DAYANANDA SAGAR UNIVERSITY

KUDLU GATE, BANGALORE – 560068

Bachelor of Technology
in
COMPUTER SCIENCE AND ENGINEERING

Major Project Phase-II Report

HYBRID WATERMARKING TECHNIQUE FOR IMAGE AUTHENTICATION USING BIOMETRICS

By
Lalith Sagar J - ENG18CS0147
Lalith Anand S - ENG18CS0146
M Ranga Sai Ruthvik - ENG18CS0158
Kuruva Divya Sree - ENG18CS0144
Musfirah Suha - ENG18CS0176

Under the supervision of

Dr. T. Kumaresan
Associate Professor, CSE

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING,
SCHOOL OF ENGINEERING
DAYANANDA SAGAR UNIVERSITY,
BANGALORE

(2021-2022)

DAYANANDA SAGAR UNIVERSITY

School of Engineering
Department of Computer Science & Engineering
Kudlu Gate, Bangalore – 560068
Karnataka, India

CERTIFICATE

This is to certify that the Major project work titled **"HYBRID WATERMARKING TECHNIQUE FOR IMAGE AUTHENTICATION USING BIOMETRICS"** is carried out by **LALITH SAGAR J (ENG18CS0147), M R S RUTHVIK (ENG18CS0158), MUSFIRAH SUHA (ENG18CS0176), KURUVA DIVYA SREE (ENG18CS0144), LALITH ANAND (ENG18CS0146)** bonafide students of Bachelor of Technology in Computer Science and Engineering at the School of Engineering, Dayananda Sagar University, Bangalore in partial fulfilment for the award of degree in Bachelor of Technology in Computer Science and Engineering, during the year **2021-2022**.

Dr. T. Kumaresan Associate professor Dept. of CS&E, School of Engineering Dayananda Sagar University Date:	**Dr Girisha G S** Chairman CSE School of Engineering Dayananda Sagar University Date:	**Dr. A Srinivas** Dean School of Engineering Dayananda Sagar University Date:

Name of the Examiner **Signature of Examiner**

1.

2.

DECLARATION

We, **LALITH SAGAR J (ENG18CS0147), M R S RUTHVIK (ENG18CS0158), MUSFIRAH SUHA (ENG18CS0176), KURUVA DIVYA SREE (ENG18CS0144), LALITH ANAND (ENG18CS0146)** are students of the eighth semester B.Tech in **Computer Science and Engineering**, at School of Engineering, **Dayananda Sagar University**, hereby declare that the major project titled **"HYBRID WATERMARKING TECHNIQUE FOR IMAGE AUTHENTICATION USING BIOMETRICS"** has been carried out by us and submitted in partial fulfilment for the award of degree in **Bachelor of Technology in Computer Science and Engineering** during the academic year **2021-2022**.

Student	Signature
Lalith Sagar J ENG18CS0147	
M R S Ruthvik ENG18CS0158	
Musfirah Suha ENG18CS0176	
Kuruva Divya Sree ENG18CS0144	
Lalith Anand S ENG18CS0146	

Place: Bengaluru
Date:

ACKNOWLEDGEMENT

It is a great pleasure for us to acknowledge the assistance and support of many individuals who have been responsible for the successful completion of this project work.

First, we take this opportunity to express our sincere gratitude to School of Engineering & Technology, Dayananda Sagar University for providing us with a great opportunity to pursue our Bachelor's degree in this institution.

We would like to thank **Dr. A Srinivas, Dean**, **School of Engineering & Technology**, **Dayananda Sagar University** for his constant encouragement and expert advice. It is a matter of immense pleasure to express our sincere thanks to **Dr. Girisha G S, Department Chairman**, **Computer Science, and Engineering**, **Dayananda Sagar University,** for providing the right academic guidance that made our task possible.

We would like to thank our guide **Dr. T. Kumaresan**, **Associate Professor**, **Dept. of Computer Science and Engineering**, **Dayananda Sagar University**, for sparing his valuable time to extend help in every step of our project work, which paved the way for smooth progress and the fruitful culmination of the project.

We would like to thank our Project Coordinators **Dr. Meenakshi Malhotra** and **Dr. Bharanidharan N**, and all the staff members of Computer Science and Engineering for their support.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

DWT	Discrete Wavelet Transform
DCT	Discrete Cosine Transform
SVD	Singular Valued Decomposition
PSNR	Peak Signal to Noise Ratio
NCC	Normal Correlation Coefficient
SSIM	Structural Similarity Index Metric

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

In the modern era of cyberspace, protection of crucial documents is highly significant. To achieve this motto, digital watermarking with biometric features plays an important part. It uses modern technology of hiding information inside some digital media i.e. text, image, video, or audio files. The key purpose of this project is to implement the technique of hiding an image inside another image using biometric features namely signature and fingerprint using watermarking techniques. To accomplish this, a hybrid watermarking scheme consisting of Discrete Wavelet Transform, Discrete Cosine Transform and Singular Value Decomposition (DWT-DCT-SVD) is proposed for image authentication that is robust against attacks. Here, singular values of watermark1(fingerprint) and watermark2(signature) are obtained by applying DWT-DCT-SVD. By adding both the singular values of watermarks we acquire the transformed watermark. Later the same is applied to cover image to extract the singular values. Then we add the singular values of cover image and transformed watermark to obtain the final watermarked image containing both signature and fingerprint. To improve the security, robustness and provide authenticity for the image, a two-step watermarking method is demonstrated. The effectiveness of this method in terms of digital attacks has shown better experimental outcomes.

CHAPTER 1

INTRODUCTION

CHAPTER 1

INTRODUCTION

The concept of biometric watermarking is used for advanced security of biometrics. Watermarking techniques have been used in biometric systems for the purpose of protecting and authenticating biometric data and enhancing accuracy of recognition. The transform domain techniques used are DWT, DCT and SVD.

The DCT transform is mainly used to compress the data or image. DWT decomposes an image into a set of four non-overlapping multi-resolutions. The SVD of a matrix is orthogonal transforms used for matrix diagonalization. Watermarking embedding can be done with each of the above-mentioned techniques, but each one has some drawbacks with regards to some attacks. So, in order to overcome these drawbacks, we integrate all three techniques and make a hybrid system which is more robust and secure. This hybrid model withstands different image processing attacks. Thus, the final result does not change even after applying the attacks.

Therefore, we can say this technique improves the security without altering the existing image data properties to a great extent.

1.1. HYBRID DWT-DCT-SVD:

A hybrid watermarking scheme consisting of Discrete Wavelet Transform, Discrete Cosine Transform and Singular Value Decomposition (DWT-DCT-SVD) is proposed for image authentication that is robust against attacks. In the process of watermarking, two major steps viz., embedding and extraction are performed. In the embedding and extraction processes, the combinations of DWT, DCT and SVD along with their inverses are carried out. This hybrid works well for different image processing attacks by achieving the properties of watermark i.e. integrity, authenticity and confidentiality of digitized image documents. The performance comparison is done by considering the performance metrics i.e. Peak Signal to Noise Ratio (PSNR), Structural Similarity Index (SSIM) and Mean Square Error (MSE). This proposed methodology is deployed on dual watermarking where

the embedding process consists of DWT, DCT and SVD that provides image authentication and robust against attacks.

Our project depicts the embedding process that consists of DWT, DCT and SVD watermarking techniques. Here, to the cover image one level of DWT is applied. So, we have applied SVD to the LL sub-band. Besides that, we have applied DWT to the biometric and then DCT and followed by SVD. Parallelly we have applied SVD to the signature, by applying SVD to the images we obtain three matrices namely U S and V. Here we consider only the S matrix that is a singular valued matrix because it contains the diagonal properties of the image. Now we add the singular values of the biometric and alpha times singular values of the signature. Now apply inverse SVD to recreate the LL sub-hand of biometric. Later, we have applied inverse DCT as we applied DCT in the earlier steps. Now we have applied inverse DWT to create an image with a modified LL sub-band. This gives a Transformed watermark, now apply SVD to it in order to get a singular valued matrix. Now add the singular values of cover image and beta times singular matrix of transformed watermark. Now apply the inverse SVD to recreate the cover image with manipulated singular values. Then followed by applying DCT and then DWT to create an image with a modified LL sub-band. This gives a final watermarked image; this contains the signature and biometric embedded on the cover image. This completes the embedded process.

1.2. DCT:

Digital images require an enormous amount of storage capacity when they are in their uncompressed form. Large transmission bandwidth is required for such uncompressed data for the transmission over the network. Discrete Cosine Transform (DCT) is the most widely used image compression method.

DCT is used in the JPEG image compression algorithm. The input image is divided into 8-by-8 or 16-by-16 blocks, and the two-dimensional DCT is computed for each block. The DCT coefficients are then quantized, coded, and transmitted.

Discrete Cosine Transform(DCT) is used in lossy image compression because it has very strong energy compaction, i.e., its large amount of information is stored in very low frequency component of a signal and rest other frequency having very small data which

can be stored by using very less number of bits and used to reduce the redundancy between the neighbouring pixels. Here is the formula for DCT having 2D matrix,

The DCT equation (Eq. 1) computes the i,jth entry of the DCT of an image.

$$D(i,j) = \frac{1}{\sqrt{2N}} C(i)C(j) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} p(x,y) \cos\left[\frac{(2x+1)i\pi}{2N} \right] \cos\left[\frac{(2y+1)j\pi}{2N} \right]$$

$$C(u) = \begin{cases} \frac{1}{\sqrt{2}} & \text{if } u = 0 \\ 1 & \text{if } u > 0 \end{cases}$$

where,

p (x, y) is the x, yth element of the element of image represented by the matrix p. N is the size of the block that the DCT is done on. The equation calculates one entry (i, jth) of the transformed image from the pixel values of the original image matrix. For the standard 8*8 blocks that JPEG compression uses, N equals 8 and x and y range from 0 to 7.

