image subjected to various attacks:

Attacks	DWT-AES	DWT-RSA	DWT-SVD-AES	DWT-SVD-RSA
Salt and Pepper Noise (Density=0.05)				
Rotation (Angle in degree= 45)				
Crop				
Gaussian Noise (Variance=0.05)				
Speckle Noise (Variance=0.05)				
Mean				
Median				

Figure 4.17: Extracted Watermarks at different attack conditions using different algorithms

Figure 4.17 shows the extracted watermark images from encrypted watermarked image under various attack conditions.

Table 4.27: Comparison of similarity measures of Extracted Watermark with the Original Watermark at different attack conditions using different algorithms

Attacks	DWT-AES			DWT-RSA			DWT-SVD-AES			DWT-SVD-RSA		
	MSE	PSNR(dB)	NCC	MSE	PSNR(dB)	NCC	MSE	PSNR(dB)	NCC	MSE	PSNR(dB)	NCC
Salt and Pepper Noise(Density=0.05)	0.012	67.355	0.98	0.01	68.201	0.983	1.70E-03	75.948	0.997	0.015	66.508	0.976
Rotation(Angle in degree= 45)	0.017	65.855	0.972	0.012	67.411	0.98	0.001	78.119	0.998	0.01	68.095	0.983
Crop	0.014	66.712	0.977	0.009	68.436	0.984	0.0022	74.74	0.996	0.02	65.117	0.966
Gaussian Noise (Variance=0.05)	0.016	66.225	0.974	0.011	67.543	0.981	0.002	75.066	0.997	0.008	69.01	0.986
Speckle Noise(Variance=0.05)	0.014	66.627	0.976	0.01	68.324	0.984	0.0026	74.012	0.996	0.02	65.121	0.966
Mean	0.014	66.633	0.976	0.009	68.441	0.984	4.85E-04	81.277	0.999	0.027	63.898	0.956
Median	0.015	66.277	0.974	0.009	68.429	0.984	0.0018	75.621	0.997	0.025	64.102	0.958

Table 4.27 gives the comparison of the different similarity measures, MSE, PSNR and NCC obtained while extracting the watermark images as shown in Figure 4.17.

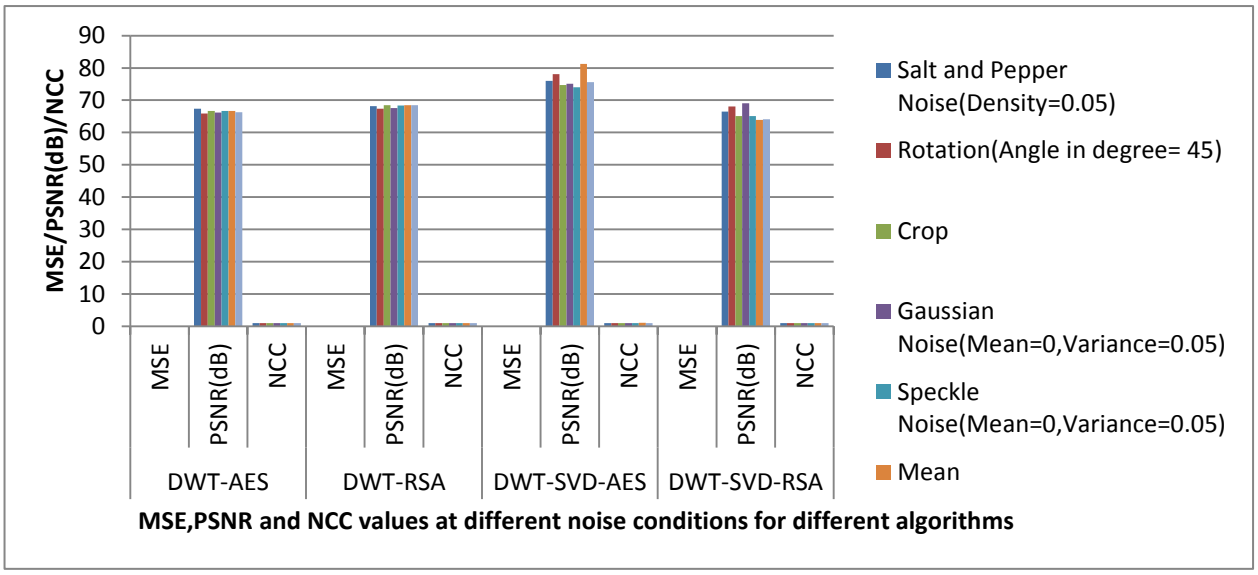


Figure 4.18: Bar Diagram for the results of Table 4.27

Figure 4.18 is the bar diagram representing the values of Table 4.27. We can see from the bar diagram that, the extracted watermark from the encrypted watermarked image subjected to various attacks, is robust and of good quality when DWT-SVD-AES algorithm is used. The PSNR value is in the range of 75 dB and value of NCC is nearly equal to 1. In the case of

watermark embedded using alpha-blending in DWT domain, DWT-RSA and DWT-AES algorithms are giving similar results.

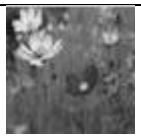
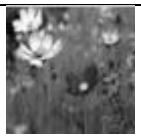
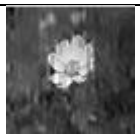
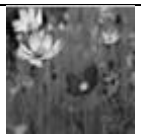
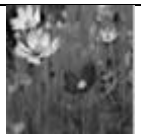
4.4 EXPERIMENTAL ANALYSIS ON REAL IMAGE

Cover Image		Watermark Image	

Figure 4.19: Real Image as Cover and Watermark Images

Example 1

Table 4.28: Comparison of Watermarked Image and Extracted Watermark using different algorithms

Algorithms	Cover Image	Watermark Image	Watermarked Image	PSNR(dB)	Extracted Watermark	NCC
DWT-AES				136.4321		0.9755
DWT-RSA				136.4321		0.9844
DWT-SVD-AES				82.4527		1
DWT-SVD-RSA				82.4527		1

Comparing the similarity measures MSE and PSNR of the Table 4.28 above, we can see that after embedding the watermark image in the cover image, the obtained watermarked image is more imperceptible using DWT transform algorithm than DWT-SVD transform algorithms. Here, the PSNR value for DWT transform algorithms is 136 dB whereas for DWT-SVD is 82 dB. Evaluating the extracted watermark, it is more robust using DWT-SVD-AES and DWT-

SVD-RSA algorithms than DWT-AES and DWT-RSA algorithms. NCC gives the robustness measure between the extracted watermark image and the original watermark image and using DWT-SVD algorithm the NCC value obtained is equal to 1.

