

OPTIMIZED IMAGE WATERMARKING
BASED ON HD AND SVD IN IWT DOMAIN

AHMAD HISYAM BIN SURYANTO SUGIAN

UNIVERSITI MALAYSIA PAHANG

UNIVERSITI MALAYSIA PAHANG

DECLARATION OF THESIS AND COPYRIGHT

Author's Full Name : AHMAD HISYAM BIN SURYANTO SUGIAN

Date of Birth : 26 May 2000

Title : Optimized Image Watermarking Based on HD and SVD In IWT Domain

Academic Session : 2022/2023

I declare that this thesis is classified as:

- CONFIDENTIAL (Contains confidential information under the Official Secret Act 1997)*
- RESTRICTED (Contains restricted information as specified by the organization where research was done)*
- OPEN ACCESS I agree that my thesis to be published as online open access (Full Text)

I acknowledge that Universiti Malaysia Pahang reserves the following rights:

1. The Thesis is the Property of Universiti Malaysia Pahang
2. The Library of Universiti Malaysia Pahang has the right to make copies of the thesis for the purpose of research only.
3. The Library has the right to make copies of the thesis for academic exchange.

Certified by:

(Student's Signature)

(Supervisor's Signature)

0002000200
New IC/Passport Number
Date: 10 July 2023

Associate Prof. Ts. Dr. Ferda Ernawan
Name of Supervisor
Date: 10 July 2023

NOTE : * If the thesis is CONFIDENTIAL or RESTRICTED, please attach a thesis declaration letter.

THESIS DECLARATION LETTER (OPTIONAL)

Librarian,
Perpustakaan Universiti Malaysia Pahang,
Universiti Malaysia Pahang,
Lebuhraya Tun Razak,
26300, Gambang, Kuantan.

Dear Sir,

CLASSIFICATION OF THESIS AS RESTRICTED

Please be aware that for a period of three years starting from the date of this letter, the following thesis is designated as RESTRICTED. The following reasons are given for this classification.

Author's Name	Ahmad Hisyam Bin Suryanto Sugian
Thesis Title	Optimized Image Watermarking Based on HD and SVD In IWT Domain

Reasons	(i)
	(ii)
	(iii)

Thank you.

Yours faithfully,

(Supervisor's Signature)

Date: **TS. DR. FERDA ERNAWAN**
SENIOR LECTURER
FACULTY OF COMPUTING
COLLEGE OF COMPUTING & APPLIED SCIENCES
Stamp: **UNIVERSITI MALAYSIA PAHANG**
26600 PEKAN, PAHANG DARUL MAKMUR
TEL : 09-424 4648 FAX : 09-424 4686

Note: The supervisor should draw this letter and send it to the librarian at Perpustakaan Universiti Malaysia Pahang with a copy of the letter attached to the thesis.



SUPERVISOR'S DECLARATION

By signing this document, I/We attest that we have examined the thesis or project in question and believe it to be of sufficient quality and scope to be awarded the degree of *Doctor of Philosophy/Master of Engineering/Master of Science in. (.....)

(Supervisor's Signature)

Full Name : DR FERDA ERNAWAN

Position : Senior Lecturer

Date : 10 July 2023



STUDENT'S DECLARATION

I affirm that the content of this thesis is entirely my own work, with the exception of any quotes or citations that have been properly acknowledged. The work has not previously been submitted for a degree at Universiti Malaysia Pahang or any other academic institution.

(Student's Signature)

Full Name : AHMAD HISYAM BIN SURYANTO SUGIAN

ID Number : CB20160

Date : 10 July 2023

OPTIMIZED IMAGE WATERMARKING BASED ON HD AND SVD IN IWT
DOMAIN

AHMAD HISYAM BIN SURYANTO SUGIAN

This thesis is submitted to fulfill the requirements for the
award of the degree of
Doctor of Philosophy/Master of Science/Master of Engineering

Faculty of Computing
UNIVERSITI MALAYSIA PAHANG

NOVEMBER 2022

ACKNOWLEDGEMENTS

I am immensely grateful to God for guiding me through my research and providing me with the means to complete it successfully. I would like to extend my sincerest gratitude to my advisor, Dr. Ferda Ernawan, for his unwavering support, patience, and valuable feedback throughout this process. I would not have been able to embark on this journey without his invaluable guidance and assistance.

Furthermore, this project would not have been possible without the generous funding provided by Jabatan Perkhidmatan Awam, which supported my study expenses and more.

I am also thankful for my friends for their support, feedback, and moral support during late-night sessions. I also want to acknowledge the University's librarians and study participants for their influence and motivation.

I am also deeply grateful to my family, particularly my parents, sister, and grandmother, for their unwavering support and confidence in me. Their encouragement and support helped to keep my spirits and motivation strong throughout this endeavor. Additionally, I would like to thank my cats for providing me with both fun and emotional support.

ABSTRAK

Di zaman digital hari ini, melindungi kepemilikan kandungan multimedia telah menjadi isu yang penting. Penggunaan internet yang meluas dan kemudahan menyalin dan mengedarkan media digital telah menjadikan semakin sukar untuk mencegah penggunaan dan pengedaran tanpa kebenaran. Untuk mengatasi masalah ini, penanda air telah muncul sebagai penyelesaian yang berkesan. Penanda air imej merujuk kepada proses menyematkan pengenalan unik ke dalam imej dengan cara yang tidak kelihatan oleh mata manusia tetapi dapat diekstrak untuk membuktikan kepemilikan. Dalam kajian ini, kami mencadangkan kaedah penanda air imej yang dioptimumkan berdasarkan Hessenberg Decomposition (HD) dan Singular Value Decomposition (SVD) dalam domain Integer Wavelet Transform (IWT). Kaedah yang dicadangkan menggunakan ciri HD imej untuk meningkatkan ketahanan penanda air terhadap serangan, sementara teknik SVD digunakan untuk mencapai ketidakterlihatan dan keselamatan yang tinggi. Domain IWT digunakan untuk menjadikan proses penanda air lebih cekap, yang menghasilkan algoritma penanda air yang lebih cepat dan lebih boleh dipercayai. Untuk menilai keberkesanan kaedah yang dicadangkan, kami menjalankan beberapa eksperimen menggunakan dataset imej standard. Hasilnya menunjukkan bahawa kaedah yang dicadangkan lebih unggul daripada kaedah penanda air yang terdahulu dalam hal ketahanan dan ketidakterlihatan. Selain itu, kaedah yang dicadangkan adalah tahan terhadap pelbagai serangan pemprosesan imej. Kesimpulannya, kaedah penanda air imej yang dioptimumkan yang dicadangkan berdasarkan HD dan SVD dalam domain IWT menawarkan penyelesaian yang sangat berkesan untuk melindungi kepemilikan kandungan multimedia. Penggunaan teknik HD dan SVD dalam domain IWT memastikan ketahanan, ketidakterlihatan, dan keselamatan yang tinggi pada penanda air, sementara kecekapan pengiraan kaedah menjadikannya praktikal untuk aplikasi dunia nyata.

ABSTRACT

In today's digital age, protecting the ownership of multimedia content has become a crucial issue. The widespread use of the internet and the ease of copying and distributing digital media have made it increasingly challenging to prevent unauthorized use and distribution. To address this problem, watermarking has emerged as an effective solution. Image watermarking refers to the process of embedding a unique identifier into an image in a way that it is imperceptible to the human eye but can be extracted to prove ownership. In this research, we propose an optimized image watermarking method based on Hessenberg Decomposition (HD) and Singular Value Decomposition (SVD) in the Integer Wavelet Transform (IWT) domain. The proposed method utilizes the HD feature of the image to enhance the robustness of the watermark against attacks, while the SVD technique is used to achieve high invisibility and security. The IWT domain is employed to make the watermarking process more efficient, leading to a faster and more reliable watermarking algorithm. To evaluate the effectiveness of the proposed method, we conducted several experiments using standard image datasets. The results show that the proposed method outperforms existing state-of-the-art watermarking methods in terms of robustness and invisibility. Additionally, the proposed method is resistant to various image processing attacks. In conclusion, the proposed optimized image watermarking method based on HD and SVD in the IWT domain offers a highly effective solution for protecting the ownership of multimedia content. The use of HD and SVD techniques in the IWT domain ensures high robustness, invisibility, and security of the watermark, while the computational efficiency of the method makes it practical for real-world applications.