The DCT separates images into parts of differing frequencies. The term “lossy” is in use because less important frequencies are discarded during quantization in the compression part. Next, only the remaining most important frequencies are used to retrieve the image in the decompression process. As a result, some distortion is present in reconstructed images but as we shall soon see, in the compression stage the levels of distortion can be adjusted. For both colour and black-and-white images JPEG method is used, but compression of the latter is the main focus of this article.

1.2. DWT:

We used the Discrete Wavelet Transform (DWT) approach to withstand the attacks and to make the model robust enough.

DWT produces four sub-bands low-low (LL), low-high (LH), high-low (HL) and high-high (HH). By using these four sub-bands we can regenerate the original image. Theoretically, a filter bank shown in Fig. 1 should work on the image in order to generate different sub-band frequency images.

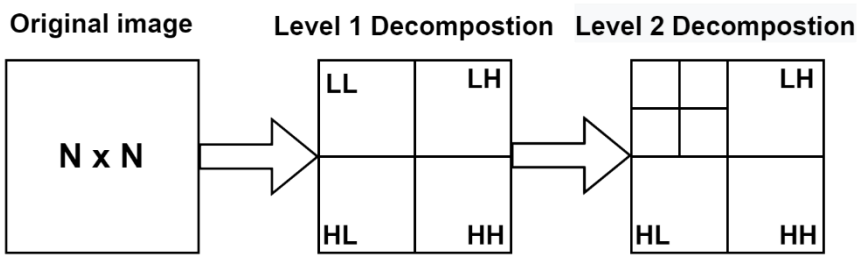


Fig.1. Sub-bands resulting after 2-level decomposition

As shown in fig.2 The LL sub-band specifies low-pass filtering on each row and each column, and it is a low-resolution approximation of the original image. Similarly, the LH sub-band resulted from the low-pass filtering on each row and the high-pass filtering on each column. The high-frequency details along the column direction influence the LH sub-band. The HL sub-band is the result of high-pass filtering on each row and the low-pass filtering on each column. The high-frequency details along the row direction influence the HL sub-band. The HH sub-band is constructed from the high-pass filtering on each row and each column. The high-frequency details along the diagonal direction influence the HH sub-band.

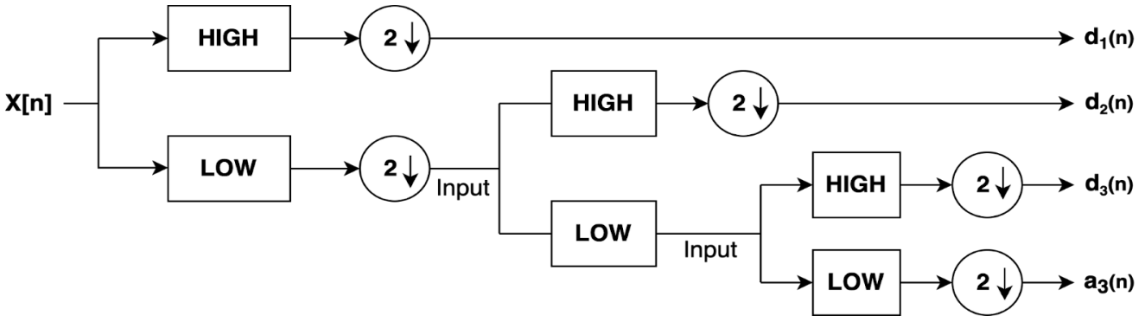


Fig.2. Block diagram of the 2 level DWT scheme

DWT Based Feature Extraction: DWT performs multi-level decomposition of the pre-processed image which results in efficient extraction of discriminant features which are insensitive to arbitrary environmental variations.

DWT is a wavelet transform for which the discrete interval wavelets are sampled. DWT gives an image's simultaneous frequency and spatial domain information. In DWT

operation, combination of analysis filter bank and decimation operation an image can be analysed. A pair of low and high pass filters corresponding to each decomposition level is the composition of the analysis filter bank. Approximate information of the image is extracted by a low pass filter whereas the details such as edges are extracted by high pass filter.

1.4. SVD:

Singular Value Decomposition (SVD) is used to approximate the matrix decomposition of the data into an optimal estimate of the signal and the noise components. This property is one of the most important properties of the SVD decomposition in noise filtering, compression and forensic which could also be treated as adding noise in a proper detectable way.

SVD refactors into three matrices for the given digital image. To refactor the image singular values are used and at the end of this process storage space required by the image is reduced as the image is represented with a smaller set of values. The SVD of mxn matrix A is given by the formula,

$$SVD = u\ vT\ w$$

Where,

U: mxn matrix of the orthonormal eigenvectors of AAT.

VT: transpose of a n x n matrix containing the orthonormal eigenvectors of A^{T}A.

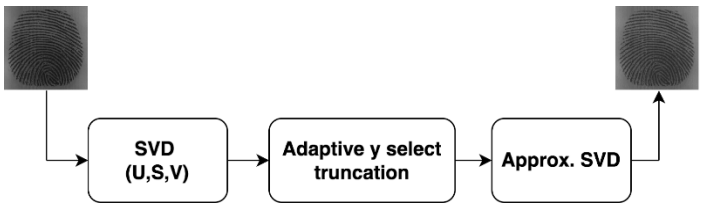
W: a nxn diagonal matrix of the singular values which are the square roots of the eigenvalues of ATA.

In linear algebra the SVD is a factorization of a rectangular real or complex matrix analogous to the diagonalization of symmetric or Hermitian square matrices using a basis of eigenvectors. SVD is an effective and most stable method to split the system into a set of linearly independent components, each of them bearing their own energy contribution [1,3]. A digital Image X of size MxN, with $M \geq N$, can be represented by its SVD as follows:

Where U is a MxM orthogonal matrix, V is a NxN orthogonal matrix, and S is aMxN matrix with the diagonal elements representing the singular values, si of X. The transpose of the matrix is denoted by subscript T. The orthogonal matrix U columns are called the left singular vectors, and the orthogonal matrix columns V are called the right singular vectors.

Several SVD properties are highly advantageous for images such as; its maximum energy packing, solving of least squares problem, computing pseudoinverse of a matrix and multivariate analysis [1,2]. The relation to the rank of a matrix and its ability to approximate matrices of a given rank is a key property of SVD. Digital images are often represented by low rank matrices and, therefore, are able to be described by a sum of a relatively small set of eigen images.

Image Compression SVD with the maximum energy packing property is usually used in compression. As mentioned above, SVD decomposes a matrix into orthogonal components with which optimal sub rank approximations may be obtained [5, 14]. Significant savings in storage over storing the whole matrix with accepted quality offered by truncated SVD transformation with rank r. Figure shows the block diagram of the SVD based compression.



First, the singular value matrix obtained by SVD contains illumination information. Therefore, changing the singular values will directly affect the illumination of the image. Hence, the other information in the image will not be changed. Second, by applying the illumination enhancement in LL subband will protect the edge information in other sub-bands (i.e. LH, HL, and HH).

CHAPTER 2

PROBLEM STATEMENT

CHAPTER 2
PROBLEM DEFINITION

The rapid growth in internet and communication technology has facilitated an escalation in the exchange of digital multimedia content. This has resulted in an increase in copyright infringement. Digital watermarking is a means of detecting ownership and illegal use of digital products. This project presents an approach to watermarking images by embedding Biometric information in a digital image, and also brings a new hybrid technique that consists of three different algorithms.

In this project, a watermarking algorithm of colour or grayscale image is proposed based on Discrete Wavelet Transform, Discrete Cosine Transform and Singular Value Decomposition (DWT-DCT-SVD).

Scope:

This project is prepared for the students at beginner and intermediate level who aspire to understand biometrics and various biometric systems and to protect them using watermarking. It would also be useful for enthusiasts in the fields of Electronics, IT security, and Biology.

This project is intended for an audience willing to acquire a high-level view of the relevant current topics in biometrics, as well as needing a starting point reference to get a deeper knowledge in the field of watermarking biometrics. Biometric systems find applications in law enforcement, e-commerce, smart cards, passports and visas etc.

CHAPTER 3

LITERATURE SURVEY

CHAPTER 3

LITERATURE SURVEY

1. "A robust blind colour image watermarking based on Fourier transform domain" published in 2020 used colour images watermarking based on the Fourier transform in a frequency domain technique to achieve good imperceptibility and also to generate watermarking images robust against various attacks with a high-quality watermark. The author Kahlessenane Fares et al., concludes saying the watermark into the higher coefficients can produce severe distortion of the image, whereas integrating into the lower coefficients makes the watermark robust to compression and filtering.
2. The author JUNXIU LIUet al., worked on watermarks with different sizes and proposed a image water -marking method that can achieve a good invisibility and robustness. Paper titled "An Optimized Image Watermarking Method Based on HD and SVD in DWT Domain" published in 2019.here the attacks were shown using graphs and plots.
3. Method of digital watermarking based on DWT-DCT-SVD was proposed using a scale factor and Arnold Transformation in the paper titled "A Proposed Digital Image watermarking Based on DWT-DCT-SVD" published in the year 2018 by Yuqi He.et al. Technologies used in the paper are Arnold Transform, discrete Wavelet Transform, discrete Cosine transform, singular value decomposition. In this paper, a method of digital watermarking based on DWT-DCT-SVD was proposed using a scale factor and Arnold Transformation in YUV Colour space. Proposed algorithm can be even more improvised to increase the robustness and imperceptibility.
4. The review of all existing steganographic methods (data embedding and extracting) for data hiding inside the text, image, audio and video channels have been described by the author Himanshu Arora et al., in the paper "Comparative study of image steganography techniques"
5. The paper titled "DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection" published in 2017 by Durgesh Singh et al. Here the proposed

scheme is free from false positive detection problems which occur in the SVD based watermarking schemes.