Extracted Watermark from Encrypted Watermarked Image subjected to various attacks:

Table 4.29: Extracted Watermarks at different attack conditions using different algorithms

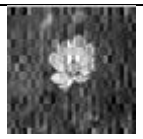
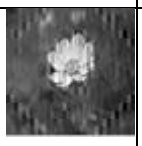
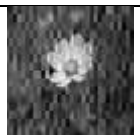
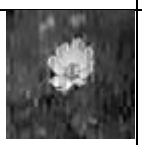
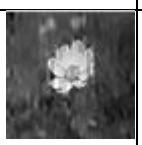
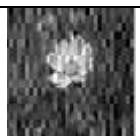
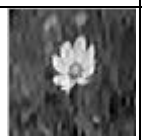
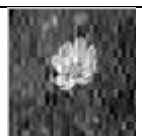
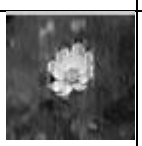
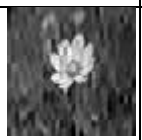
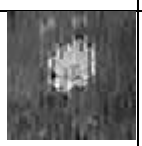
Attacks	DWT-AES	NCC	DWT-RSA	NCC	DWT-SVD-AES	NCC	DWT-SVD-RSA	NCC
Salt and Pepper Noise (Density=0.05)		0.9667		0.9807		0.9811		0.9856
Rotation(Angle in degree= 45)		0.9382		0.9739		0.9738		0.9943
Crop		0.9463		0.9864		0.9822		0.9767
Gaussian Noise (Variance=0.05)		0.9506		0.9811		0.9805		0.9892
Speckle Noise (Variance=0.05)		0.9504		0.9845		0.9841		0.9779
Mean		0.9196		0.9883		0.9839		0.9076
Median		0.955		0.9878		0.9778		0.9317

Table 4.29 shows the extracted watermark images from encrypted watermarked image under various attack conditions.

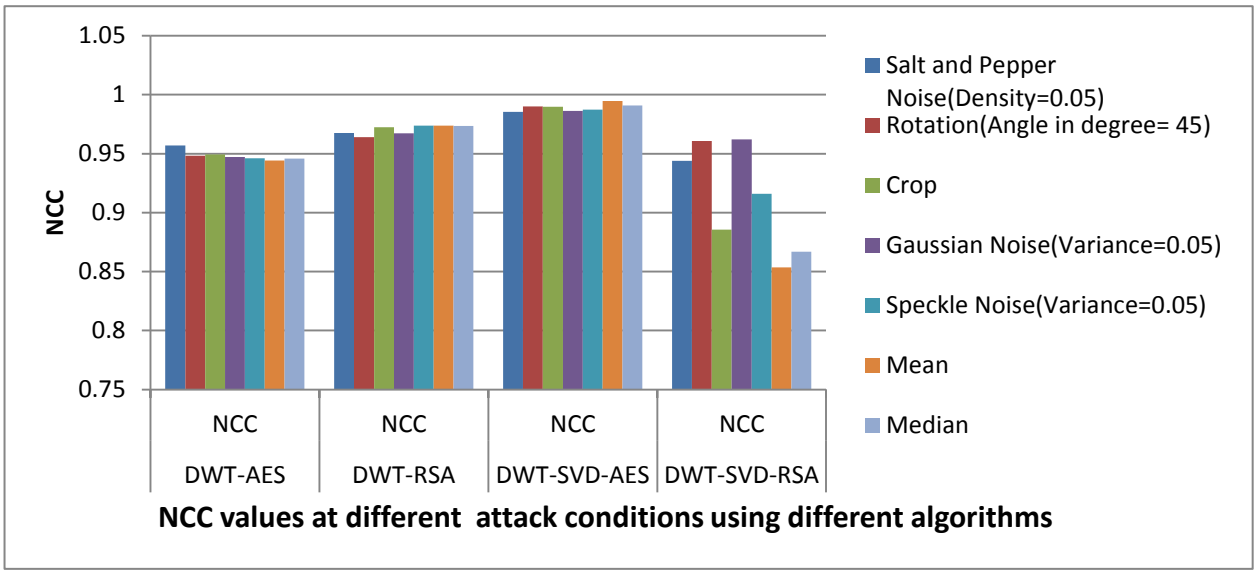


Figure 4.20: Bar Diagram for the results of Table 4.29

Figure 4.20 is the bar diagram representing the values of Table 4.29. We can see from the bar diagram that, the extracted watermark from the encrypted watermarked image subjected to various attacks, is robust and of good quality when DWT-SVD-AES and DWT-RSA algorithms are used. The value of NCC is nearly equal to 1.

4.5 DISCUSSION

Watermarking is a process done to protect our image and to claim copyright in the case of image authentication process. Watermarking can be done in spatial and transform domain. In this study, transform domain techniques are considered. The watermarking done in transform domain is more robust than in spatial domain. The algorithms in [1],[7],[10],[12] and [14] are studied in this thesis and implemented.

Here, watermarking is done using 2-level Haar transform for discrete wavelet transform. HL sub-band has been used to embed watermark and generate robust extracted watermark image as seen from the analytical result of Table 4.2. The watermarking results are calculated using MSE, PSNR and NCC parameters. The watermarking done using the combination of discrete wavelet transform and singular value decomposition gives better result than the watermark embedded in the transform domain using only discrete wavelet transform as seen from the study above. The study shows that the images watermarked in transform domain using DWT and DWT-SVD

techniques give robust watermark image when extracted. The watermarked images are further encrypted for security purpose. The encryption is done using AES for symmetric key encryption and RSA for asymmetric key encryption respectively using both DWT and DWT-SVD techniques. Here, a dual security approach using watermarking and encryption is studied and implemented. For AES, 128-bit key has been used as symmetric key and the rounds used for encryption are 10 rounds. For RSA algorithm, the key used for testing depends on the prime numbers we input.

In the experiments, image dimension of 64*64 has been considered so that the embedding and extraction of watermark can be done faster using the encryption algorithms. But, this method can be applicable to other image dimension also i.e., 128*128,256*256. Various attacks like noise attack – Salt and Pepper noise, Gaussian noise and Speckle noise, Rotation attack, Crop attack, Mean attack and Median attacks are done on the encrypted watermarked images. Then the robustness of the extracted watermark from the attacked image is evaluated using Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR) and Normalized Cross Correlation (NCC) metrics. In the algorithms used, the watermark embedded using 2-level DWT technique give better imperceptibility value for the watermarked image whereas for robustness of the extracted watermark image DWT-SVD-AES algorithm gives the best result among the four algorithms used and DWT-RSA algorithm gives better result when using DWT technique for watermark insertion. Experiment on a real image has been implemented to check whether the same result is obtained as for standard test images. In real image also, DWT-SVD-AES algorithm gave the best result among the four algorithms implemented.

CHAPTER 5

CONCLUSION AND RECOMMENDATION

5. CONCLUSION AND RECOMMENDATION

5.1 CONCLUSION

Watermarking is a process done to protect our image and to claim copyright in the case of image authentication process. Watermarking can be done in spatial and transform domain. In this study, transform domain techniques are considered since the watermarking done in transform domain is more robust than in spatial domain as seen from the study of various papers. The encryption is done using AES for symmetric key encryption and RSA for asymmetric key encryption respectively. Here, a dual security approach using watermarking and encryption is studied and implemented.

In this thesis, robustness performance evaluation of DWT and DWT-SVD techniques with AES and RSA encryption algorithms for watermarked images are examined by conducting experiments on various images. The study shows that the watermarked images can be further secured by using encryption algorithms. The result of the algorithms shows that this dual security approach of watermarking and encryption is capable of providing high robustness and imperceptibility while maintaining the structural integrity of the images. PSNR achieved by our method is higher than 45 dB and NCC value is nearly equal to 1. The results show that the techniques can resist different noise attacks and other implemented attacks.

Moreover it is also reflected from the tabulated values that, this system is capable to maintain the MSE, PSNR and NCC values for the good quality watermark image extraction, and hence leads to a clear indication of the high robustness against the different attacks.