TABLE OF CONTENT

DECLARATION	
ACKNOWLEDGEMENTS	ii
ABSTRAK	iii
ABSTRACT	iv
TABLE OF CONTENT	v
LIST OF TABLES	viii
LIST OF FIGURES	ix
LIST OF ABBREVIATIONS	x
CHAPTER 1 INTRODUCTION	1
1.1 Background	1
1.2 Problem Statement	2
1.3 Objectives	3
1.4 Scope	4
1.5 Thesis Organization	4
CHAPTER 2 LITERATURE REVIEW	5
2.1 Introduction	5
2.2 Optimized watermarking method	5
2.3 Embedded sub-band	7
2.4 Watermark Security	7
2.5 Transform Domain	8
2.5.1 Integer Wavelet Transform (IWT)	8
2.5.2 Singular Value Decomposition (SVD)	9

2.5.3	Hessenberg Decomposition (HD)	10
2.5.4	Hybrid Method	11
2.6	Existing System/Works	11
2.6.1	Explanation	13
2.7	Analysis/Comparison of Existing Systems	16
2.7.1	Analysis of the proposed optimized watermarking	16
2.8	Measurement of imperceptibility	18
2.9	Robustness measurement	18
CHAPTER 3 METHODOLOGY		20
3.1	Introduction	20
3.2	General Research Design	20
3.3	Experimental Setup	21
3.4	Experimental Design	22
3.5	Proposed Watermarking Scheme	23
3.5.1	Explanation of the IWT-HD-SVD optimized image watermarking technique	23
3.6	Evaluation of the watermarked image	28
3.6.1	Robustness and imperceptibility	28
3.6.2	Various attack analysis	28
3.7	Summary	29
CHAPTER 4 RESULTS AND DISCUSSION		30
4.1	Introduction	30
4.2	Performance of imperceptibility for various watermark images	30
4.3	Invisibility performance	32

4.4	Quality of the extracted watermark	34
4.5	Performance comparison with existing research	39
4.5.1	Various attacks comparison	40
4.6	Summary	45
CHAPTER 5 CONCLUSION		47
5.1	Introduction	47
5.2	Research contributions	47
5.3	Conclusion	48
5.4	Future recommendation	49
REFERENCES		51
APPENDIX A LIST OF TESTING IMAGES FROM INTERNET with sizes of 512x512		54
APPENDIX B RESEARCH GANTT CHART		55

LIST OF TABLES

Table 1: Research Problem	3
Table 2: Optimized Watermarking Existing Research	11
Table 3: Analysis of the research	16
Table 4: Acronyms for several sorts of attacks	28
Table 5: List of host images to be tested	31
Table 6: Imperceptibility performances for different W1 sizes	31
Table 7: Invisibility performance	32
Table 8: Facing different type of attacks with W1 size of 64 x 64	33
Table 9: Robustness performance for image Lenna facing various attacks	34
Table 10: Extracted watermarks of W2	39
Table 11: Comparison with schemes in IWT-SVD research paper	40
Table 12: Comparison with schemes in IWT-SVD-MOACO research paper	42
Table 13: Comparison with DWT-HD-SVD research paper	44

LIST OF FIGURES

Figure 1: Optimization of Alpha Values	6
Figure 2: Integer Wavelet Transform	8
Figure 3: Flowchart of research design	21
Figure 4: Watermark images (A: W1, B: W2)	22
Figure 5: Watermark embedding process	22
Figure 6: Watermark extraction process	23
Figure 7: NC values for several parameters, including JPEG compression (A) and (B). Compression for JPEG 2000 (C) Sharpening Attack (D), Gaussian Low Pass Filter (E), Median Filter (F), and Gaussian Noise	37
Figure 8: Line graph comparison with schemes in IWT-SVD research	41
Figure 9: Line graph comparison for schemes in IWT-SVD-MOACO research	43
Figure 10: Line graph comparison with DWT-HD-SVD research	45

LIST OF ABBREVIATIONS

SVD	Singular Value Decomposition
DCT	Discrete Cosine Transform
DWT	Discrete Wavelet Transform
HD	Hessenberg Decomposition
IWT	Integer Wavelet Transform
CWT	Continuous Wavelet Transform
PSNR	Peak Signal-to-Noise Ratio
SSIM	Structural Similarity Index
NC	Normalised Cross-correlation
PSO	Particle Swarm Optimization
SGOA	Social Group Optimization Algorithm
FA	Firefly Algorithm
OA	Optimization of Alpha
ABC	Artificial Bee Colony
QF	Quality Factor
CR	Compression Ratio

CHAPTER 1

INTRODUCTION

1.1 Background

The speedy development of digital technology has made it simpler to access digital information such as social media and any type of multimedia. As a result, more people are becoming aware of how simple it is to replicate the data. Perfect copies are simple to make, which could result in widespread unauthorised copying especially on images [1]. When we talk about images, it has a strong relation with the artists who are the creators of them. Nowadays, we can barely see any artists who sell their artwork physically. Most of them has moved their artwork into images which could be view and sold online. But physical artwork and online image has a big difference. It is hard to identify who is making the changes when putting the image online. Numerous solutions are being developed to prevent unauthorised copying as a result of this worry over copyright issues. Use of digital watermark is one of these solutions. In simple terms, copyright is the legal right given to the creators of an original work to control its reproduction. The authors of a work are the only ones who have the exclusive ability to duplicate it, unless they give permission to others [2]. Digital watermark or optimized watermark has the same definition which is to embedded data that identifies the creator or owner of digital intellectual property. A digital watermark monitors how digital media is used online and issues a cautionary note about possible illicit access. Information concealment, data embedding, forensic watermarking, and watermarking are other names for digital watermarks [3]. Digital watermarking is similar to steganography in that it involves hiding sensitive information within a regular file or message to avoid detection. Digital watermark can be visible or hidden. By altering the digital data's contents, the information that needs to be concealed is inserted, making it possible to locate the original owner or, in the event of unlawful copying. To infer something about the data, this digital watermark can be found or retrieved afterwards. Somehow, the digital watermark is not

totally safe if there is no extra protection added. Watermarking is susceptible to various types of attacks. The attacks aim to remove, alter, or otherwise compromise the watermark in the image. [4]. Therefore, it is also crucial to always prioritise security in the digital watermarking. Digital watermarking can be implemented using a variety of methods, including Singular Value Decomposition (SVD), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT). This research aims to utilize Hessenberg Decomposition (HD), SVD and Integer Wavelet Transform (IWT) as the methods of choice. IWT is a wavelet analysis algorithm that converts integers to integers and can be inverted. IWT is better appropriate for lossless data-compression applications and is computationally quicker and memory-efficient than the continuous wavelet transform (CWT). The calculated integer coefficients can be used by the IWT to perfectly reconstruct an integer signal [5]. The integer variants are more easily invertible in finite precision arithmetic than the traditional DWT. Because the cover media requires integers, these transformations are highly helpful in data concealing applications. Overall, the use of IWT in optimized watermarking allows for more accurate and robust watermarking, as the wavelet coefficients of an image can provide more detailed information about the data compared to other methods. A potential attacker may find it more challenging as a result to remove or change the watermark without affecting the quality of the image. Meanwhile, HD is particularly useful in image watermarking because it transforms the original image into a form that is less sensitive to perturbations caused by attacks such as rotation, scaling, and translation [6]. SVD is a technique used in image processing to break down an image matrix into three separate matrices. These matrices can be used to represent the image in a new coordinate system, which can be useful for image compression and feature extraction. It also can be used to denoise images by removing small singular values considered as noise and reconstruct the image by using the remaining large singular values [7].

1.2 Problem Statement

The first problem in image watermarking is to determine the suitable alpha value that maximizes the robustness of the watermark while minimizing its impact on the host image quality. Achieving an optimal alpha value is crucial as it directly influences the trade-off between robustness and visual fidelity. The challenge lies in finding the right

balance, where the watermark can withstand various attacks and signal processing operations while maintaining perceptual transparency. This problem requires developing a comprehensive framework that investigates the effects of different alpha values on robustness metrics (e.g., normalized correlation) and perceptual quality indicators (such as the structural similarity index and peak signal-to-noise ratio) to identify the optimal alpha value for watermark embedding and extraction. The second problem is related to the limitation of existing watermarking techniques in accommodating multiple sizes of watermarks. Many watermarking methods are designed to handle a specific watermark size, which restricts their applicability in scenarios where multiple watermark sizes need to be supported. The challenge here is to develop an adaptive approach that can efficiently embed and extract watermarks of various sizes without sacrificing robustness or requiring redundant computations. This problem requires investigating novel strategies to dynamically adjust the embedding and extraction processes to cater to different watermark sizes while ensuring reliable detection. The summary of the aforementioned claims is shown in Table 1.

Table 1: Research Problem

No	Research Problem
1	Find the suitable alpha value that maximizes the robustness of the watermark while minimizing its impact on the host image quality.
2	Limitation of existing watermarking techniques in accommodating multiple sizes of watermarks.

1.3 Objectives

The objective of this research are:

- i. To study the current methods of optimized image watermarking using HD and SVD in IWT domain.
- ii. To develop optimized image watermarking using HD and SVD in IWT domain to achieve high robustness and maintain imperceptibility.
- iii. To evaluate the results for optimized image watermarking using HD and SVD in IWT domain in terms of imperceptibility and robustness.

1.4 Scope

This study provides optimized image watermarking approach on the image's content. The research boundary is covered in the scope. The extent of a study defines the depth and breadth of the research field that will be examined throughout the work and outlines the limitations within which the examination will be conducted. The boundaries of the study are as follows:

- i. Two grayscale image for watermark image are used in this study with 3 sizes (64x64, 128x128, 256x256).
- ii. 8 different 512x512 pixels of grayscale images for the host image are used in this study.
- iii. The quality of the watermarked image was evaluated using PSNR and SSIM.
- iv. The proposed scheme's resistance to various image attacks was evaluated using the normalised cross-correlation (NC) metrics.
- v. The experiments for the research will be conducted using MATLAB R2022b on a computer with an AMD Ryzen 5 3600 6-Core Processor @ 3.6 GHz and 16 GB of RAM, running on the Windows 10 operating system.

1.5 Thesis Organization

This thesis is divided into five chapters. The first chapter will introduce the project, the second chapter will present an overview and discussions of the literature review, the third chapter will detail the methodology to be used, the fourth chapter will focus on the testing, results, and implementation, and the final chapter will summarize the conclusions of the entire thesis.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter contains information about the proposed digital watermarking in general. It outlines the current issue or past scholars' work on a solution. This chapter goes into great length on the techniques they used or the technology that might be applied to their study of digital watermarking. In order to evaluate and analyse the relevant studies on the study topics, the benefits and drawbacks of the current watermarking systems are also included. Section 2.2 presents the research from past and current scholars that is from 2017 to this year, 2023. The existing research that has been done is using optimized watermarking method. The experimental results of the current watermarking systems are also identified in this chapter in terms of performance, embedding capacity, optimal threshold, imperceptibility, robustness, various types of attacks, and security analysis.