6. Another paper titled "Implementation of DCT DWT SVD based watermarking algorithms for copyright protection" published in 2015. The author A.B. Nandurbarkar et al., concludes that DWT is not robust against low pass filter attacks. DCT gives quite better results in all listed attacks. Here the comparative analysis of various Image compression techniques for different images is done based on three parameters: compression ratio (CR), mean square error (MSE), peak signal to noise ratio (PSNR).

7. The algorithm used in the paper "An optimized watermarking technique based on self-adaptive DE in DWT-SVD transform domain" published in 2014 has prominent imperceptibility and good robustness. The technology used here was an image watermarking scheme using self-adaptive differential evolution (SDE) algorithm based on optimal discrete wavelet transform–singular value decomposition (DWT–SVD) by author Mussrat Ali et al.
8. The paper titled "A Comparative Study of DCT, DWT & Hybrid (DCT-DWT) Transform" published in the year 2013 achieved higher compression ratio using Hybrid technique but loss of information is more. Here the author Archana Deshlahra et al., also describes that DWT requires more processing power and DCT overcomes this disadvantage since it needs less processing power, but it gives less compression ratio.
9. An Improved Image Watermarking by Modifying Selected DWT-DCT Coefficients. Ferda Ernawan, Dhani Ariatmanto, & Ahmad Firadus have published this journal in the year 2021. This paper proposed the adaptive scaling factor based selected DWT-DCT coefficients of its image content. The adaptive scaling factor was generated based on the role of selected DWT-DCT coefficients against the average value of DWT-DCT coefficients.
10. A DWT based watermarking approach for medical image protection. Fares Kahlessenane, Amine Khaldi, Redouane Kafi, & Salah Euschi have published this paper in 2021. A discrete wavelet transform is applied to the image before the

integration process, then, a topological reorganization of the coefficients of the LL sub-bands is done by the ZigZag scanning method. The obtained coefficients are then combined to integrate the watermark bits. A hash of the electronic patient record being integrated in the image, the integrity of the watermark can easily be verified. After the evaluation of our approach in terms of invisibility and robustness, the experimental results obtained show that our approach offers excellent imperceptibility

11. Hybrid SVD-Based Image Watermarking Schemes: A Review published in 2021 by wafa hamdan alshoura, zurinahni zainol, je sen teh ,moatsum alwida, and abdullatif al abdullatif. There are many existing hybrid SVD-based image watermarking schemes found to be insecure. As there is also a lack of in-depth reviews in this domain, the focus of this paper is the analysis of the state-of-the-art in hybrid SVD-based image watermarking. We perform efficiency comparisons to highlight various security problems, open issues, and research gaps. Based on our findings, we additionally provide some recommendations for the development of more robust schemes in the future, This paper provides essential information for researchers and practitioners alike to advance the field of image watermarking.

CHAPTER 4

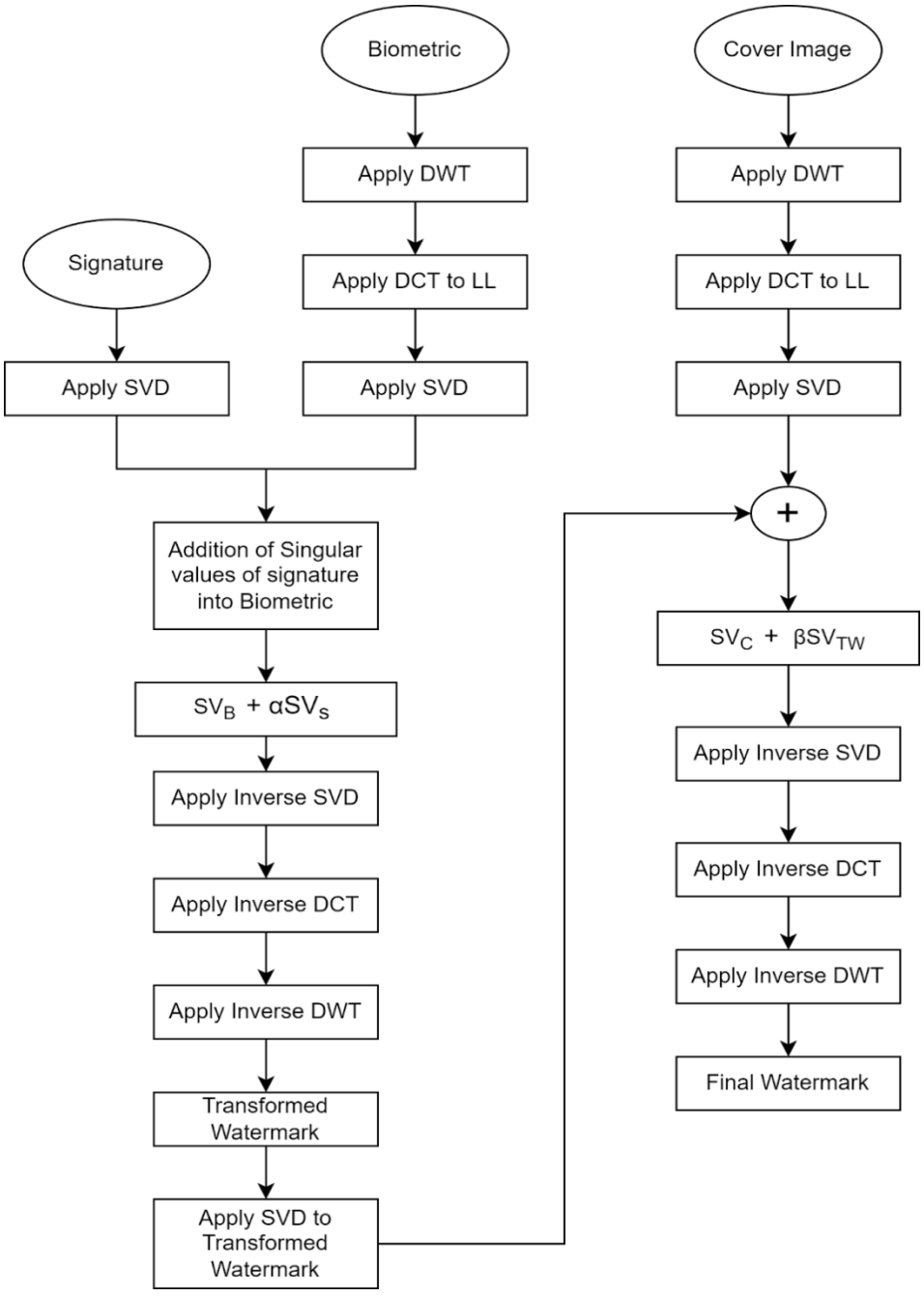
PROJECT DESCRIPTION

CHAPTER 4

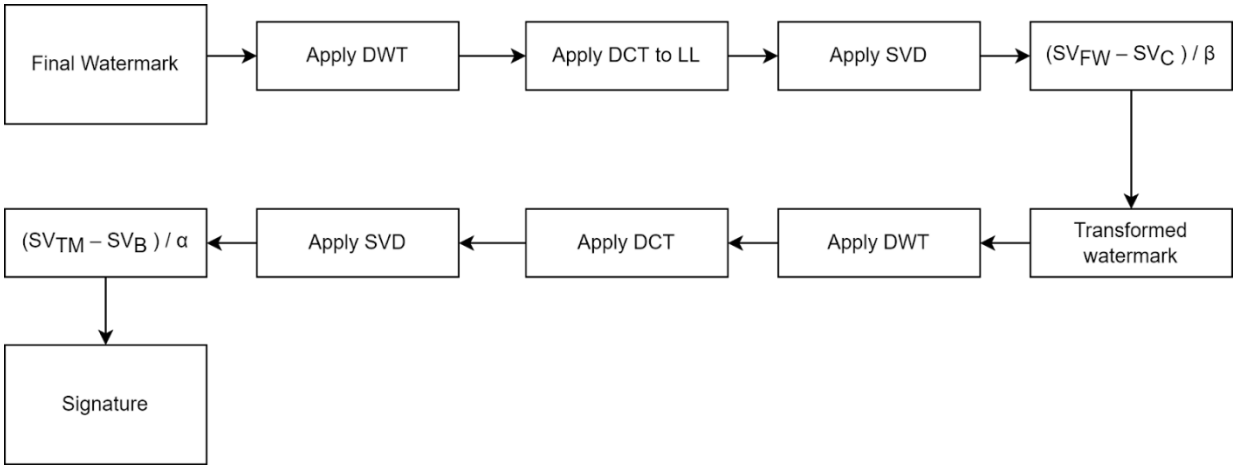
PROJECT DESCRIPTION

4.1 PROPOSED DESIGN

4.1.1. EMBEDDING:



4.1.2 EXTRACTION:



CHAPTER 5

REQUIREMENTS

CHAPTER 5

REQUIREMENTS

5.1. Functional Requirements:

- MATLAB 2021a.
- Windows 8 and above or any equivalent OS.