5.2 LIMITATIONS

There are many transform domain algorithms and encryption algorithms. Among those only DWT and SVD techniques have been used for watermarking images in transform domain and AES and RSA algorithms have been used for watermarked image encryption in this thesis. The key used for AES algorithm is 128-bit.

Also, in this thesis, the observation models cover only Gaussian, Speckle and Salt and Pepper noise and Crop, Rotation, Mean and Median attacks. So, robustness measure has only been calculated for these noise additions and attacks.

5.3 RECOMMENDATION

In this thesis, comparative study is done using two transform domain techniques and encryption algorithms. These algorithms can be compared with other transform domain watermarking algorithms and encryption algorithms to do a better performance study. The encryption algorithms used in this thesis have only been checked for certain length of encryption keys. The algorithms can be checked for varying key lengths to determine which is better for secure watermarked image encryption. These algorithms can be further studied for other different type of noise and attack methods.

Further enhancement of this work can be done by combining these transform domain algorithms with other encryption algorithms and can be tested to find if there can be further improvements on the robustness of watermarking methods.

In this thesis, only grayscale images have been used as cover and watermark images. This method can also be applied and tested for color images, text, audio, video and other medias.

REFERENCES

[1] N. K. G.R., "Image Watermarking Using 2-Level DWT," *Advances in Computational Research*, 2012.

[2] G. a. Sinha, "Image Watermarking using 3-level Discrete Wavelet Transform(DWT)," *I.J.Modern Education and Computer Science*, 2012.

[3] A. K. Satendra Kumar, "SVD based Robust Digital Image Watermarking using Discrete Wavelet Transform," *International Journal of Computer Applications*, 2012.

[4] A. J. Anusudha, "Robust watermarking based on DWT SVD," *International Journal of Signal & Image Processing*, p. 2013.

[5] R. K. Singh, "A Survey: Digital Image Watermarking Techniques. International Journal of Signal Processing," *Image Processing and Pattern Recognition*, 2014.

[6] Cyril Prasanna Raj, Y. Manjula & M.Z. Kurian Santhosh Kumar R, "FPGA Implementation of a DWT and AES Processor for secure Image Coding," *nternational Journal of Electrical and Electronics Engineering (IJEEE)*, 2012.

[7] A. & Suresh,N. Joshy, "A Dual Security Approach for Image Watermarking using AES and DWT," *International Journal of Digital Application & Contemporary research*, 2014.

[8] R.V., Mahalakshmi, R. Rani, "DWT-AES based Information Security System for unmanned vehicles," *American Journal of Engineering Research*, 2014.

[9] A. S. K. Singh, "Digital Watermarking using Asymmetric Key Cryptography and Spatial Domain Technique," *International Journal of Advance Research in Spatial Domain Technique*, 2014.

[10] P. Padmaja E. Yuva Kumar, "RSA Based Secured Image Steganography Using DWT Approach," *International Journal of Engineering Research and Applications*, 2014.

[11] S.,Kamal,L. Varghese, "Enhanced RSA Combined with DWT Domain Watermarking," *International Journal of Modern Engineering Research*, 2012.

[12] M.,Soni, J. Dhanka, "Robustness Analysis of DWT-SVD with AES Encryption Based Highly Secure Image Data Hiding System via Various Attacks," *International Journal of Computer Science and Mobile Computing*, 2015.

[13] S., Hajjaji, A.A., Abdellatif,M. Ajili, "Hybrid SVD- DWT watermarking technique using AES algorithm for medical image safe transfer," in *16th international conference on Sciences and Techniques of Automatic control*, 2015.

[14] Siddaiah.P V. G. Reddy, "A Dual Security Approach for Medical Images using Encryption and Watermarking Optimized by Differential Evolution Algorithm," *International Journal of Emerging Technologies in Computational and Applied Sciences*, 2015.

[15] M. E. Y. Lakrissi, "A Joint Encryption/Water marking Algorithm for Secure Image Transfer," *International Journal of Computer Networking and Communication*, 2013.

APPENDIX A

Dataset:

Cover Image:

a. The USC-SIPI Image Database - http://sipi.usc.edu/database/

b. Kodak Lossless True Color Image Suite - http://r0k.us/graphics/kodak/

c. Image Processing Place –

http://www.imageprocessingplace.com/root_files_V3/image_databases.htm

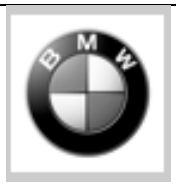
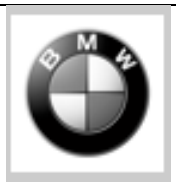
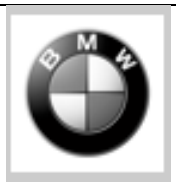
Watermark Image:

a. Flickr Logos – http://image.ntua.gr/iva/datasets/flickr_logos/

APPENDIX B

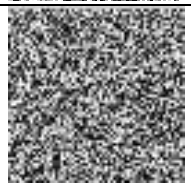
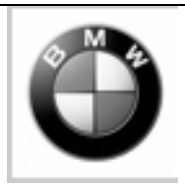
Test Image 1:

Table B.1: Comparison of similarity measure of Watermarked Image with the Cover Image using different algorithms

Algorithms	Cover Image	Watermark Image	Watermarked Image	MSE	PSNR(dB)
DWT-AES				5.8406e-09	130.4662
DWT-RSA				5.8406e-09	130.4662
DWT-SVD-AES				0.0015	76.4868
DWT-SVD-RSA				0.0015	76.4868

From the Table B.1, comparing the similarity measures MSE and PSNR, we can see that after embedding the watermark image in the cover image, the obtained watermarked image is more imperceptible using DWT transform algorithm than DWT-SVD transform algorithms. PSNR gives the imperceptibility measure between the watermarked image and the original cover image. Here, the PSNR value for DWT transform algorithms is 130 dB whereas for DWT-SVD is 76.4 dB.

Table B.2: Comparison of similarity measure of Extracted Watermark with the Original Watermark using different algorithms

Algorithms	Watermarked Image	Encrypted Watermarked image	Extracted Watermark	MSE	PSNR(dB)	NCC
DWT-AES				0.0078	69.2137	0.9874
DWT-RSA				0.0068	69.7791	0.9889
DWT-SVD-AES				5.4228e-06	100.7886	1
DWT-SVD-RSA				5.4228e-06	100.7886	1

From the Table B.2, we can see that after embedding the watermark image in the cover image, the obtained watermarked image is more robust using DWT-SVD-AES and DWT-SVD-RSA algorithms than DWT-AES and DWT-RSA algorithms. NCC gives the robustness measure between the extracted watermark image and the original watermark image and using DWT-SVD algorithm the NCC value obtained is equal to 1. Using DWT algorithm also, the obtained value of NCC is equal to 0.97. So both algorithms in DWT only and DWT-SVD domain give good results in case of the watermark extracted from the encrypted watermarked image not subjected to any attacks.

Extracted Watermark from Encrypted Watermarked Image subjected to Salt and Pepper Noise:

Attacks	DWT-AES	DWT-RSA	DWT-SVD-AES	DWT-SVD-RSA
Salt and Pepper Noise(Density=0.1)				
Salt and Pepper Noise(Density=0.5)				
Salt and Pepper Noise(Density=0.01)				
Salt and Pepper Noise(Density=0.09)				

Figure B.1: Extracted Watermarks at different noise conditions using different algorithms

Figure B.1 shows the extracted watermark images from encrypted watermarked image under various densities of salt and pepper noise conditions.