2.2 Optimized watermarking method

Optimized watermarking is a technique used to embed a secret message, or watermark, into a digital image or video for the purpose of copyright protection or authentication. The goal of optimized watermarking is to achieve a balance between robustness, which refers to the ability of the watermark to withstand various attacks and modifications, and imperceptibility, which refers to the ability of the watermark to remain undetected by human observers. There are various techniques used in optimization algorithms such as Particle Swarm Optimization (PSO), Social Group Optimization Algorithm (SGOA), and Firefly Algorithm (FA) [9].

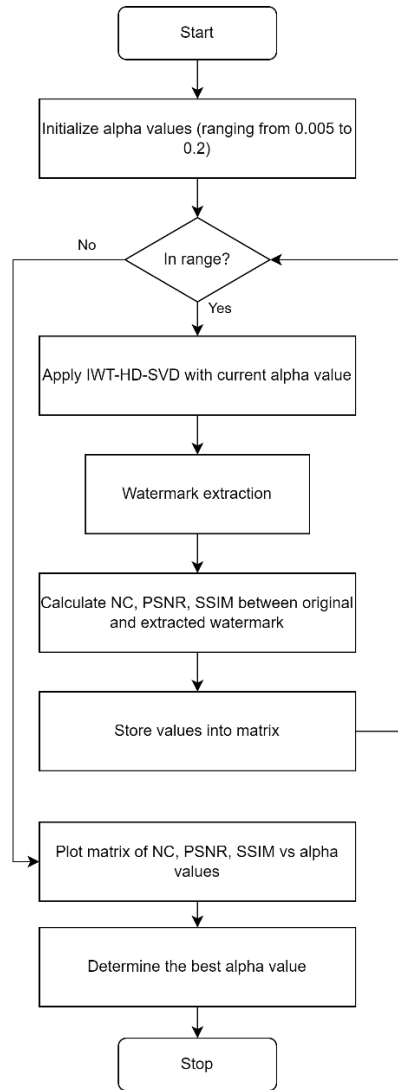


Figure 1: Optimization of Alpha Values

In the proposed scheme, **optimization of alpha (OA)** value is used. Alpha value represents the amount of strength of the watermarking signal. Calculation was made for NC, PSNR and SSIM between the original watermark and the extracted watermark for different alpha values and different types of attacks. The purpose is to evaluate the performance of the watermarking process for different alpha values and types of attacks by calculating the NC, PSNR and SSIM. By analyzing the variations for different alpha values, one can determine the optimal alpha value that maximizes the correlation between the original and extracted watermarks. If the alpha value is too high, then the watermark will be visible and degrade the quality of the image. On the other hand, if the alpha value is too low, then the watermark will not be robust enough to withstand various attacks. Therefore, an optimized alpha value is essential to achieve a balance between robustness and imperceptibility.

2.3 Embedded sub-band

In image processing, subband refers to a portion of an image that has undergone decomposition using a transform such as the IWT. IWT is a mathematical transformation technique that can decompose an image into different frequency sub-bands. The LL subband (Low-Low) contains the lowest frequency components of an image, and it is the subband that corresponds to the coarsest level of decomposition in IWT. The LL subband is often chosen for watermark embedding due to its high energy content, which means that it contains most of the image's essential information.

Moreover, the LL sub-band is less sensitive to image processing operations such as filtering, compression, and geometric transformations, making it a suitable choice for embedding the watermark without severely affecting the image's quality. This robustness to image processing attacks makes the LL sub-band a popular choice for watermark embedding in image watermarking [10].

2.4 Watermark Security

Security matters in image watermarking because it is a way to protect the ownership and copyright of digital images. Without security measures, it would be easy for unauthorized users to copy, distribute, or use the image without permission. The watermark image also must be protected against unauthorised users and attackers. In this study, SVD will be the choice for security wise. Using SVD before embedding a watermark provides a security benefit by making it more difficult for an attacker to remove the watermark from the image. The SVD process decomposes the watermark image into its constituent singular values and vectors. These singular values and vectors contain the important information of the watermark image and by embedding them into the host image, the watermark is effectively hidden.

If an attacker attempts to remove the watermark, they will need to identify the embedded singular values and vectors, which can be challenging without knowledge of the original watermark image and the specific embedding process used. Additionally, even if an attacker is able to identify the embedded singular values and vectors, removing them without causing noticeable distortion in the host image can be difficult, thus making the watermark more robust. Therefore, incorporating SVD before embedding a watermark can provide an added layer of security to the watermarking process.

2.5 Transform Domain

2.5.1 Integer Wavelet Transform (IWT)

In the study of digital watermarking, wavelet transform was often utilised. Decimals would be produced using the standard wavelet transform. It was unable to fully undo the extraction once the watermark had been placed. The integer-integer wavelet transform based on the lifting strategy was employed in this study to avoid these issues. The system made sure that during deconstruction and reconstruction, the carrier picture did not cause data loss. It is carried out by altering DWT in order to make use of the lifting system as described by Sweldens [11]. In comparison to DWT, it is more efficient, requires less effort to invert, and does not call for any auxiliary memory. It enables complete invertibility while maintaining arithmetic with limited precision. In addition, the integer wavelet transform may be carried out on a digital computer using just three operations: addition, subtraction, and shift. These three operations make up the transform. Because of this characteristic, it is advantageous in comparison to other discrete wavelet transforms [12].

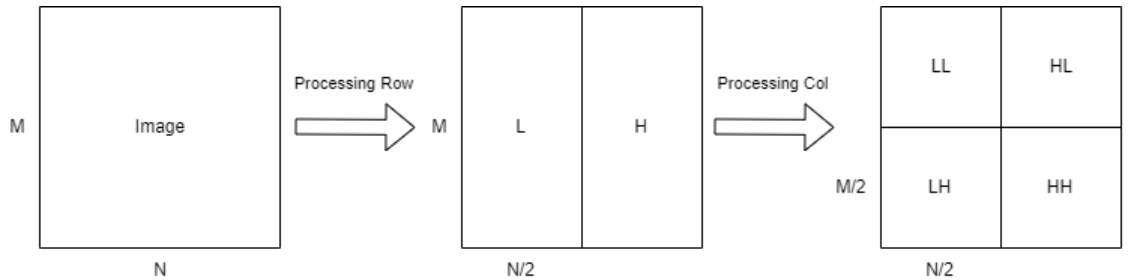


Figure 2: Integer Wavelet Transform

At the first level, IWT provides two subbands: high frequency (HF) and low frequency (LF). Approximation (LL), horizontal (LH), vertical (HL), and diagonal are all included in the second level of decomposition (HH). The equation as below.

$$HF = C_{odd} - C_{even}$$

$$LF = C_{even} + \left[\frac{HF}{2} \right]$$

C_{odd} and C_{even} are, respectively, odd and even column pixels.

$$\begin{aligned}
LH &= LF_0 - LF_e \\
LL &= LF_e + \left[\frac{LH}{2} \right] \\
HL &= HF_0 - HF_e \\
HH &= HF_e + \left[\frac{HL}{2} \right]
\end{aligned}$$

The odd row of LF is LF_0 , the even row is LF_e , the even row of HF is HF_0 , and the odd row of HF is HF_e [13].

The reason that the watermark is typically embedded in the LL subband is due to the nature of the lifting scheme and the properties of the LL subband. The lifting scheme is a specific type of wavelet transform that uses integer coefficients to perform the decomposition, which makes it computationally efficient and well-suited for real-time applications. The lifting scheme is also well-suited to lossy compression, as it preserves the low-frequency components of the image better than other wavelet transforms.

2.5.2 Singular Value Decomposition (SVD)

Singular value decomposition (SVD) is a powerful mathematical tool that can be used in image processing to analyse and manipulate images. SVD is a method for breaking down a matrix into three parts, which are the left-singular vectors (U), the singular values (S), and the right-singular vectors (V).

The matrix used in SVD is usually the image matrix, which is a 2-dimensional array of pixels. Each pixel in the image is represented by a value (e.g., a grey level or a color value) and these values are arranged in a matrix. By using SVD to decompose the image matrix, we can obtain the following three matrices:

$$D = USV^T$$

Left-singular vectors matrix (U) - This matrix contains the eigenvectors of the image matrix. Each column of the matrix represents an eigenvector and represents a direction in which the image data varies. These eigenvectors can be used to represent the image in a new coordinate system, which can be useful for image compression and feature extraction.

Singular values matrix (S) - This matrix holds the square roots of the eigenvalues of the image matrix, known as singular values. These values indicate the extent of variation of the image data in relation to each eigenvector. The larger the singular value, the more significant the eigenvector is in describing the image.

Right-singular vectors matrix (V) - This matrix holds the right-singular vectors of the image matrix. Each column in the matrix represents one right-singular vector. These vectors can be utilized to rebuild the original image from the compressed representation that resulted from using the left-singular vectors and singular values.

SVD can be used to lower the dimensionality of the image matrix and generate a compressed version of the image. This is achieved by retaining only the most significant singular values and the left and right-singular vectors that correspond to them. This compressed representation still captures the most important features of the image, while discarding the less important details. This is useful for image compression and feature extraction [14].