5.2. Non-Functional Requirements:

There are several more reasons for its requirement, such as:

Availability of multiple traits makes the hybrid system more reliable.

- A biometric system increases security and secrecy of user data. A biometric system conducts fusion strategies to combine decisions from each subsystem and then comes up with a conclusion. This makes the biometric system more accurate.
- The hybrid systems can provide knowledge about "liveliness" of the sample being entered by applying liveness detection techniques. This makes them capable of detecting and handling spoofing.

5.3. Hardware Requirements:

- Ram - Minimum 4GB (recommended 8GB)
- Processor - Any processor with base clock frequency 2.0 GHz or more recommended octa core.
- Secondary Storage - 50GB (recommended)

Chapter 6

METHODOLOGY

CHAPTER 6

METHODOLOGY

ALGORITHM:

The proposed methodology is divided into two steps:

A. Watermark Embedding Algorithm

B. Watermark Extraction Algorithm

A. Watermark Embedding Algorithm:

The Embedding algorithm can be split into two phases,

- Embedding process of signature into biometric -
  a. Apply SVD to the signature to obtain the singular values SV_S.
  b. Apply DWT level-1 to the biometric to obtain 4-subbands.
  c. Apply DCT to LL subband in order to remove redundancy.
  d. Apply SVD to the biometric to obtain singular values SV_B.
  e. Change the singular values of biometric SV_B by adding the singular values of signature SV_S.

$$SV_{TW} = SV_B + alpha*SV_S$$

  f. The Transformed watermark TW is obtained by applying inverse SVD, DCT and DWT.

- Embedding process of Transformed watermark into Cover image
  a. Apply DWT to cover image to obtain 4-subbands.
  b. Apply DCT to LL subband in order to remove redundancy.
  c. Apply SVD to obtain the singular values of cover image SV_C.
  d. Manipulate the singular values of cover image SV_C by adding the singular values of transformed image SV_{TW}.

$$SV_{FW} = SV_C + beta*SV_{TW}$$

e. Obtain the final watermarked image by applying the inverse of SVD, DCT and DWT techniques on the modified matrix.

B. Watermark Extraction Algorithm:

Extraction process is the extraction of watermarks i.e. biometric and signature from the cover image.

The extraction is carried out in two steps:

- Extraction of Transformed watermark (i.e., biometric)
  a. Apply DWT on the final watermark to obtain four sub-bands.
  b. Apply DCT to LL subband in order to remove redundancy.
  c. Apply SVD to obtain the singular values of the final watermarked image SV_{FW}
  d. To obtain the Transformed watermark image, subtract the singular values of Final watermarked image SV_{FW} from the cover image singular values $SV_{C.}$ and divide the whole with the beta parameter.

$$SV_{TW} = (SV_{FW} - SV_C) / \beta$$

- Extraction of signature watermark from Transformed watermark (i.e. biometric)
  a. Apply DWT on transformed watermark to obtain four sub-bands.
  b. Apply DCT to LL subband in order to remove redundancy.
  c. Apply SVD to obtain the singular values of the Transformed watermark.
  d. To obtain a signature, subtract the singular values of transformed watermark SV_{TM} from the biometric singular values $SV_{B.}$ and divide the whole with the alpha parameter.

$$SV_S = (SV_{TM} - SV_B) / \alpha$$

CHAPTER 7

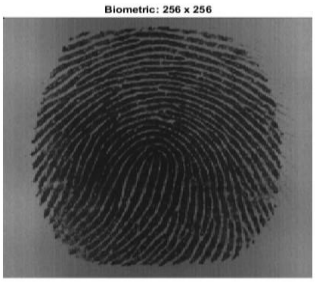
EXPERIMENTATION

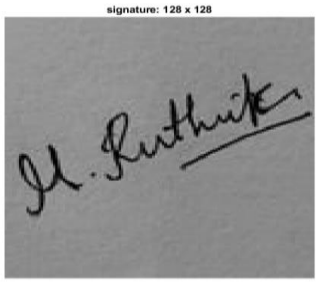
CHAPTER 7

EXPERIMENTATION

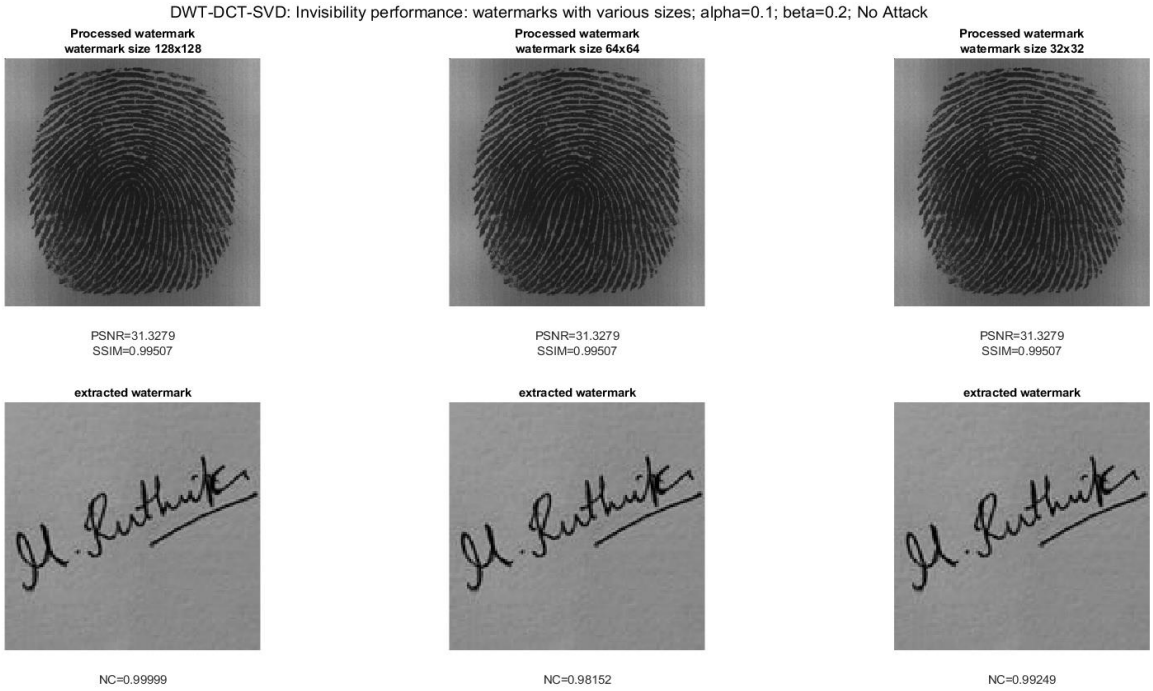
The experimentation was carried out according to the steps mentioned in the algorithm i.e embedding (hiding the cover image with the biometric and signature) followed by extraction. In this case we've embedded a biometric and a signature within a cover image. The images are extracted using an unique algorithm (DWT-DCT-SVD) without losing its actual detail. Here, the watermarked image will undergo different attacks and then the watermarks will be extracted to see the robustness of the hybrid model.