Table B.3: Comparison of similarity measures of Extracted Watermark with the Original Watermark at different salt and pepper noise conditions using different algorithms

Attacks	**DWT-AES**			**DWT-RSA**			**DWT-SVD-AES**			**DWT-SVD-RSA**		
	MSE	**PSNR(dB)**	**NCC**	**MSE**	**PSNR(dB)**	**NCC**	**MSE**	**PSNR(dB)**	**NCC**	**MSE**	**PSNR(dB)**	**NCC**
Salt and Pepper Noise (Density=0.1)	0.0112	67.6558	0.982	0.0076	69.3293	0.9877	0.003	73.3798	0.9952	0.0047	71.3844	0.9923
Salt and Pepper Noise (Density=0.5)	0.0112	67.654	0.982	0.013	67.0017	0.9791	0.0024	74.2467	0.996	0.002	75.1886	0.9968
Salt and Pepper Noise (Density=0.01)	0.0085	68.8609	0.9863	0.0066	69.9534	0.9893	0.003	73.4179	0.9952	0.0075	69.3618	0.9878
Salt and Pepper Noise (Density=0.09)	0.0095	68.3464	0.9846	0.0076	69.3226	0.9877	0.0025	74.2229	0.996	0.0035	72.7368	0.9944

Table B.3 gives the comparison of the different similarity measures, MSE, PSNR and NCC obtained while extracting the watermark images as shown in Figure B.1.

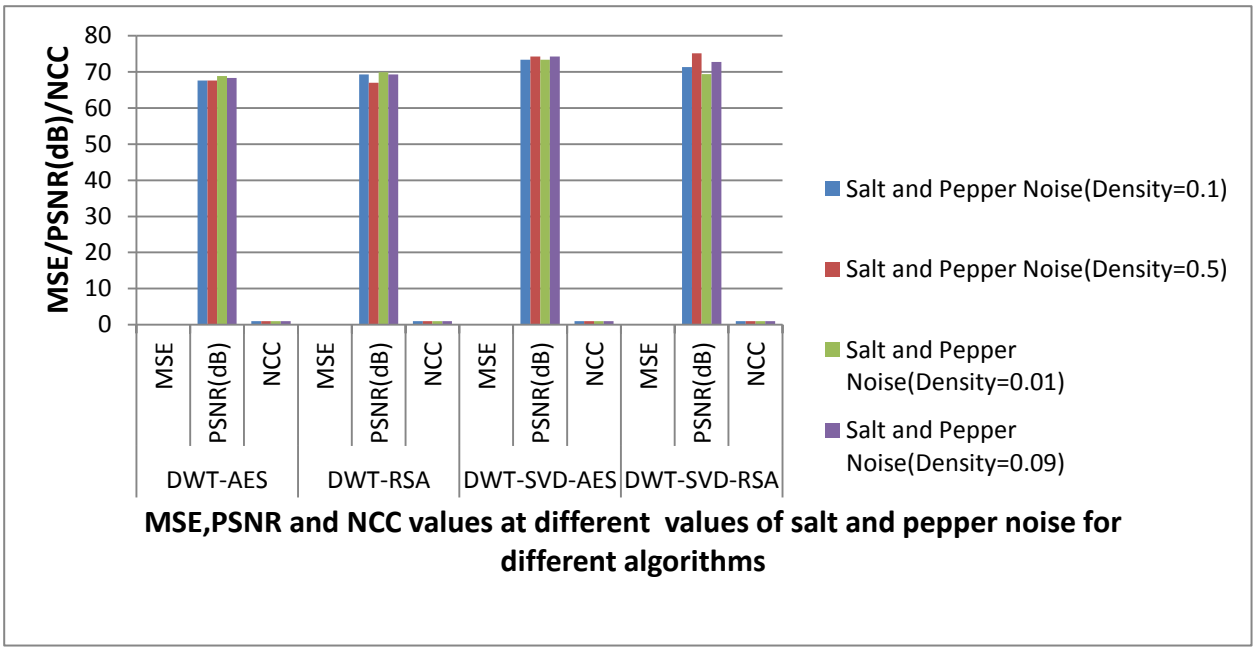


Figure B.2: Bar Diagram for the results of Table B.3

Figure B.2 is the bar diagram representing the values of Table B.3. We can see from the bar diagram that, the extracted watermark from the encrypted watermarked image subjected to various attacks, is robust and of good quality when DWT-SVD-AES and DWT-SVD-RSA algorithms are used. The PSNR value is in the range of 73 dB and value of NCC is nearly equal to 1. In the case of watermark embedded using DWT algorithm, DWT-AES and DWT-RSA algorithms are giving similar results.

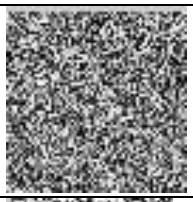
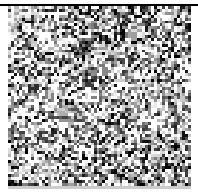
Test Image 2:

Table B.4: Comparison of similarity measure of Watermarked Image with the Cover Image using different algorithms

Algorithms	Cover Image	Watermark Image	Watermarked Image	MSE	PSNR(dB)
DWT-AES				1.5948e-09	136.1038
DWT-RSA				1.5948e-09	136.1038
DWT-SVD-AES				3.9869e-04	82.1244
DWT-SVD-RSA				3.9869e-04	82.1244

From the Table B.4, comparing the similarity measures MSE and PSNR, we can see that after embedding the watermark image in the cover image, the obtained watermarked image is more imperceptible using DWT transform algorithm than DWT-SVD transform algorithms. PSNR gives the imperceptibility measure between the watermarked image and the original cover image. Here, the PSNR value for DWT transform algorithms is 136 dB whereas for DWT-SVD is 82 dB.

Table B.5: Comparison of similarity measure of Extracted Watermark with the Original Watermark using different algorithms

Algorithms	Watermarked Image	Encrypted Watermarked image	Extracted Watermark	MSE	PSNR(dB)	NCC
DWT-AES				0.0024	74.3345	0.9973
DWT-RSA				0.0024	74.2804	0.9972
DWT-SVD-AES				1.0347e-05	97.9825	1
DWT-SVD-RSA				1.0347e-05	97.9825	1

From Table B.5, we can see that after embedding the watermark image in the cover image, the obtained watermarked image is more robust using DWT-SVD-AES and DWT-SVD-RSA algorithms than DWT-AES and DWT-RSA algorithms. NCC gives the robustness measure between the extracted watermark image and the original watermark image and using DWT-SVD algorithm the NCC value obtained is equal to 1. Using DWT algorithm also, the obtained value of NCC is nearly equal to 1. So both algorithms in DWT only and DWT-SVD domain give good results in case of the watermark extracted from the encrypted watermarked image not subjected to any attacks.

Extracted Watermark from Encrypted Watermarked Image subjected to Gaussian Noise:

Attacks	DWT-AES	DWT-RSA	DWT-SVD-AES	DWT-SVD-RSA
Gaussian Noise (Variance=0.1)				
Gaussian Noise (Variance=0.5)				
Gaussian Noise (Variance=0.01)				
Gaussian Noise (Variance=0.08)				

Figure B.3: Extracted Watermarks at different Gaussian noise conditions using different algorithms

Figure B.3 shows the extracted watermark images from encrypted watermarked image under different variance value of Gaussian noise conditions.