2.5.3 Hessenberg Decomposition (HD)

Hessenberg decomposition is a matrix factorization technique that transforms a matrix into an upper Hessenberg matrix, which has the property that all elements below the first subdiagonal are zero. In image watermarking, HD is often used to reduce the computational complexity of SVD-based watermarking methods. Given an input matrix A, HD produces two matrices Q and H such that:

$$A = Q \times H \times Q^T$$

where Q is an orthogonal matrix and H is an upper Hessenberg matrix. Mathematically, this can be expressed as:

$$H = Q \times A \times Q^T$$

where Q^T is the transpose of Q.

HD can be computed efficiently using Householder reflections or given rotations. By using HD, the computational complexity of the watermarking process can be reduced, as HD only requires $O(n^3)$ operations. This makes HD particularly useful for large images

or for real-time applications where computational efficiency is important. Once HD is obtained, watermarking can be performed by modifying the elements of the matrix H. The watermark can be embedded by adding a small perturbation to the diagonal elements of H or by modifying the off-diagonal elements to encode the watermark information. The watermark can then be extracted by performing the reverse process of the embedding operation [6].

2.5.4 Hybrid Method

Hybrid method in image watermarking refers to the combination of different watermarking techniques to achieve better performance and robustness [15]. The idea behind a hybrid method is to use the strengths of different techniques to overcome the limitations of each individual method. For example, one technique may be good at providing robustness against image processing attacks, but not very good at providing imperceptibility. Another technique may provide good imperceptibility, but not very good robustness. By combining these two techniques, a hybrid method can provide both robustness and imperceptibility.

Hybrid methods can provide better performance than single methods, by combining the robustness and imperceptibility of different techniques. However, they also can be more complex to implement and may require more computational resources as what have been compared in **Chapter 2, Section 2.2**. The hybrid method that will be applied in this study is IWT-HD-SVD.

2.6 Existing System/Works

Table 2 shows the existing optimized watermarking research that consists of many hybrid methods such as DWT, DCT, SVD and many more. There is various optimization method used in the existing research such as Artificial Bee Colony (ABC), Multi multi-objective ant colony optimization The pros and cons for each research also been stated. Hence, summarization of each research is provided for easier understanding.

Table 2: Optimized Watermarking Existing Research

No	Author(s)	Method	Advantage	Disadvantage
----	-----------	--------	-----------	--------------

1	Nasrin M.Makbol, Bee Ee Khoo, Taha H. Rassem, Khaled Loukhaoukha [16]	IWT-SVD- MOACO	Optimal scaling factor. Improved robustness.	Complexity of implementation
2	Irshad Ahmad Ansari, Millie Pant, Chang Wook Ahn [17]	IWT-SVD- ABC	Simplicity of implementation. Ability to handle a large search space.	Slow convergence rate. Careful parameter tuning or the result will be worse.
3	Anurag Mishra, Charu Agarwal, Arpita Sharma, Punam Bedi [18]	DWT-SVD- FA	Optimize multiple parameters simultaneously.	Sensitivity to initialization and randomization.
4	Yong Guo, Bing- Zhao Li, Navdeep Goel [19]	DWT-QR-FA	High computing speed. Automatic regrouping.	Can be computationally expensive.
5	Neeraj Kumar Sharma, Subodh Kumar, Ankit Rajpal, Naveen Kumar [20]	MRFO- DTCWT- SVD	Achieving a balance between durability and invisibility. High degree of watermark recoverability.	Inherently-slow, resulting that it cannot be applied in real-time applications.
6	A. Mohan, A. Anand, A.K Singh, R.	DWT-HD- SVD-PSO	High robustness. Balances the	Computational complexity.

	Dwivedi, B. Kumar [21]		trade-off between robustness and imperceptibility.	Not suitable for real-time applications.
7	Dilip Golda, Prabha B., Murali K., Prasuna K., Sai Sri Vatsav, Sowmika Adepu [22]	DWT-SVD- SGOA	Provide high robustness to various attacks. Efficient optimization of the scaling factors.	Require a significant amount of time and resources. High computation requirements.
8	Pranab K.Muhuri, Zubair Ashraf, Swati Goel [23]	IWT-PSO	Effective in solving a wide range of optimization problems.	Computationally expensive.

2.6.1 Explanation

Method (1): IWT-SVD-MOACO is a novel technique for image watermarking that addresses the issue of false positives while meeting all the requirements of watermarking. Unlike other methods, it uses the S and V matrices of the watermark as secret keys, embedding the S singular vector into the singular values of the host image. This approach also generates an additional secret key from the watermarked image during embedding, enhancing security and eliminating false positive problems. Moreover, the method employs multi-objective ant colony optimization (MOACO) to determine optimal scaling factors, including multiple zooming factors, to achieve a balance between robustness and imperceptibility.

Method (2): IWT-SVD-ABC introduces a new solution. It applies IWT to the host image, followed by SVD, to achieve strong robustness. The singular values of the transformed image are utilized for watermark embedding. Additionally, the quality of watermarking is further improved by optimizing the scaling factor through the artificial bee colony (ABC) algorithm.

Method (3): DWT-SVD-FA. The researchers propose an optimized image watermarking technique that employs DWT and SVD. The binary watermark's singular values are embedded into the singular values of the LL3 sub-band coefficients of the host image, utilizing several scaling factors (MSFs). To optimize the MSFs, a new Firefly Algorithm is introduced, with an objective function that combines imperceptibility and robustness.

Method (4): DWT-QR-FA presents a new approach to image watermarking that incorporates the firefly algorithm (FA) within the domain of discrete wavelet transform (DWT) and QR transform. FA is an optimization algorithm inspired by the flashing behavior of fireflies, which are attracted to brighter fireflies in their vicinity. This algorithm offers two notable benefits: local attractions and automatic regrouping. By integrating FA into the DWT-QR transform domain, the proposed method aims to enhance the effectiveness of watermarking.

Method (5): MRFO-DTCWT-SVD. The authors introduce MantaRayWmark, an adaptive image watermarking technique that uses Manta Ray Foraging Optimization (MRFO). The method balances robustness and imperceptibility by employing multiple embedding strengths. The proposed embedding process involves converting the image using 4-level Dual-Tree Complex Wavelet Transform (DTCWT) and then applying Singular Value Decomposition (SVD) on the approximated sub-band matrix. In order to avoid false positives, the method adds a binary watermark to the PC matrix. A ConvNet-based geometric correction approach is used to evaluate the proposed method's resistance to geometric attacks. SVD-based hashing is used for watermark image authentication, while the transposition cipher is used for watermark scrambling and security. Despite geometric and image processing attacks, MantaRayWmark demonstrates excellent watermark recoverability from the watermarked image, indicating its resilience.

Method (6): DWT-HD-SVD-PSO introduces a novel image watermarking algorithm that aims to enhance both invisibility and robustness simultaneously. The algorithm combines various transform domain techniques to identify appropriate coefficients for embedding data. To strike a balance between robustness and invisibility, the algorithm employs a fusion of particle swarm optimization (PSO) and the Firefly algorithm to compute optimal embedding factors. The watermark is then scrambled using a step space-filling curve and embedded into the wavelet domain of the host image using the computed optimal factor. Additionally, selective encryption is applied to the original host image, adding an extra layer of security with minimal computational overhead.

Method (7): DWT-SVD-SGOA. The authors propose a novel approach to watermarking that combines SVD, DWT, and SGOA. The SGOA algorithm is used to determine the appropriate coefficient for watermarking based on dynamic thresholding of the SVD and DWT information. The goal is to ensure that the watermarked image does not deviate significantly from the original image. SGOA is a popular evolutionary computing tool that has been successfully applied to image processing problems.

Method (8): IWT-PSO presents a novel steganography approach that utilizes Particle Swarm Optimization (PSO) in conjunction with Integer Wavelet Transform (IWT) for encoding secret data into substituted forms. The method incorporates an optimal pixel adjustment procedure to minimize distortion and improve perceptual transparency. By embedding the secret data into image wavelet coefficients, this technique enhances imperceptibility, security, and robustness. The research paper explores the application of PSO in three different image steganography techniques, namely LSB substitution, Discrete Wavelet Transform (DWT), and Integer Wavelet Transform (IWT).

2.7 Analysis/Comparison of Existing Systems

2.7.1 Analysis of the proposed optimized watermarking

Table 3 is the analysis of the proposed optimized watermarking in terms of the chosen embedding sub-bands, optimization algorithm, watermark action, host image size, watermark image size and type.

Table 3: Analysis of the research

Activities	Methods								
	IWT-SVD-MOACO	IWT-SVD-ABC	DWT-SVD-FA	DWT-QR-FA	MRFO-DTCWT-SVD	DWT-HD-SVD-PSO	DWT-SVD-SGOA	IWT-PSO	Proposed Scheme
Embedding sub-bands	LL	LL + LH + HL	3 level DWT: LL3	LL: 4 × 4 blocks	4 level DTCWT: LL4	HL	3 level DWT: LL3	HH	LL
Optimisation Algorithm	ACO	ABC	FA	FA	MRFO	PSO	SGOA	PSO	OA

Watermark action before embedding	SVD	-	SVD	-	Scrambled using transposition cipher	Step space-filling curve scrambling	-	Encryption using matrix M	SVD
Host image size	512×512	512×512	256×256	512×512	512×512	512×512	512×512	512×512	512×512
Watermark size	256×256	256×256	32×32	64×64	512×512	256×256	256×256	256×256	256×256 , 128×128 , 64×64
Watermark image type	Grayscale	Grayscale	Binary	BIT	Binary	Grayscale	Grayscale	Grayscale	Grayscale

2.8 Measurement of imperceptibility

Imperceptibility measurement is a method used to evaluate the similarity between the watermarked image and the original image. There are various metrics that can be used for this purpose, such as the Peak Signal-to-Noise Ratio (PSNR) and the Structural Similarity Index (SSIM).