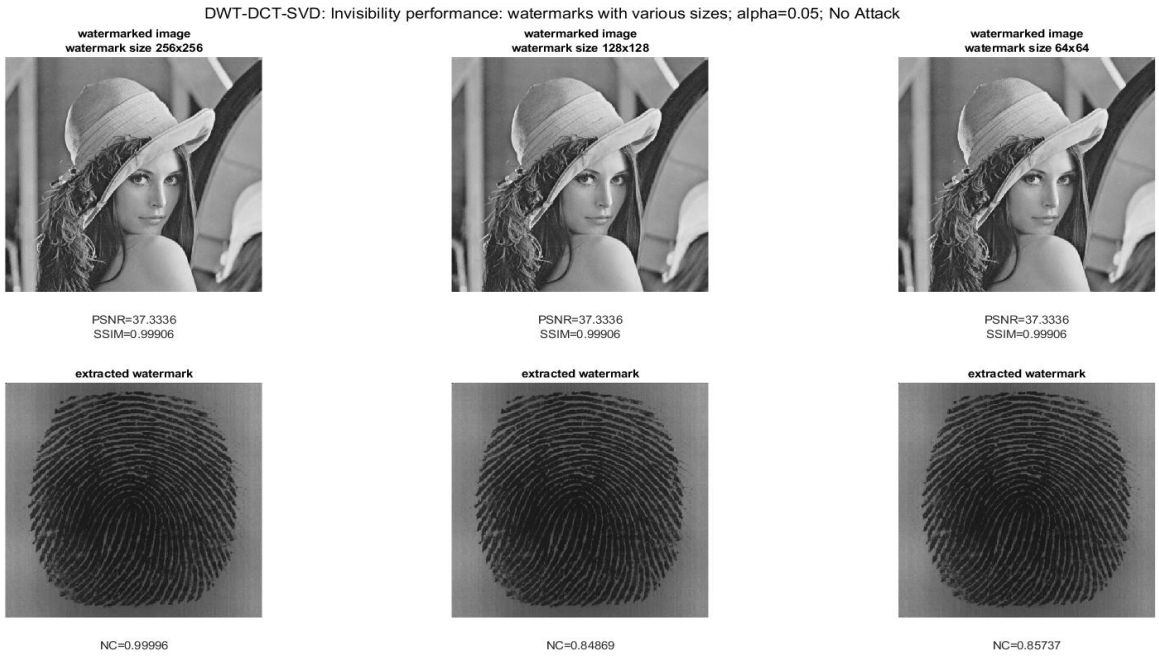
Images used in the experiment -





Invisible Performance –





Driver Code

1. Embedding

```
%% Embedding
%%Signature into Biometric
[BLL, BLH, BHL, BHH] = dwt2(biometric, 'haar');
J = dct2(BLL);
[BU, BS, BV] = svd(J, 'econ');
save(fullfile(tempdir, 'BS.mat'), 'BS', '-mat');     %save

% Apply SVD to Signature
[SU, SS, SV] = svd(double(signature), 'econ');
save(fullfile(tempdir, 'SU.mat'), 'SU', '-mat');     %save
save(fullfile(tempdir, 'SV.mat'), 'SV', '-mat');     %save

New_BS = BS + alpha.*SS;
MBS = BU * New_BS * BV';
New_LL = idct2(MBS);

Processed_watermark = idwt2(New_LL, BLH, BHL, BHH, 'haar');
Processed_watermark = uint8(Processed_watermark);

imwrite(Processed_watermark,'Pwatermark.png');
```

```
%% embed pwatermark into cover image

[CLL, CLH, CHL, CHH] = dwt2(cover_image, 'haar');
DLL = dct2(CLL);
[cU, cS, cV] = svd(DLL, 'econ');
save(fullfile(tempdir, 'cS.mat'), 'cS', '-mat');    %save

[pwU, pwS, pwV] = svd(double(Processed_watermark),'econ');
save(fullfile(tempdir, 'pwU.mat'), 'pwU', '-mat');  %save
save(fullfile(tempdir, 'pwV.mat'), 'pwV', '-mat');  %save
HSw = cS + beta.*pwS;
H = cU * HSw * cV';
CLL_new = idct2(H) ;

Final_watermark = idwt2(CLL_new, CLH, CHL, CHH, 'haar');
Final_watermark = uint8(Final_watermark);
imwrite(Final_watermark,'FinalWatermarked.png');
```

2. Extraction

```
%% Extraction of Pwatermark from Final Watermark

[fLL, fLH, fHL, fHH] = dwt2(Final_watermark, 'haar');
dfLL = dct2(fLL);
[fU, fS, fV] = svd(dfLL);

Pw_s = (fS - cS)./beta;
w_hat = pwU * Pw_s * pwV';

Expw = uint8(w_hat);
imwrite(Expw,'Extracted_pw.png');
```

```
%% Extraction of Signature from Pwatermark
[pLL, pLH, pHL, pHH] = dwt2(Expw, 'haar');
Pw = dct2(pLL);
[ESU, ESS, ESV] = svd(Pw);
SS = (ESS - BS)./alpha;      %%

ExSS = SU*SS*SV';
EXS = uint8(ExSS);
imwrite(EXS,'ExSig.png');
```

3. Attacks

```
%% This function applies attacks on images
%  Input: image, attack type, attack parameters (different for each attack)
function [watermarked_image] = Attacks(watermarked_image,attack,param)
switch attack
    case 'No Attack'
    case 'Median'
        watermarked_image = medianAttack(watermarked_image,param);
    case 'Gaussian noise'
        watermarked_image = noiseGauss(watermarked_image,param);
    case 'Salt and pepper noise'
        watermarked_image = noiseSaltPepper(watermarked_image);
    case 'Speckle noise'
        watermarked_image = noiseSpeckle(watermarked_image);
    case 'Sharpening attack'
        watermarked_image = sharpenAttack(watermarked_image,param);
    case 'Rotating attack'
        watermarked_image = rotatAttack(watermarked_image);
    case 'Motion blur'
        watermarked_image = motionAttack(watermarked_image);
    case 'Average filter'
        watermarked_image = averageFilter(watermarked_image);
    case 'JPEG2000 compression'
        watermarked_image = jp2Attack(watermarked_image,param);
```

CHAPTER 8

TESTING AND RESULTS

CHAPTER 8

TESTING AND RESULTS

The hybrid algorithm worked robust against all possible image processing attacks with good NCC, SSIM and PSNR values. The different test cases carried out are as follows:

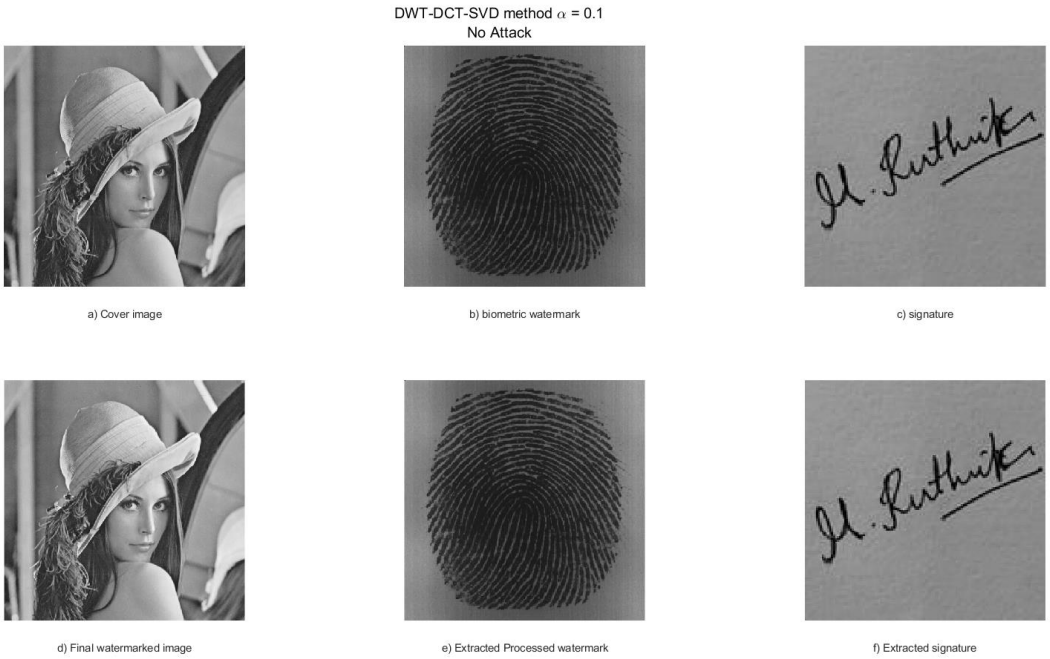


Figure 1: No Attack

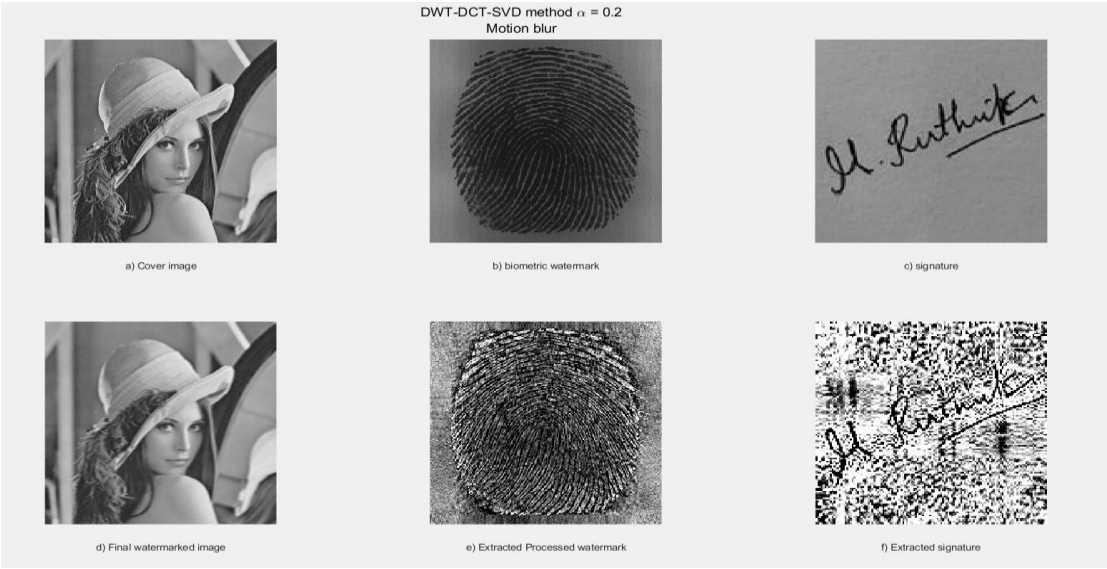


Figure 2: Motion Blur

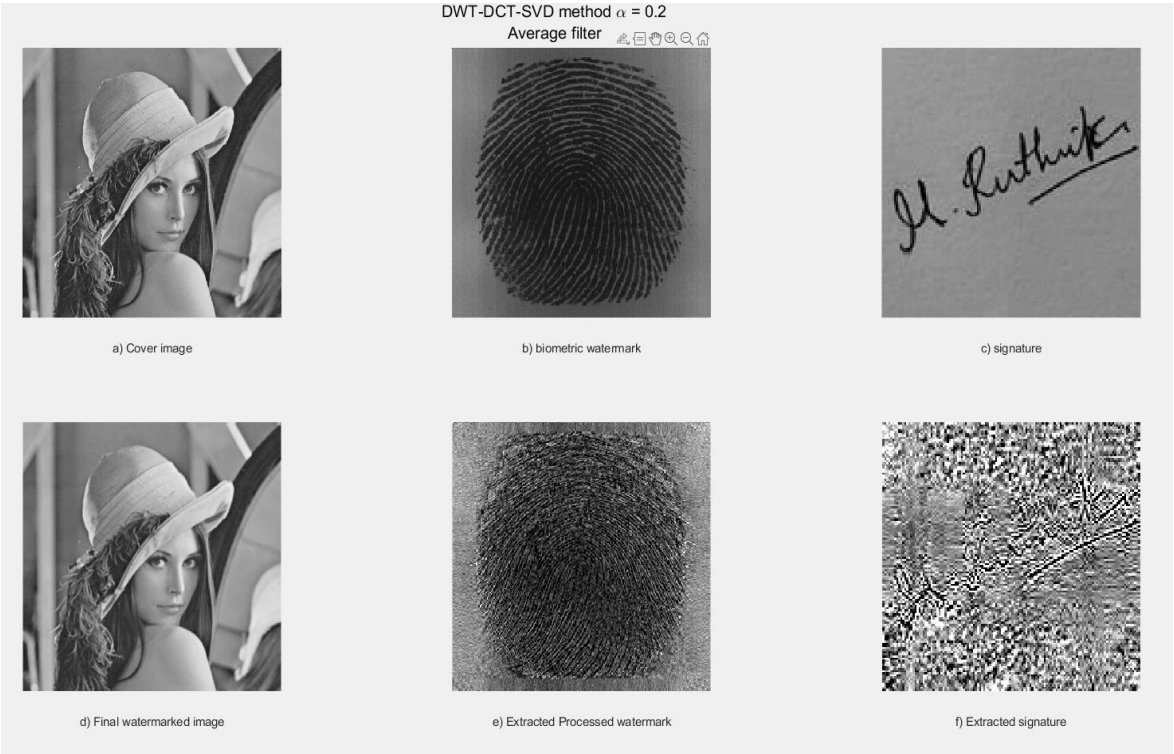


Figure 3: Average Filter

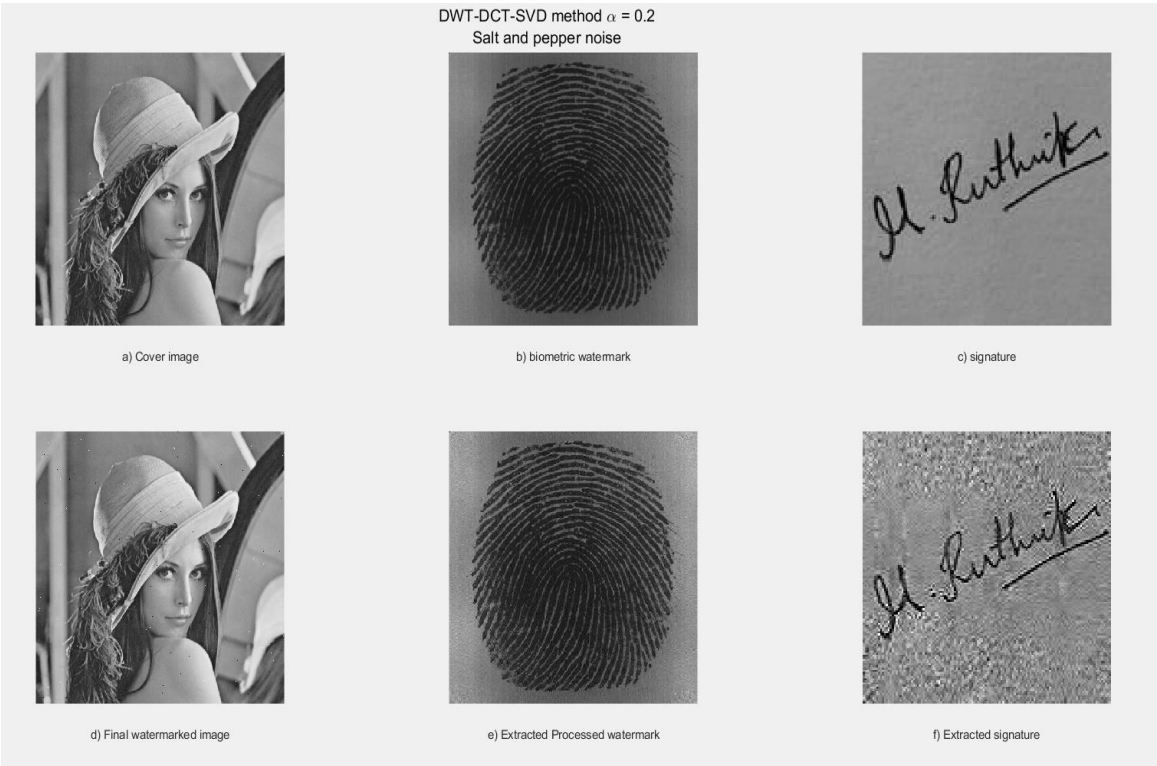


Figure 4: Salt & Pepper noise

Figure 5: Histogram Equalization

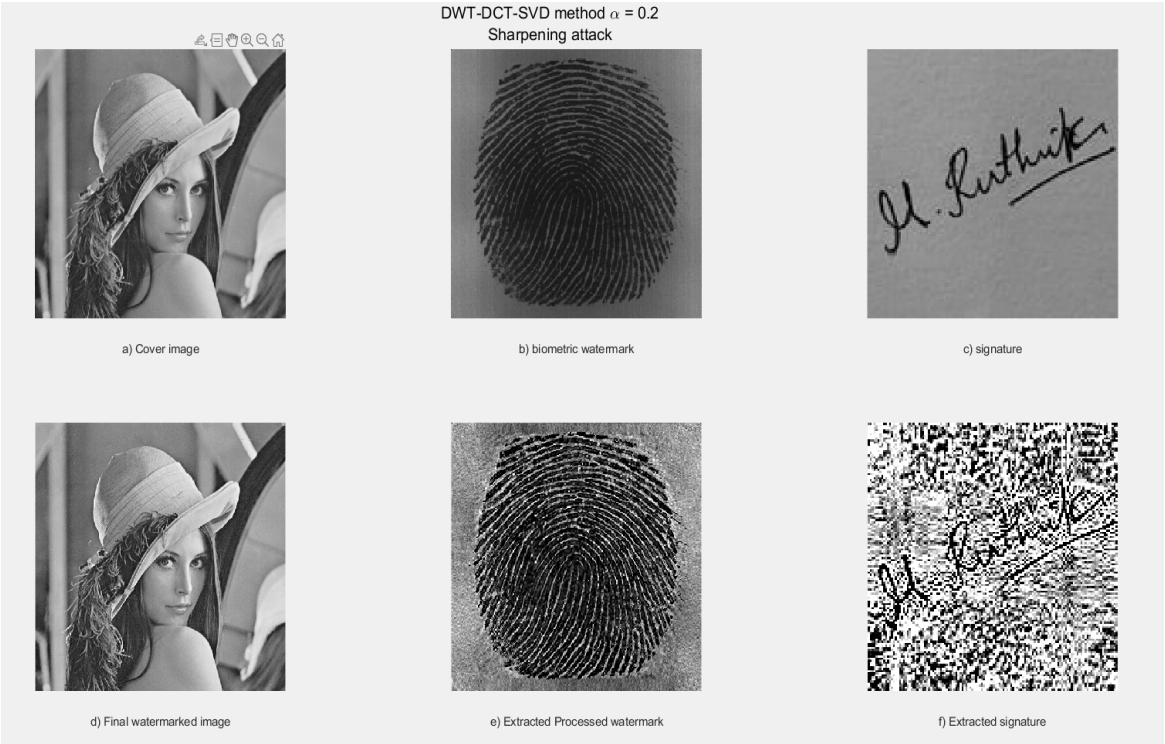


Figure 6: Sharpening Attack

Figure 7: Jpeg2000 Compression

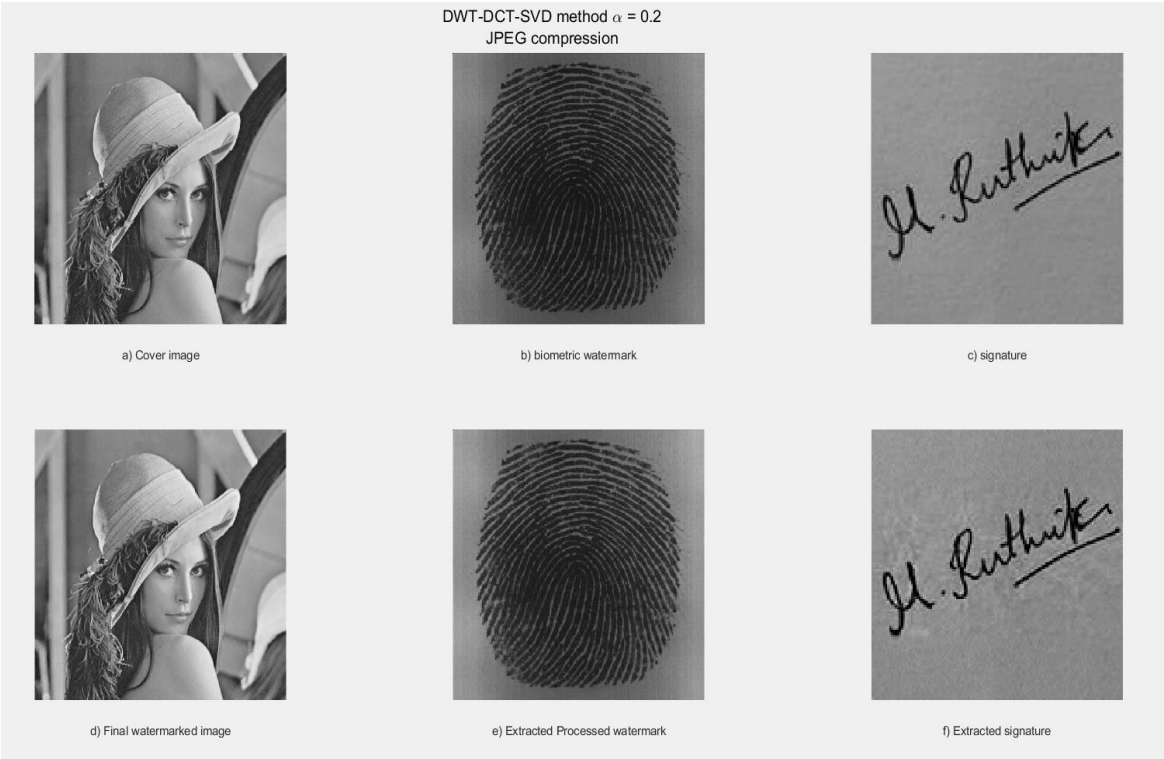


Figure 8: Jpeg Compression

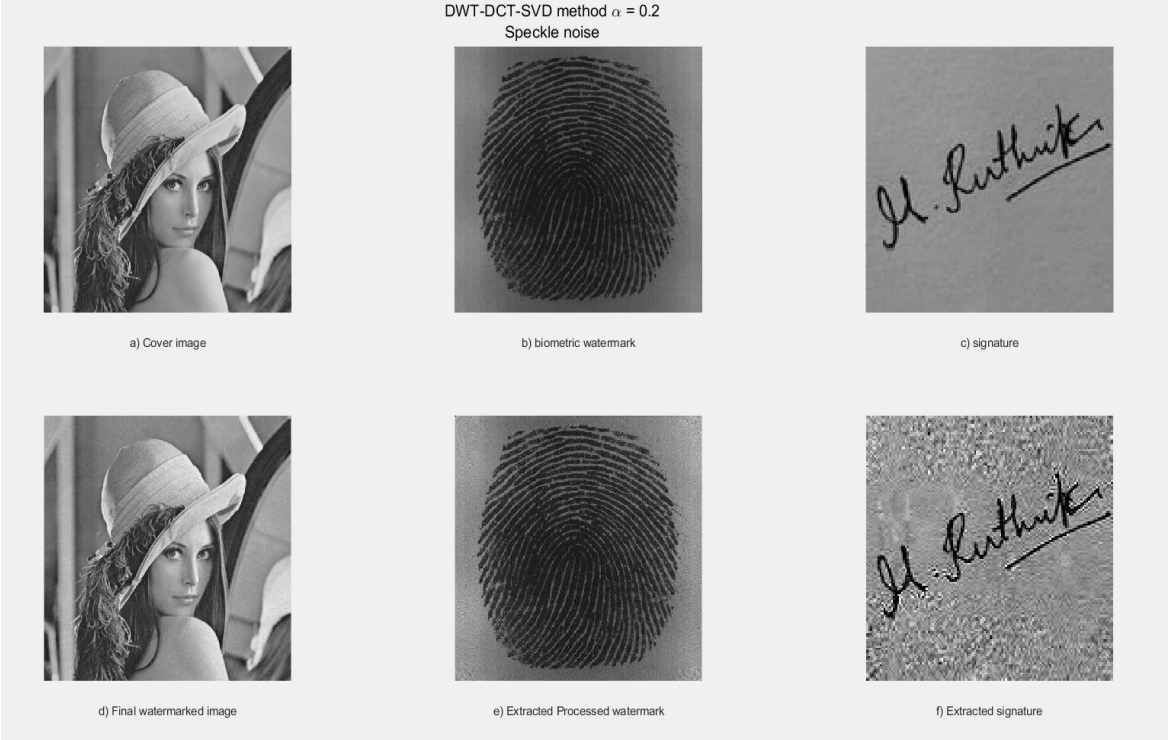


Figure 9: Speckle Noise

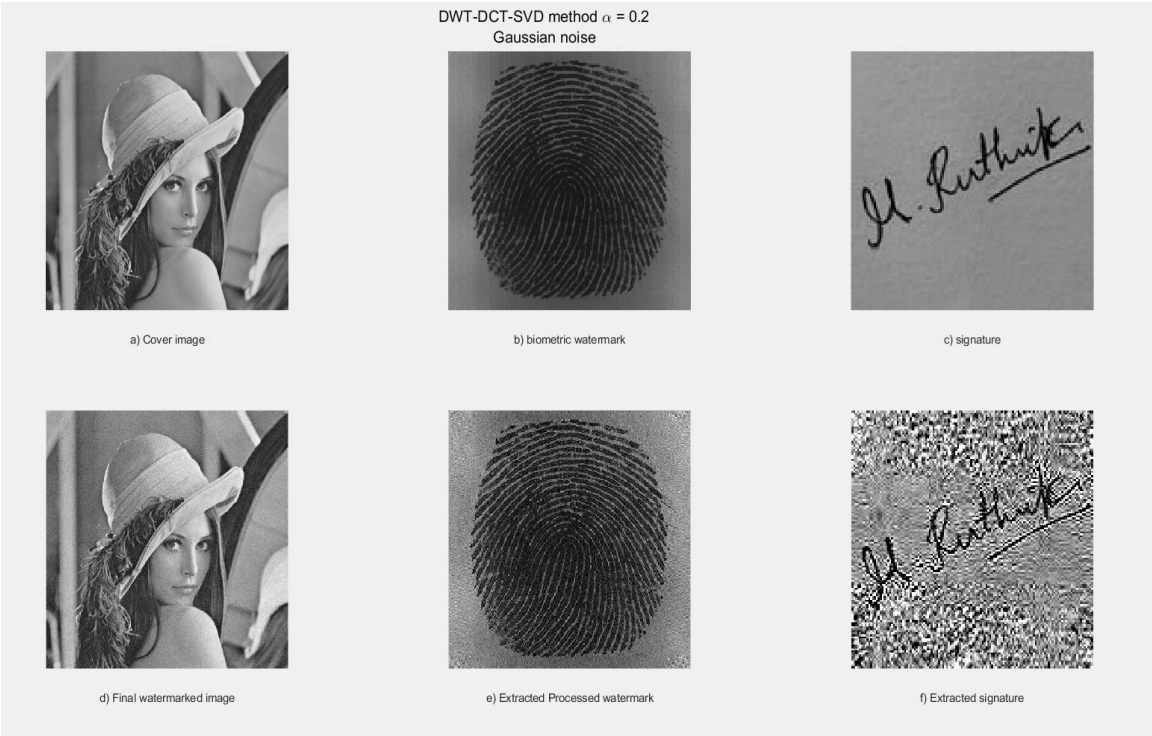


Figure 10: Gaussian Noise

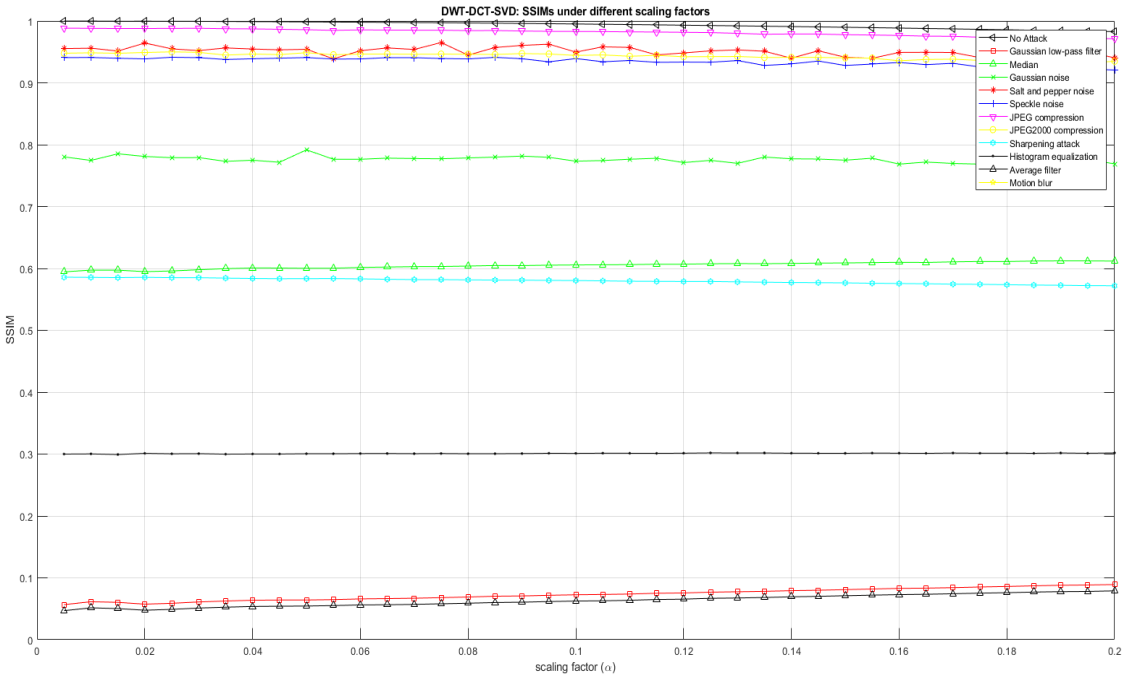


Figure 11: SSIM vs $\boldsymbol{\alpha}/\boldsymbol{\beta}$

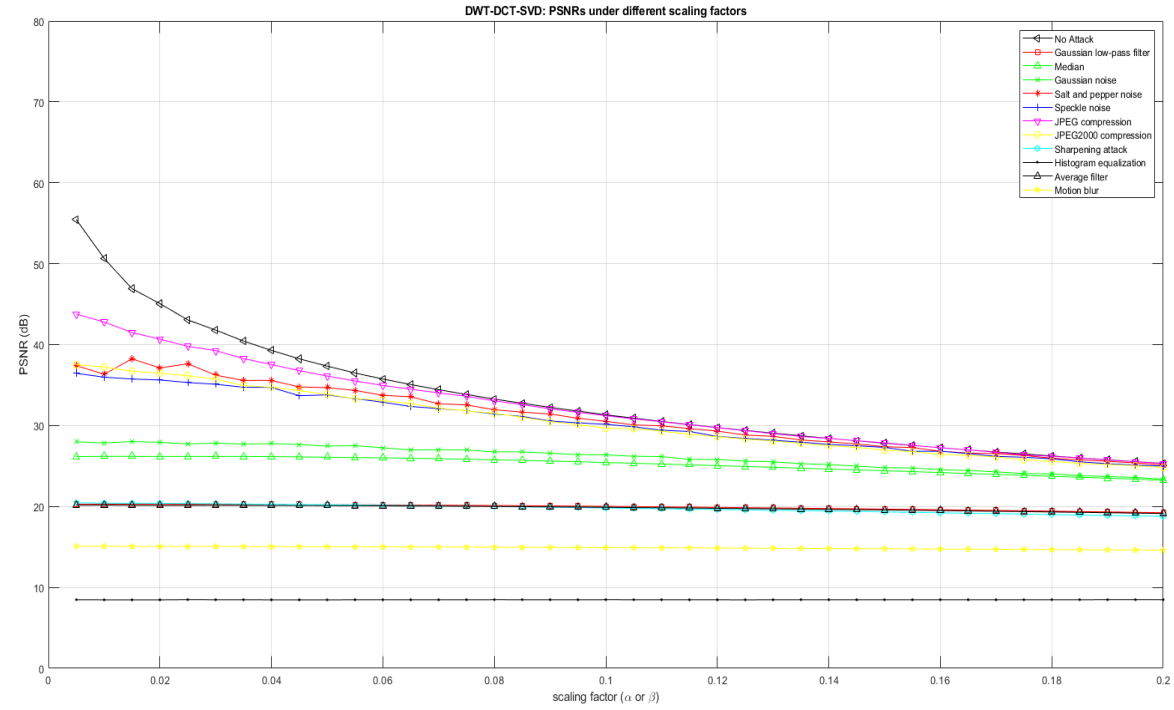


Figure 12: PSNR vs $\boldsymbol{\alpha}/\boldsymbol{\beta}$

Table 1: NCC values

ATTACKS	**NCC_B**	**NCC_S**
CROP	0.4345	0.9922
SALT & PEPPER	0.7586	0.7862
GUASSIAN	0.7472	0.7002
SPECKLE	0.4865	0.8047
ROTATION	0.5005	0.8827
SCALE 2X	0.9590	0.9340
SCALE 0.5X	0.6307	0.7165
MEDIAN	0.9650	0.9751
SHARPENING	0.5507	0.6234
MOTION BLUR	0.6217	0.8421
AVERAGE FILTER	0.62	0.8090
HISTOGRAM EQUALIZATION	0.6012	0.6104
JPEG	0.857	0.846
JPEG2000	0.846	0.8562

Table 1 depicts Normalised Cross Correlation (NC) values for biometric (NCCB) and signature (NCCS) under different types of attacks. In all the test cases the result obtained with better NCC values even after the extraction of watermarks viz, biometric and signature.

Table 2: PSNR

ATTACKS	**$PSNR_B$**	**$PSNR_S$**
CROP	4.1422	23.5847
SALT & PEPPER	5.2669	6.9213
GUASSIAN	6.8711	7.3798
SPECKLE	5.4516	11.4783
ROTATION	9.0110	7.2282
SCALE 2X	24.0391	17.1220
SCALE 0.5X	5.5592	7.5178
MEDIAN	6.6279	7.2673
SHARPENING	4.7371	9.6499
MOTION BLUR	4.3715	7.5336
AVERAGE FILTER	4.3984	7.8970
HISTOGRAM EQUALIZATION	5.4978	10.2860
JPEG	5.4542	9.5644
JPEG2000	6.4532	10.8961

Table 2 shows Peak Signal to Noise Ratio (PSNR) values for biometric (PSNRB) and signature (PSNRS) under different types of attacks. In all the test cases the result obtained with better PSNR values even after the extraction of watermarks viz, biometric and signature.

Table 3: SSIM

ATTACKS	**$SSIM_B$**	**$SSIM_S$**
CROP	0.87634	0.90724
SALT & PEPPER	0.99536	0.76606