Table B.6: Comparison of similarity measures of Extracted Watermark with the Original Watermark at different Gaussian noise conditions using different algorithms

Attacks	DWT-AES			DWT-RSA			DWT-SVD-AES			DWT-SVD-RSA		
	MSE	PSNR(dB)	NCC	MSE	PSNR(dB)	NCC	MSE	PSNR(dB)	NCC	MSE	PSNR(dB)	NCC
Gaussian Noise (Variance=0.1)	0.0064	70.0824	0.9928	0.002	75.1163	0.9977	0.0038	72.3234	0.9957	0.00094	78.3957	0.9989
Gaussian Noise (Variance=0.5)	0.0067	69.8833	0.9924	0.0038	72.3487	0.9957	0.0056	70.684	0.9937	0.0033	72.9643	0.9963
Gaussian Noise (Variance=0.01)	0.0068	69.7786	0.9922	0.0021	74.8644	0.9976	0.0056	70.6733	0.9937	0.001	77.9863	0.9988
Gaussian Noise (Variance=0.08)	0.007	69.6727	0.992	0.0021	75.0036	0.9977	0.0063	70.1206	0.9929	0.001	78.013	0.9988

Table B.6 gives the comparison of the different similarity measures, MSE, PSNR and NCC obtained while extracting the watermark images as shown in Figure B.3.

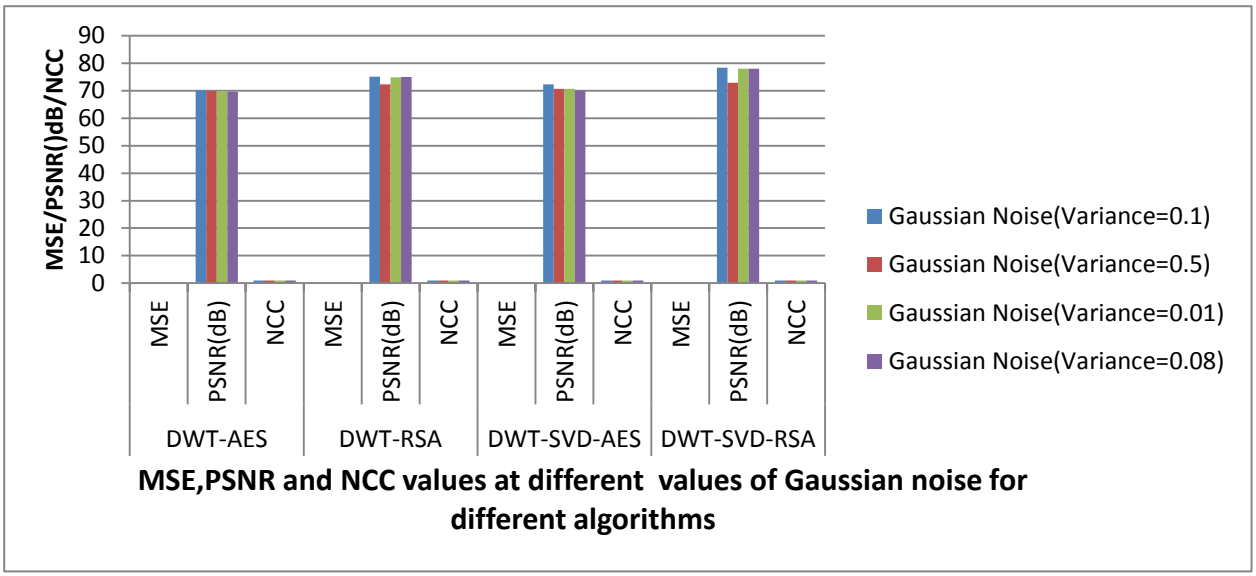
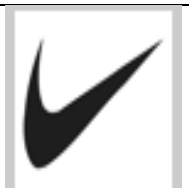
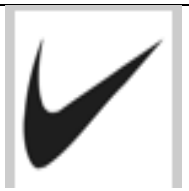
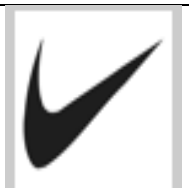
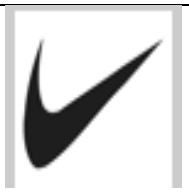


Figure B.4: Bar Diagram for the results of Table B.6

Figure B.4 is the bar diagram representing the values of Table B.6. We can see from the bar diagram that, the extracted watermark from the encrypted watermarked image subjected to Gaussian noise attacks, is robust and of good quality when DWT-SVD-RSA algorithm is used. The PSNR value is in the range of 77 dB and value of NCC is nearly equal to 1. DWT-RSA and DWT-SVD-AES algorithms show similar result.

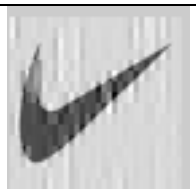
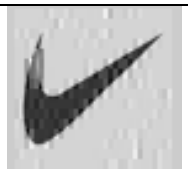
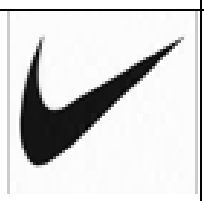
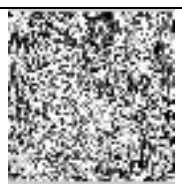
Test Image 3:

Table B.7: Comparison of similarity measure of Watermarked Image with the Cover Image using different algorithms

Algorithms	Cover Image	Watermark Image	Watermarked Image	MSE	PSNR(dB)
DWT-AES				5.3056e-09	130.8834
DWT-RSA				5.3056e-09	130.8834
DWT-SVD-AES				0.0013	76.9040
DWT-SVD-RSA				0.0013	76.9040

From the Table B.7, comparing the similarity measures MSE and PSNR, we can see that after embedding the watermark image in the cover image, the obtained watermarked image is more imperceptible using DWT transform algorithm than DWT-SVD transform algorithms. PSNR gives the imperceptibility measure between the watermarked image and the original cover image. Here, the PSNR value for DWT transform algorithms is 130 dB whereas for DWT-SVD is 76 dB.

Table B.8: Comparison of similarity measure of Extracted Watermark with the Original Watermark using different algorithms

Algorithms	Watermarked Image	Encrypted Watermarked image	Extracted Watermark	MSE	PSNR(dB)	NCC
DWT-AES				0.0091	68.5256	0.9890
DWT-RSA				0.0061	70.2945	0.9927
DWT-SVD-AES				2.2637e-05	94.5826	1
DWT-SVD-RSA				2.2637e-05	94.5826	1

From the above table, we can see that after embedding the watermark image in the cover image, the obtained watermarked image is more robust using DWT-SVD-AES and DWT-SVD-RSA algorithms than DWT-AES and DWT-RSA algorithms. NCC gives the robustness measure between the extracted watermark image and the original watermark image and using DWT-SVD algorithm the NCC value obtained is equal to 1. Using DWT algorithm also, the obtained value of NCC is nearly equal to 1. So both algorithms in DWT only and DWT-SVD domain give good results in case of the watermark extracted from the encrypted watermarked image not subjected to any attacks.