- Peak Signal-to-Noise Ratio (PSNR): PSNR is a widely used metric that calculates the ratio of the peak signal power to the noise power in an image. It is defined as:

$$PSNR = 10 \log \frac{(255)^2}{MSE}$$

where MSE is the Mean Squared Error between the original image and the watermarked image and 255 is the highest possible value of a pixel in the image. A higher PSNR value suggests that the watermarked image is more similar to the original image and therefore less perceptible. [24].

- Structural Similarity Index (SSIM): SSIM is a newer metric that takes into account both the luminance and structural information of the image. It is defined as:

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)}$$

where x and y are the original and watermarked images, μ_x and μ_y are the mean values of the images, σ_x and σ_y are the variances of the images, σ_{xy} is the covariance between the images and c_1 and c_2 are constants used to stabilize the division in the formula. A value of 1 indicates that the images are identical and a value closer to 0 indicates that the images are dissimilar [25].

2.9 Robustness measurement

The ability of a watermark to remain intact in the face of various types of modifications, such as cropping, resizing, compression or filtering is referred to as robustness. Different methods can be used to evaluate the robustness of a watermark, such as Normalized Correlation (NC).

- Normalized Correlation (NC) is a measure of the similarity between the original image and the watermarked image. It is calculated using the following formula:

$$NC = \frac{\sum_{i=1}^M \sum_{j=1}^N W(i,j) \cdot W'(i,j)}{\sqrt{\sum_{i=1}^M \sum_{j=1}^N W(i,j)^2 \sum_{i=1}^M \sum_{j=1}^N W'(i,j)^2}}$$

The NC value ranges from -1 to 1, where 1 indicates a perfect match between the two signals, 0 indicates no correlation, and -1 indicates a perfect anti-correlation. NC is often used in image registration applications to measure the similarity between two images. By calculating the NC between two images, it is possible to determine how well the images match up with each other and to estimate the transformation parameters required to align them.

CHAPTER 3

METHODOLOGY

3.1 Introduction

The previous chapter discussed a review of watermarking methods. This chapter is structured as follows: the research design is outlined in Section 3.2, the experimental setup is discussed in Section 3.3, the methods for embedding and removing watermarks are presented in Section 3.4, the process of creating an embedding watermark using IWT-HD-SVD is covered in Section 3.5, the evaluation of the watermarked image is explained in Section 3.6 and the chapter is summarized in Section 3.7.

3.2 General Research Design

An optimized watermarking method for copyright protection was suggested in this paper. The study approach was then developed to provide an optimized watermarking and enhance the image's resilience and imperceptibility.

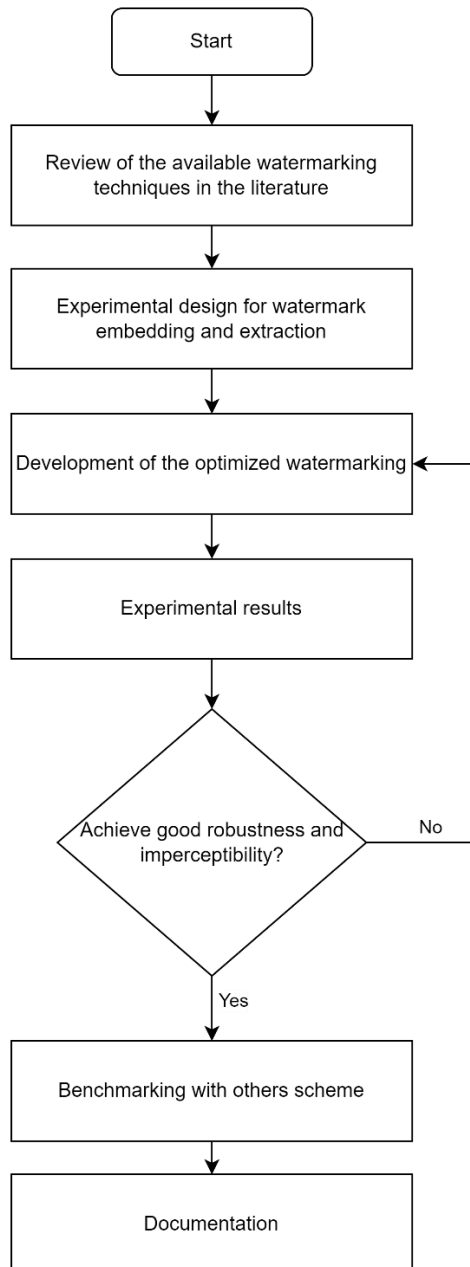


Figure 3: Flowchart of research design

3.3 Experimental Setup

This study will employ a proposed technique using MATLAB R2022b on a CPU AMD Ryzen 5 3600 6-Core Processor @ 3.6 GHz with 16 GB RAM, operated on a Windows 10 system. An experiment will be conducted, specifically an optimized image watermarking approach. The experiment will use 8 images of 512 x 512 pixels as the host for the watermarking process. Two images with sizes categorized as big (256x256), medium (128x128), and small (64x64) will be used for embedding into the host.



Figure 4: Watermark images (A: W1, B: W2)

3.4 Experimental Design

The experimental design contains only a single scheme. This system demonstrates its ability to achieve imperceptibility and resilience against many forms of attacks. Figures 5 and 6 depict the embedding and extraction processes for the proposed watermarking techniques respectively.

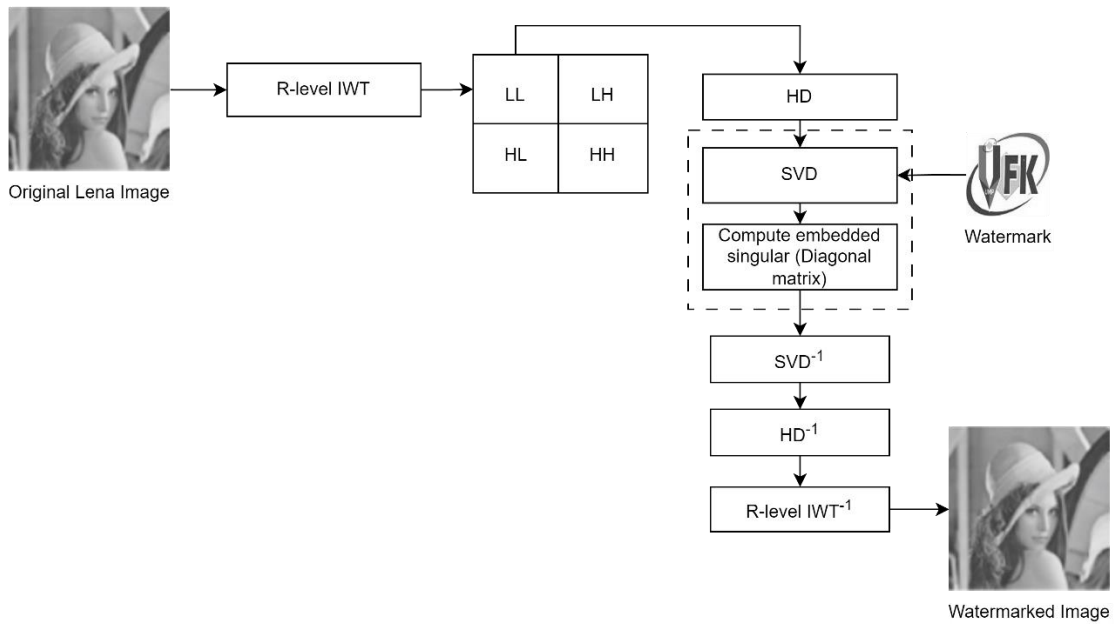


Figure 5: Watermark embedding process

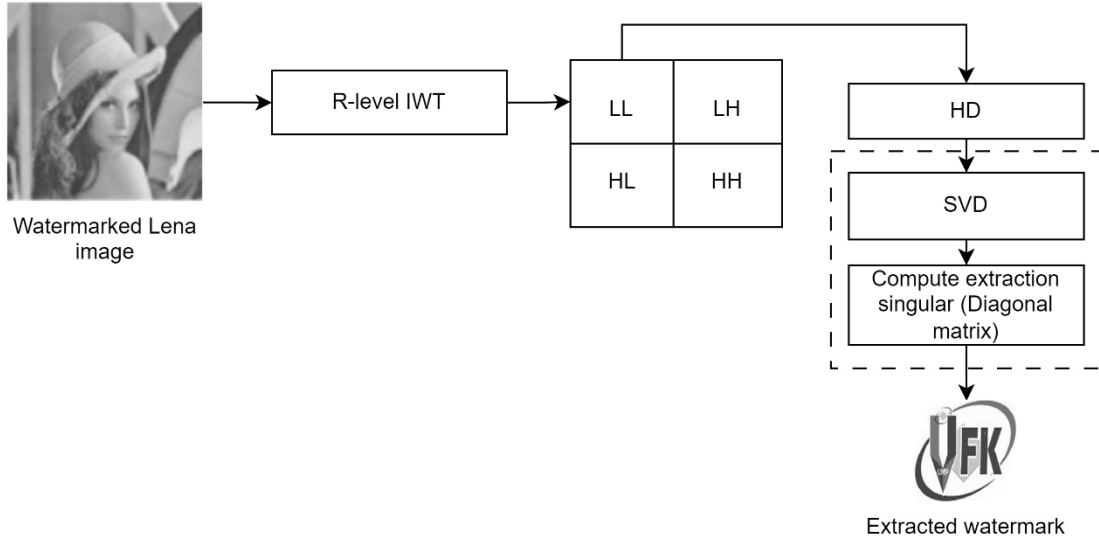


Figure 6: Watermark extraction process

3.5 Proposed Watermarking Scheme

The suggested optimized image watermarking technique is based on HD and SVD in IWT domain. The purpose of this technique is to increase the robustness and imperceptibility. The detailed procedure will be described in the next subsection.