GUASSIAN	0.46688	0.55715
SPECKLE	0.78373	0.84695
ROTATION	0.78654	0.49736
SCALE 2X	0.98742	0.97214
SCALE 0.5X	0.99146	0.98632
MEDIAN	0.097755	0.36953
SHARPENING	0.32219	0.26843
MOTION BLUR	0.14037	0.049129
AVERAGE FILTER	0.12215	-ve
HISTOGRAM EQUALIZATION	0.29474	0.50328
JPEG	0.9519	0.94418
JPEG2000	0.80577	0.84715

Table 3 depicts Structural Similarity Index Metrics (SSIM) values for biometric (SSIMB) and signature (SSIMS) under different types of attacks. In all the test cases the result obtained with better SSIM values even after the extraction of watermarks viz, biometric and signature.

CHAPTER 9

CONCLUSION AND FUTURE WORK

CHAPTER 9

CONCLUSION AND FUTURE WORK

This project extends a scheme of watermarking that is a combination of spatial and transform domain methods. The DWT-DCT-SVD technique to embed watermark can be of the same size as that of cover image due to the shift invariant feature of RDWT. Here in the proposed method the outcome of RDWT implementation of watermarked images has high PSNR and Normal Cross Correlation. The results illustrate, suggested method is not only efficient in defending against attacks but also improving the performance with respect to noise. In the course of time, a new plan to upgrade the strategy of watermark embedding considering the loopholes. In the future, this work can be extended for video, audio, 3D images and other biometric features like iris, face, voice, palm, etc.

REFERENCES

[1] Ernawan, Ferda, Dhani Ariatmanto, and Ahmad Firdaus. "An Improved Image Watermarking by Modifying Selected DWT-DCT Coefficients." *IEEE Access* 9 (2021): 45474-45485.

[2] Kahlessenane, Fares, et al. "A DWT based watermarking approach for medical image protection." *Journal of Ambient Intelligence and Humanized Computing* 12.2 (2021): 2931-2938.

[3] Zainol, Zurinahni, et al. "Hybrid SVD-based image watermarking schemes: a review." *IEEE Access* 9 (2021): 32931-32968.

[4] Begum, Mahbuba, Jannatul Ferdush, and Mohammad Shorif Uddin. "A Hybrid robust watermarking system based on discrete cosine transform, discrete wavelet transform, and singular value decomposition." *Journal of King Saud University-Computer and Information Sciences* (2021).