Extracted Watermark from Encrypted Watermarked Image subjected to Speckle Noise:

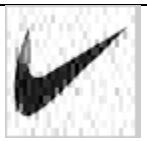
Attacks	DWT-AES	DWT-RSA	DWT-SVD-AES	DWT-SVD-RSA
Speckle Noise (Variance=0.1)				
Speckle Noise (Variance=0.5)				
Speckle Noise (Variance=0.01)				
Speckle Noise (Variance=0.08)				

Figure B.5: Extracted Watermarks at different Speckle noise conditions using different algorithms

Above figure shows the extracted watermark images from encrypted watermarked image under different variance values of speckle noise conditions.

Table B.9: Comparison of similarity measures of Extracted Watermark with the Original Watermark at different speckle noise conditions using different algorithms

Attacks	DWT-AES			DWT-RSA			DWT-SVD-AES			DWT-SVD-RSA		
	MSE	PSNR(dB)	NCC	MSE	PSNR(dB)	NCC	MSE	PSNR(dB)	NCC	MSE	PSNR(dB)	NCC
Speckle Noise (Variance=0.1)	0.0109	67.7594	0.9869	0.0059	70.4343	0.9929	0.0042	71.9201	0.995	0.0169	65.8439	0.9796
Speckle Noise (Variance=0.5)	0.0104	67.9705	0.9875	0.0077	69.2414	0.9907	0.0041	72.0011	0.995	0.0078	69.2219	0.9906
Speckle Noise (Variance=0.01)	0.0092	68.51	0.989	0.0059	70.4284	0.9929	0.0052	70.9763	0.9937	0.0167	65.9154	0.98
Speckle Noise (Variance=0.08)	0.011	67.7043	0.9867	0.0059	70.4322	0.9929	0.0058	70.5134	0.993	0.0167	65.9108	0.9799

Table B.9 gives the comparison of the different similarity measures, MSE, PSNR and NCC obtained while extracting the watermark images as shown in Figure B.5.

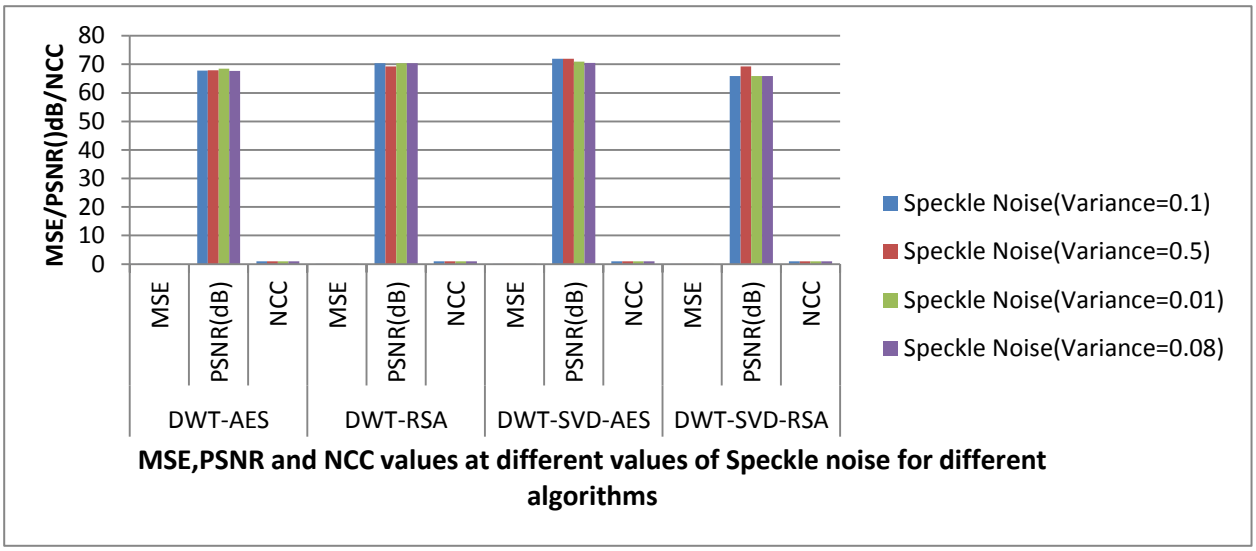


Figure B.6: Bar Diagram for the results of Table B.9

Figure B.6 is the bar diagram representing the values of Table B.9. We can see from the bar diagram that, the extracted watermark from the encrypted watermarked image subjected to speckle noise of various values, is robust and of good quality when DWT-RSA and DWT-SVD-AES algorithms are used. The PSNR value is in the range of 70 dB and value of NCC is nearly equal to 1. DWT-AES and DWT-SVD-RSA algorithms show similar result.

Test Image 4:

Table B.10: Comparison of similarity measure of Watermarked Image with the Cover Image using different algorithms

Algorithms	Cover Image	Watermark Image	Watermarked Image	MSE	PSNR(dB)
DWT-AES				1.8264e-09	135.5148
DWT-RSA				1.8264e-09	135.5148
DWT-SVD-AES				4.5661e-04	81.5354
DWT-SVD-RSA				4.5661e-04	81.5354

From the table B.10, comparing the similarity measures MSE and PSNR, we can see that after embedding the watermark image in the cover image, the obtained watermarked image is more imperceptible using DWT transform algorithm than DWT-SVD transform algorithms. PSNR gives the imperceptibility measure between the watermarked image and the original cover image. Here, the PSNR value for DWT transform algorithms is 135 dB whereas for DWT-SVD is 81 dB.

Table B.11: Comparison of similarity measure of Extracted Watermark with the Original Watermark using different algorithms

Watermarked Image	Encrypted Watermarked image	Extracted Watermark	MSE	PSNR(dB)	NCC
			0.0027	73.8927	0.9955
			0.0026	73.9751	0.9956
			4.8181e-06	101.3020	1
			4.8181e-06	101.3020	1

From Table B.11, we can see that after embedding the watermark image in the cover image, the obtained watermarked image is more robust using DWT-SVD-AES and DWT-SVD-RSA algorithms than DWT-AES and DWT-RSA algorithms. NCC gives the robustness measure between the extracted watermark image and the original watermark image and using DWT-SVD algorithm the NCC value obtained is equal to 1. Using DWT algorithm also, the obtained value of NCC is nearly equal to 1. So both algorithms in DWT domain and DWT-SVD domain give good results in case of the watermark extracted from the encrypted watermarked image not subjected to any attacks.

Extracted Watermark from Encrypted Watermarked Image subjected to Rotation attack:

Attacks	DWT-AES	DWT-RSA	DWT-SVD-AES	DWT-SVD-RSA
Rotation(Angle in degree= 5)				
Rotation(Angle in degree= 90)				
Rotation(Angle in degree= 135)				
Rotation(Angle in degree= 180)				

Figure B.7: Extracted Watermarks at different Rotation angles using different algorithms

Figure B.7 shows the extracted watermark images from encrypted watermarked image under various rotation angles.