3.5.1 Explanation of the IWT-HD-SVD optimized image watermarking technique

3.5.1.1 R-level IWT

The "R" represents the level of wavelet decomposition. It determines the number of times the IWT is applied to the host image. The value of "R" is chosen based on the size of the watermark logo. The smaller the watermark size, the higher the value of "R" and the more levels of wavelet decomposition are applied. This means that for a smaller watermark, the cover image is decomposed into more sub-bands, capturing more detailed frequency information. The reason for this choice is that when embedding a smaller watermark, it is desirable to utilize more levels of wavelet decomposition to spread the watermark information across multiple sub-bands and capture a wider range of frequencies. This helps to increase the robustness of the watermark against various attacks and improve its visibility in different frequency components of the cover image.

Therefore, for a watermark size of 256, "R" is set to 1, indicating a single level of wavelet decomposition. For a watermark size of 128, "R" is set to 2, indicating two levels of decomposition. And for a watermark size of 64, "R" is set to 3, indicating three levels of decomposition.

3.5.1.2 Chosen sub-band

LL sub-band

The reason that the watermark is typically embedded in the LL sub-band when using Integer Wavelet Transform (IWT) with a lifting scheme is due to the nature of the lifting scheme and the properties of the LL sub-band. The lifting scheme is a specific type of wavelet transform that uses integer coefficients to perform the decomposition, which makes it computationally efficient and well-suited for real-time applications. The lifting scheme is also well-suited to lossy compression, as it preserves the low-frequency components of the image better than other wavelet transforms.

The LL sub-band contains the low-frequency components of the image, which are typically less sensitive to changes in the image compared to the high-frequency components. When the watermark is embedded in the LL sub-band, it is less likely to be affected by image modification or degradation, making the watermark more robust. Additionally, the LL sub-band is often the largest of the sub-bands in terms of size, which means that there is more room to embed the watermark. This makes it easier to embed a large watermark or to embed the watermark at a low bit rate, which can improve the imperceptibility of the watermarked image.

Overall, embedding the watermark in the LL sub-band when using IWT with a lifting scheme is a trade-off between robustness and imperceptibility, and it can provide good results in many image watermarking applications [26].

3.5.1.3 Embedding part

Diagonal Matrix in SVD (S)

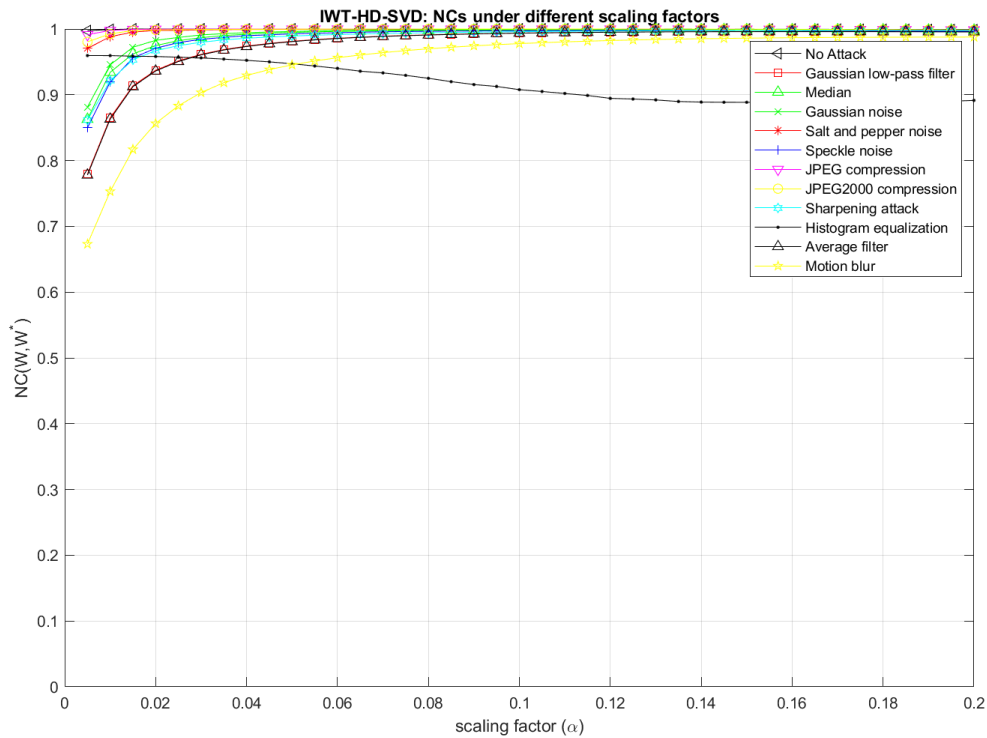
The watermark is embedded into the diagonal matrix $\hat{H}S_w$, which is obtained by adding the scaled watermark singular values S_w to the original host singular values $H S_w$. The choice of the diagonal matrix for embedding the watermark is motivated by

the fact that the singular values capture the magnitudes of the transformations performed by the SVD.

By modifying the singular values, we can introduce the watermark in a way that affects the perceptual characteristics of the host image [27]. The diagonal matrix is used because it allows independent modification of each singular value. Since each diagonal element represents the magnitude of a singular value, we can directly manipulate them to embed the watermark. By adding the scaled watermark singular values to the host singular values, we modify the relative importance of the singular values and introduce the watermark information.

The diagonal matrix also preserves the orthogonality of the left and right singular vectors, which ensures that the reconstructed image remains faithful to the original image structure. By modifying only the diagonal elements, the embedding process affects the magnitude of the singular values without altering the underlying structure represented by the singular vectors.

3.5.1.4 Optimized Alpha Values



The plotting of NC values is important in evaluating the performance of a watermarking scheme and selecting the optimal scaling factor (alpha) for different

attacks. NC values provide a quantitative measure of the similarity between the original watermark and the extracted watermark. Higher NC values indicate a stronger correlation and a better extraction of the watermark.

By plotting NC values against different scaling factors for various attacks, we can visually analyze the performance of the watermarking scheme under different conditions. This allows us to observe the trend and determine the scaling factor that yields the highest NC value for a particular attack. The process of optimizing scaling factor values involves systematically testing different scaling factors and evaluating their impact on the NC values. By plotting the NC values for different scaling factors, we can identify the scaling factor that maximizes the NC value for each specific attack. This optimization process helps to enhance the robustness and reliability of the watermarking scheme against different types of attacks.

For example, if we observe the plot of NC values against scaling factors for the histogram equalization attack, we can identify the scaling factor (e.g., 0.01) that results in the highest NC value. This indicates that using a scaling factor of 0.01 is most suitable for mitigating the effects of histogram equalization and achieving better watermark extraction. Hence, this experiment will choose **0.015** as the best alpha values that can withstand multiple attacks.

3.5.1.5 Watermark Embedding Process

There are few steps for the embedding process. Below are the steps provided.

Step 1: Apply the IWT to the cover image at the desired decomposition level (R).

Step 2: Apply the Hessenberg matrix transformation to the LL sub-band (Lowest Frequency) obtained from the wavelet decomposition.

Step 3: Perform Singular Value Decomposition (SVD) on the Hessenberg matrix (H).

Step 4: Perform SVD on the watermark logo (W).

Step 5: Compute an embedded singular value (\widehat{HSw}) by adding the scaled watermark singular values (S_w) to the Hessenberg singular values (HSw) with a scaling factor (α).

Step 6: Reconstruct the watermarked Hessenberg matrix ($H_{\hat{}}$) by using the inverse SVD with the modified singular values.

Step 7: Reconstruct a new low-frequency approximate sub-band ($LL_{\hat{}}$) based on the inverse Hessenberg matrix transformation (P) and the watermarked Hessenberg matrix ($H_{\hat{}}$).

Step 8: Perform the inverse wavelet transform (1-level IWT) to obtain the watermarked image ($watermarked_image$).

Result: Picture that has been watermarked

3.5.1.6 Watermark Extraction Process

There are few steps for the extraction process. Below are the steps provided.

Step 1: Decompose the watermarked host image (C) into four sub-bands (LLw , LHw , HLw , HHw) using the R -level IWT.

Step 2: Perform the Hessenberg matrix transformation (HD) on the LLw sub-band obtained from the wavelet decomposition.

Step 3: Perform Singular Value Decomposition (SVD) on the Hessenberg matrix (Hw).

Step 4: Calculate the extracted singular value ($Sw_{\hat{}}$) by subtracting the original Hessenberg singular values (HSw) from the modified singular values ($HSbw_{\hat{}}$) obtained from the SVD, divided by the scaling factor (α).

Step 5: Reconstruct the extracted watermark ($w_{\hat{}}$) by performing the inverse SVD using the original left singular vectors (Uw), the extracted singular values ($Sw_{\hat{}}$), and the original right singular vectors (Vw).

Result: An original watermark image

3.6 Evaluation of the watermarked image

3.6.1 Robustness and imperceptibility

The proposed image watermarking approach was evaluated by measuring its imperceptibility and robustness. As previously discussed in **Chapter 2, Section 2.6**, the invisibility of the watermarked image was assessed using metrics such as the SSIM index and PSNR. The watermarked image was also exposed to various types of attacks to evaluate its resilience, as described in **Chapter 2, Section 2.7**. The recovered watermark was then evaluated using the normalized cross-correlation (NC).