[5] Alzahrani, Ali, and Nisar Ahmed Memon. "Blind and Robust Watermarking Scheme in Hybrid Domain for Copyright Protection of Medical Images." *IEEE Access* 9 (2021): 113714-113734.

[6] Alzahrani, Ali. "Enhanced Invisibility and Robustness of Digital Image Watermarking Based on DWT-SVD." *Applied Bionics and Biomechanics* 2022 (2022).

[7] Zeebaree, Diyar Q. "Robust watermarking scheme based LWT and SVD using artificial bee colony optimization." *Indonesian Journal of Electrical Engineering and Computer Science* 21.2 (2021): 1218-1229.

[8] Rajani, D., and P. Rajesh Kumar. "An optimized hybrid algorithm for blind watermarking scheme using singular value decomposition in RDWT-DCT domain." *Journal of Applied Security Research* 17.1 (2022): 103-122.

[9] Ikbal, Febina, and R. Gopikakumari. "Performance analysis of SMRT-based color image watermarking in different color spaces." *Information Security Journal: A Global Perspective* (2021): 1-11.

[10] Kumar, Parmalik, and A. Sharma. "A robust image watermarking technique using feature optimization and cascaded neural network." *International journal of computer science and information security (IJCSIS)* 18.8 (2019).

[11] Fares, K., Amine, K., & Salah, E. (2020). A robust blind color image watermarking based on Fourier transform domain. Optik, 208, 164562.

[12] Liu, J., Huang, J., Luo, Y., Cao, L., Yang, S., Wei, D., & Zhou, R. (2019). An optimized image watermarking method based on HD and SVD in DWT domain. IEEE Access, 7, 80849-80860.

[13] He, Y., & Hu, Y. (2018, May). A proposed digital image watermarking based on DWT-DCT-SVD. In 2018 2nd IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC) (pp. 1214-1218). IEEE.

[14] Arora, H., Bansal, C., & Dagar, S. (2018, October). Comparative study of image steganography techniques. In 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN) (pp. 982-985). IEEE.

[15] Singh, D., & Singh, S. K. (2017). DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection. Multimedia Tools and Applications, 76(11), 13001-13024.

APPENDIX A

GitHub link:
https://github.com/lalithsagarJ/Hybrid_Watermarking_Technique_for_Image_authentication_Using_Biometrics

Paper publication - IEEE Mysore conference 2021

https://drive.google.com/file/d/1AFogjoV8fkzd3RXBdh5jfl1B1QoLPpbT/view?usp=sharing