Table B.12: Comparison of similarity measures of Extracted Watermark with the Original Watermark at different rotation angles using different algorithms

Attacks	**DWT-AES**			**DWT-RSA**			**DWT-SVD-AES**			**DWT-SVD-RSA**		
	MSE	**PSNR(dB)**	**NCC**	**MSE**	**PSNR(dB)**	**NCC**	**MSE**	**PSNR(dB)**	**NCC**	**MSE**	**PSNR(dB)**	**NCC**
Rotation (Angle in degree=5)	0.0085	68.8338	0.986	0.0054	70.8147	0.991	0.0047	71.4216	0.9921	0.0007	79.5223	0.9988
Rotation (Angle in degree=90)	0.0079	69.1575	0.987	0.0024	74.4109	0.996	0.004	72.1415	0.9933	0.0033	72.9313	0.9944
Rotation (Angle in degree=135)	0.0086	68.7623	0.986	0.0037	72.3913	0.994	0.006	70.3673	0.99	0.001	77.9306	0.9982
Rotation (Angle in degree=180)	0.0071	69.6279	0.988	0.0021	74.9758	0.997	0.0053	70.902	0.9911	0.0029	73.4742	0.995

Table B.12 gives the comparison of the different similarity measures, MSE, PSNR and NCC obtained while extracting the watermark images as shown in Figure B.7.

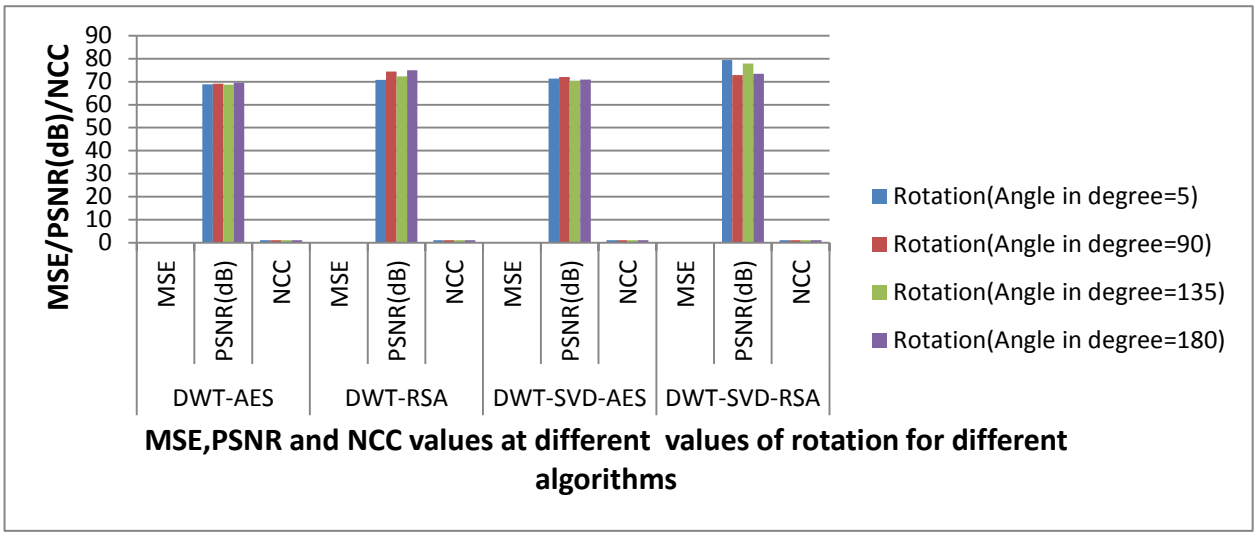


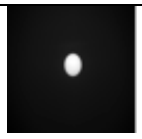
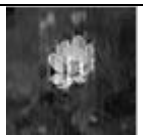
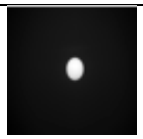
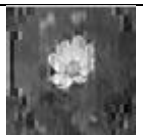
Figure B.8: Bar Diagram for the results of Table B.12

Figure B.8 is the bar diagram representing the values of Table B.12. We can see from the bar diagram that, the extracted watermark from the encrypted watermarked image subjected to rotation at various angles, is robust and of good quality when DWT-SVD-RSA algorithm is used. The PSNR value is in the range of 73 dB and value of NCC is nearly equal to 1. DWT-SVD-AES and DWT-SVD-RSA algorithms show similar results.

APPENDIX C

Test Image 1 (real image):

Table C.1: Comparison of Watermarked Image and Extracted Watermark using different algorithms

Algorithms	Cover Image	Watermark Image	Watermarked Image	PSNR(dB)	Extracted Watermark	NCC
DWT-AES				136.4321		0.9822
DWT-RSA				136.4321		0.9647
DWT-SVD-AES				82.4527		0.9999
DWT-SVD-RSA				82.4527		0.9999

Comparing the similarity measures MSE and PSNR of the Table C.1 above, we can see that after embedding the watermark image in the cover image, the obtained watermarked image is imperceptible using DWT transform algorithm than DWT-SVD transform algorithms. Here, the PSNR value for DWT transform algorithms is 136 dB whereas for DWT-SVD is 82 dB. Evaluating the extracted watermark, it is more robust using DWT-SVD-AES and DWT-SVD-RSA algorithms than DWT-AES and DWT-RSA algorithms. NCC gives the robustness measure between the extracted watermark image and the original watermark image and using DWT-SVD algorithm the NCC value obtained is equal to 0.999.

Extracted Watermark from Encrypted Watermarked Image subjected to various attacks:

Table C.2: Extracted Watermarks at different attack conditions using different algorithms

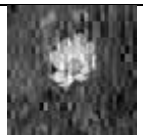
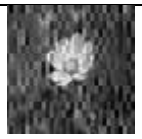
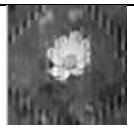
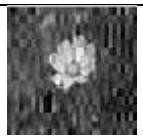
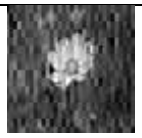
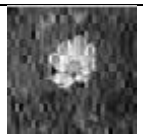
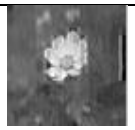
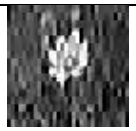
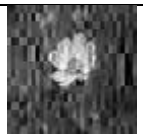
Attacks	DWT-AES	NCC	DWT-RSA	NCC	DWT-SVD-AES	NCC	DWT-SVD-RSA	NCC
Salt and Pepper Noise (Density=0.05)		0.9535		0.9611		0.9123		0.9049
Rotation(Angle in degree= 45)		0.9347		0.9705		0.9320		0.9509
Crop		0.9419		0.9541		0.9266		0.8921
Gaussian Noise (Variance=0.04)		0.9449		0.9545		0.9316		0.8725
Speckle Noise (Variance=0.03)		0.9489		0.9638		0.9318		0.8969
Mean		0.9239		0.9796		0.8882		0.9937
Median		0.9374		0.9417		0.9261		0.9828

Table C.2: shows the extracted watermark images from encrypted watermarked image under various attack conditions.