3.6.2 Various attack analysis

The performance of the proposed approach was evaluated by simulating various types of attacks on the watermarked photos and analyzing the retrieved watermarks. This included testing against image processing attacks, geometric attacks and compression. Many image processing techniques such as low-pass filter, sharpening, Gaussian noise, median filter, speckle noise, adjust, pepper and salt noise, histogram equalization, JPEG, JPEG XR and JPEG2000, as well as rotation, translation, and scaling attacks were simulated to evaluate the effectiveness of the proposed approach. In Table 4, the acronyms for several sorts of attacks are listed.

Table 4: Acronyms for several sorts of attacks

Abbreviation	Name of attacks
AD	Adjust
AF[3 3]	Average filter [3×3]
WF[3 3]	Wiener filter [3×3]
MF[3 3]	Median filter [3×3]
GN001	Gaussian noise 0.01
GN005	Gaussian noise 0.05
GLF[3 3]	Gaussian low-pass filter [3 3]
HE	Histogram equalization attack
MB	Motion Blur
JPEGQ50	JPEG (Q=40)
JPEGQ50	JPEG (Q=50)

JPEGQ70	JPEG (Q=70)
JPEGQ80	JPEG (Q=80)
JPEGQ90	JPEG (Q=90)
JPEG2000	JPEG2000 compression
SPN001	Pepper and salt noise 0.01
SPN005	Pepper and salt noise 0.05
PN	Poisson noise
SN01	Speckle noise 0.1
SN001	Speckle noise 0.01
SN005	Speckle noise 0.05
SH08	Sharpening 0.8
Rotation110	Rotation attack 110 degree
Rotation20	Rotation attack 20 degree
TR [20 20]	Translate attack (20 20)

3.7 Summary

This chapter discussed the overall research design, experimental setup, experimental design, development of embedding watermark, and evaluation of the embedded watermark. This chapter demonstrated in detail the process of IWT-HD-SVD optimized image watermarking technique. On eight images, the proposed scheme was examined. The trials utilised two watermark pictures, W1 and W2. PSNR and SSIM were used to test the imperceptibility of the watermarked image using the suggested technique. The robustness of the watermark recovery was further tested using NC for the suggested techniques. The suggested watermarking systems were evaluated against image processing, geometric, and compression attacks. Chapter 4 presents the experimental findings of the suggested strategy.

CHAPTER 4

RESULTS AND DISCUSSION






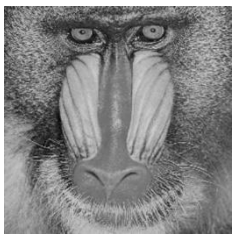


4.1 Introduction

The findings of this chapter's experiments on proposed scheme were presented, showcasing its imperceptibility, robustness, and the extraction's quality of watermarked image. The imperceptibility performance of the proposed scheme using different host images and watermark image sizes was demonstrated in Section 4.2, while the invisibility performance of the watermarked images was discussed in Section 4.3. Section 4.4 delved into the quality of the extracted watermark, and Section 4.5 provided a comparison of the offered methods's durability with other schemes based on NC values. Finally, Section 4.6 presented a summary of the experimental results obtained from the proposed scheme.

4.2 Performance of imperceptibility for various watermark images

The suggested embedding strategy will be evaluated in this experiment using eight host images, each with a size of 512x512 pixels. Two different watermark images were used: W1 for assessing the imperceptibility performance of the proposed strategy across various host images, with sizes categorized as big (256x256), medium (128x128), and small (64x64) and W2 for comparison with related works, as it is commonly used by many researchers. Table 5 provides a list of the eight host images that will be tested using this scheme. The figure below displays the two watermark images.

Table 5: List of host images to be tested

Elaine	Barbara	Airplane	Boat
			
Lenna	Mandrill	Peppers	Man
			

The proposed image watermarking process using HD and SVD in IWT domain will be applied to a list of host images. To assess the imperceptibility performance of the resulting watermarked images, we will use the PSNR and SSIM metrics. Each table will contain the evaluation results for different sizes of the watermark image. Specifically, table 6 will present the results for each embedding process.

Table 6: Imperceptibility performances for different W1 sizes

Host Image	Watermark	
	PSNR	SSIM
Big W1 size (256X256)		
Elaine	38.1709	0.9994
Barbara	38.1589	0.9992
Airplane	38.1014	0.9994
Boat	38.1889	0.9993
Lenna	38.0922	0.9994
Mandrill	38.1342	0.9993
Peppers	38.2070	0.9992
Man	38.1055	0.9993
Medium W1 size (128X128)		
Elaine	38.1829	0.9994
Barbara	38.1790	0.9992
Airplane	38.1142	0.9995
Boat	38.1998	0.9994
Lenna	38.1046	0.9994
Mandrill	38.1491	0.9994
Peppers	38.2214	0.9992







Man	38.1087	0.9993
Small W1 size (64x64)		
Elaine	38.2067	0.9994
Barbara	38.2188	0.9992
Airplane	38.1443	0.9995
Boat	38.2217	0.9994
Lenna	38.1340	0.9994
Mandrill	38.1718	0.9995
Peppers	38.2599	0.9992
Man	38.1121	0.9993







Despite using watermarks with varying sizes, the resulting PSNR and SSIM values remained largely unchanged. This suggests that the proposed scheme is suitable for use with different sizes of watermarks, as it maintains acceptable levels of PSNR and SSIM values during the image watermarking process. The average PSNR and SSIM values across all watermark sizes were 38 dB and 0.99, respectively.

4.3 Invisibility performance

In order to ensure the safety of information, it is essential that the watermarked host image is imperceptible to humans. Thus, measuring watermark invisibility is an important performance metric. To establish a baseline for the watermark's invisibility, the watermarked images must first be evaluated without undergoing any attacks. Table 7 displays two watermarked host images (Lenna and Peppers) at 256×256 , 128×128 , and 64×64 various W1 sizes and their corresponding extracted watermarks, along with the PSNRs, SSIMs, and NCs. According to [28], if the PSNR is higher than 37 dB, the watermarked image is regarded as acceptable and imperceptible to the human visual system.. Additionally, the difference between the watermarked image and the host image is minimal if the SSIM is higher than 0.93.

Table 7: Invisibility performance


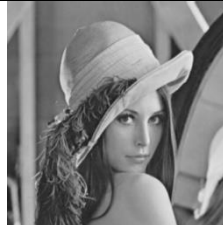


Watermark size	256x256		128x128		64x64	
	Host image	Lenna	Peppers	Lenna	Peppers	Lenna
Watermarked image						
PSNR (dB)	38.0922	38.2070	38.1046	38.2214	38.1340	38.2599
SSIM	0.9994	0.9992	0.9994	0.9992	0.9994	0.9992

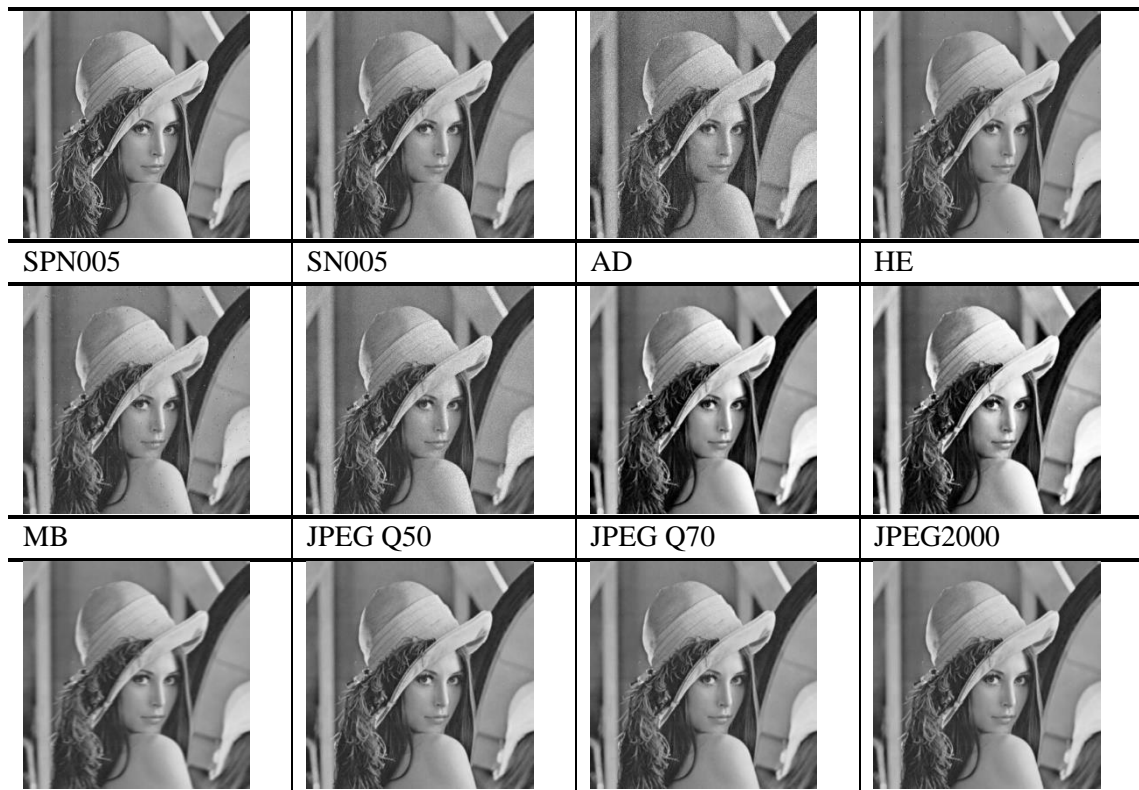
Extracted watermark						
NC	1	1	1	1	1	1

Based on table 8, the PSNR values indicate that the watermarked images have a high level of imperceptibility, with values ranging from 38.09 dB to 38.26 dB. Similarly, the SSIM values are also high, ranging from 0.9992 to 0.9994, which indicates that the watermarked images have a small difference with the host images. Additionally, the NC values are all equal to 1, which indicates that the extracted watermark is identical to the original watermark, demonstrating the high robustness of the proposed scheme. Overall, the results suggest that the proposed scheme is effective in achieving imperceptibility and robustness in the image watermarking process.