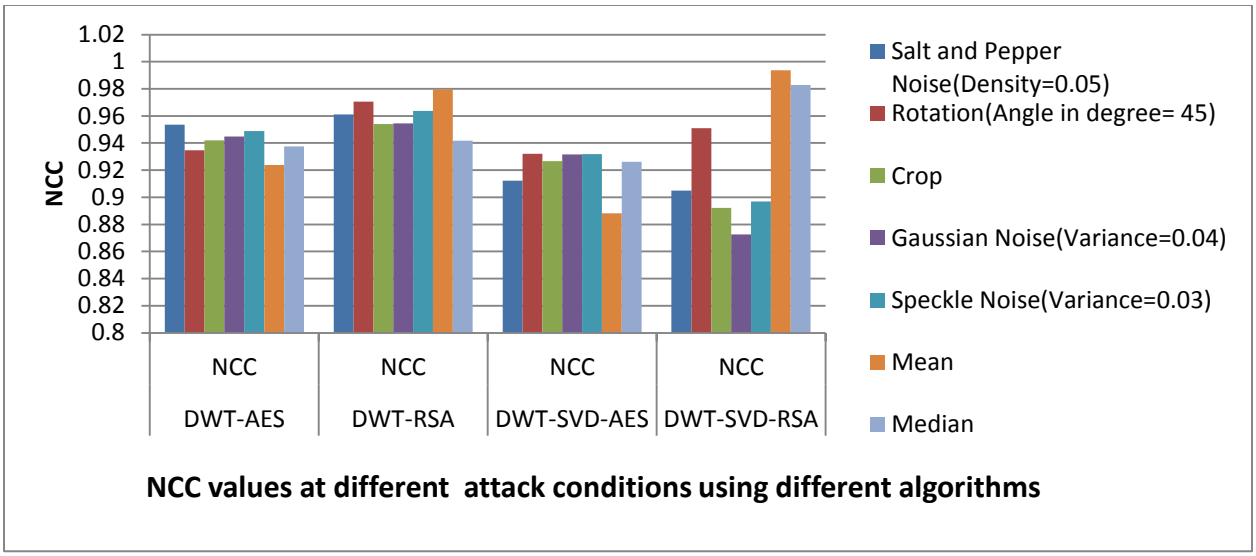
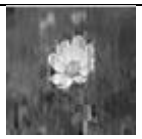


Figure C.2: Bar Diagram for the results of Table C.2

Figure C.2 is the bar diagram representing the values of Table C.2. We can see from the bar diagram that, the extracted watermark from the encrypted watermarked image subjected to various attacks, is robust and of good quality when DWT-RSA algorithm is used. The value of NCC is nearly equal to 0.95 in average.

Test Image 2 (real image):

Table C.3: Comparison of Watermarked Image and Extracted Watermark using different algorithms

Algorithms	Cover Image	Watermark Image	Watermarked Image	PSNR(dB)	Extracted Watermark	NCC
DWT-AES				136.4321		0.9817
DWT-RSA				136.4321		0.9866
DWT-SVD-AES				82.4527		1
DWT-SVD-RSA				82.4527		1

Comparing the similarity measures MSE and PSNR of the Table C.3 above, we can see that after embedding the watermark image in the cover image, the obtained watermarked image is more imperceptible using DWT transform algorithm than DWT-SVD transform algorithms. Here, the PSNR value for DWT transform algorithms is 136 dB whereas for DWT-SVD is 82 dB. Evaluating the extracted watermark, it is more robust using DWT-SVD-AES and DWT-SVD-RSA algorithms than DWT-AES and DWT-RSA algorithms. NCC gives the robustness measure between the extracted watermark image and the original watermark image and using DWT-SVD algorithm the NCC value obtained is equal to 1.

Extracted Watermark from Encrypted Watermarked Image subjected to various attacks:

Table C.4: Extracted Watermarks at different attack conditions using different algorithms

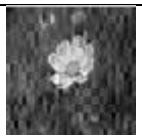
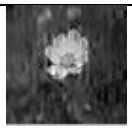
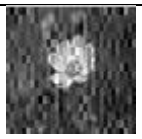
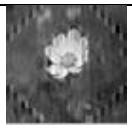
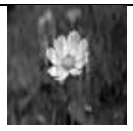
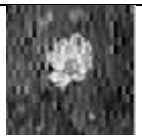
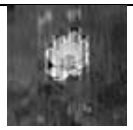
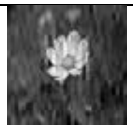
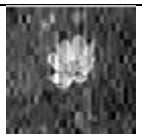
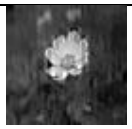
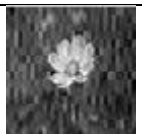
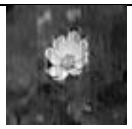
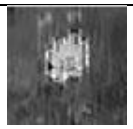
Attacks	DWT-AES	NCC	DWT-RSA	NCC	DWT-SVD-AES	NCC	DWT-SVD-RSA	NCC
Salt and Pepper Noise (Density=0.05)		0.9656		0.9813		0.9515		0.9887
Rotation(Angle in degree= 45)		0.9311		0.9761		0.9516		0.9923
Crop		0.9426		0.9868		0.9641		0.9676
Gaussian Noise (Variance=0.04)		0.9470		0.9853		0.9650		0.9867
Speckle Noise (Variance=0.03)		0.9415		0.9864		0.9615		0.9807
Mean		0.9346		0.9883		0.9408		0.9261
Median		0.9603		0.9880		0.9717		0.9447

Table C.4 shows the extracted watermark images from encrypted watermarked image under various attack conditions.

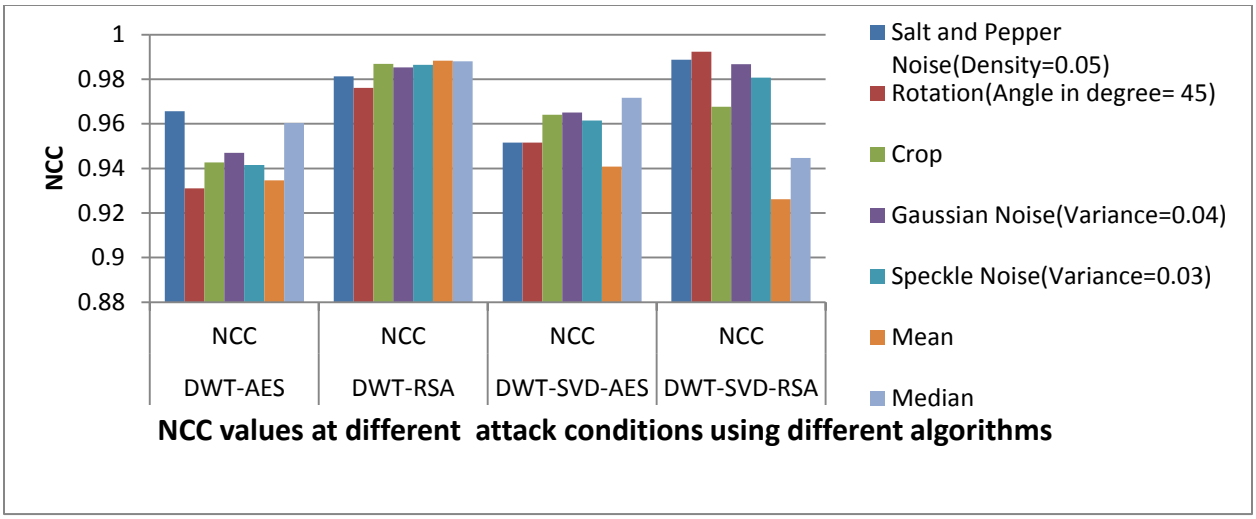


Figure C.2: Bar Diagram for the results of Table C.4

Figure C.2 is the bar diagram representing the values of Table C.4. We can see from the bar diagram that, overall, the extracted watermark from the encrypted watermarked image subjected to various attacks, is robust and of good quality when DWT-RSA algorithm is used. The value of NCC is 0.98 in average.