It is essential to assess the resilience/robustness of the suggested watermarking technology after making sure the watermark is imperceptible. Resilience/robustness refers to the ability of the system to withstand changes without compromising its initial stability. Robustness in the context of picture watermarking refers to the capacity to recover watermarks from host images that have been attacked in various ways. In this study, the quality of the extracted watermarks was evaluated under different attack scenarios, and the results were objectively evaluated. Specifically, the watermarked images were subjected to attacks with a 64 x 64 watermark, and the quality of the extracted watermarks was analysed. The same procedure was repeated for watermarks with sizes of 256 x 256 and 128 x 128, and the extracted watermarks and their corresponding values were listed in the next section. Table 8 shows the visual quality of the watermarked images that facing different types of attacks.

Table 8: Facing different type of attacks with W1 size of 64 x 64

WF [3 3]	GLF [3 3]	MF [3 3]	AF [3 3]
			
SH08	GN001	GN005	SPN001


















































4.4 Quality of the extracted watermark

In Table 9, it is evident that the extracted watermarks not only possess excellent visual quality but also exhibit good NC values. For the three watermark sizes tested, the NCs of all attacks, except for the Adjustment attack, are greater than 0.9. As the watermark size decreases, the NC value tends to improve. However, the NC value drops significantly for the Adjustment attack, ranging from 0.87 to 0.89. The Histogram Equalization attack slightly reduces the NC value to the range of 0.93 to 0.94, but it is still acceptable. The Motion Blur attack shows inconsistent NC values ranging from 0.94 to 0.99 as the watermark size decreases. Despite the slightly blurred extracted watermarks, the main information is still recognizable. The suggested watermarking technique exhibits a very good sign against the JPEG attack, with all NC values ranging from 0.9997 to 0.9999. It follows that the suggested watermarking technology is quite resistant to different kinds of attacks.

Table 9: Robustness performance for image Lenna facing various attacks

Attacks	256x256		128x128		64x64	
	Extracted Watermark	NC	Extracted Watermark	NC	Extracted Watermark	NC

WF [3 3]		0.9954		0.9987		0.9996
GLF [3 3]		0.9812		0.9949		0.9990
MF [3 3]		0.9947		0.9990		0.9998
AF [3 3]		0.9807		0.9947		0.9990
SH08		0.9893		0.9961		0.9991
GN001		0.9963		0.9997		0.9994
GN005		0.9723		0.9970		0.9996
SPN001		0.9994		0.9999		0.9999
SPN005		0.9937		0.9994		0.9997

SN005		0.9924		0.9994		0.9999
AD		0.8839		0.8791		0.8731
HE		0.9471		0.9439		0.9366
MB		0.9454		0.9703		0.9919
JPEG Q50		0.9999		0.9999		0.9999
JPEG Q70		0.9997		0.9999		0.9999
JPEG200 0		0.9997		0.9999		0.9999
Average		0.9794		0.9857		0.9873

To fully assess the robustness of the proposed method, it is necessary to test its performance against dynamic parameters. Hence, experiments were conducted using dynamic parameters and the results are presented in Figure below.

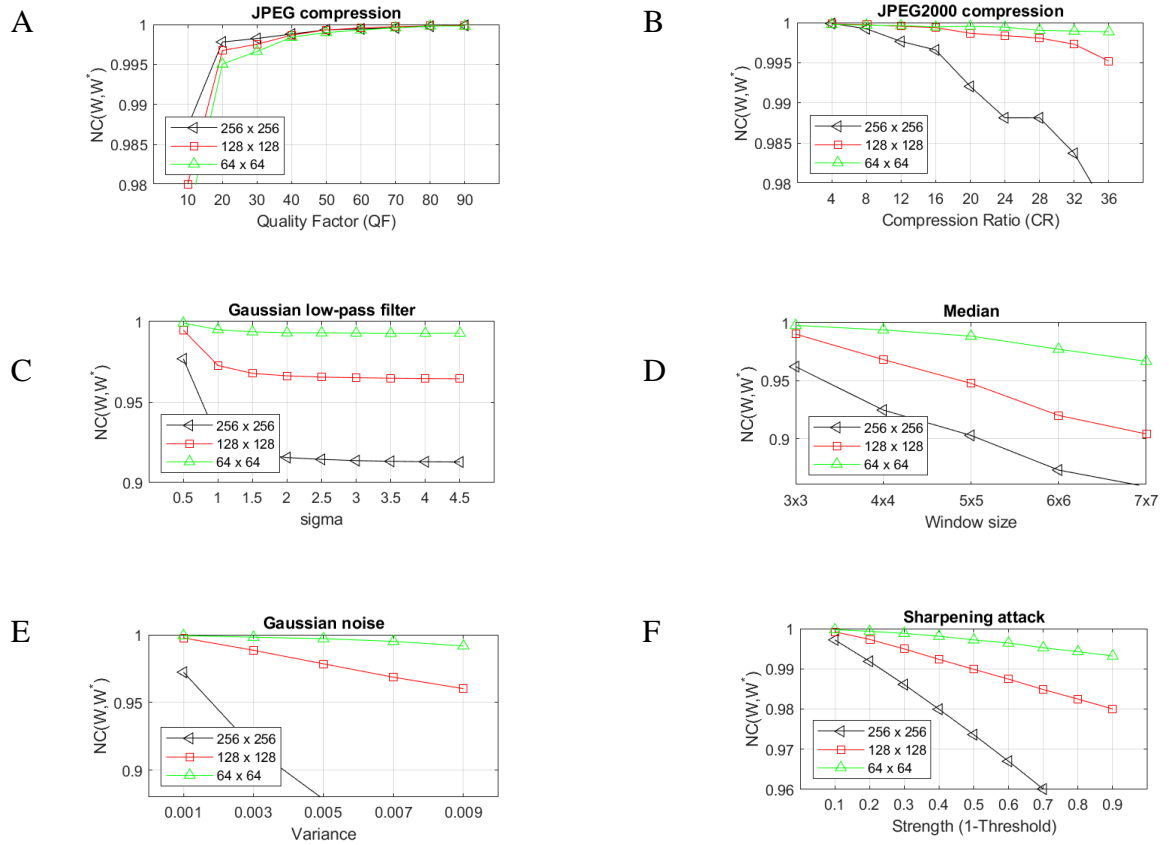


Figure 7: NC values for several parameters, including JPEG compression (A) and (B). Compression for JPEG 2000 (C) Sharpening Attack (D), Gaussian Low Pass Filter (E), Median Filter (F), and Gaussian Noise

Specifically, Figure 8(A) demonstrates the method's resistance to JPEG compression resilience with varying quality factors (QF) ranging from 10 to 90 with a step size of 10. It is important to note that the QF reflects the strength of compression, and as the QF decreases, the level of compression increases. Although there is a significant drop in the metrics, the NC values, which are shown on the Y-axis of the figure, remain within an acceptable range of 0.98 to 1. Even at the lowest QF of 10, all the NC values are higher than 0.8, indicating that the proposed method is still effective under heavy compression. Figure 8(B) presents the results of the tests carried out under JPEG2000 compression attack, where the compression ratios (CRs) were varied from 4 to 36 with a step of 4. As expected, the retrieved watermarks' NC values decreased as the CR increased, indicating a degradation in the resistance of the suggested technique to this kind of attack. Interestingly, the watermarks with sizes of 64x64 and 128x128 maintained their NC

values above 0.9995 even when the CR value was set to 36, while the largest watermark size showed a significant drop in the NC value, falling below 0.9.

Figure 8(C) illustrates the suggested method's robustness against a Gaussian low-pass filter assault. The outcomes show that the approach can keep stability across all watermark sizes. The NC values of all watermarked images remain above 0.9, which is considered very good, even when different sigma sizes of GLF are applied. In Figure 8(D), the robustness of the proposed method against median filtering attack is evaluated by varying the window size from 3x3 to 7x7 with a step of 1x1. The test results show that the NC values of Gaussian low-pass filter are all above 0.85 for the three different watermark sizes. Notably, the NC values for the 64x64 watermark are almost reaching 1, indicating a high degree of robustness against median filtering. Additionally, the NC values for the median filtering attack attain 0.99 for the 64x64 watermark as well. However, for the largest watermark size of 256x256, some NC values are relatively low, with an NC value of 0.85 obtained when the window size is 7x7.

The experiments under Gaussian noise attack in Figure 8(E) shows that the proposed method has good robustness for the watermark sizes of 64x64 and 128x128. The NC values are above 0.96 for both sizes. However, for the largest watermark size, the NC values are very low when the variance reaches 0.005, with the lowest NC value being 0.64 when the variance reaches 0.009. This indicates that the largest watermark size is not robust enough to withstand higher levels of Gaussian noise attack. Finally, Figure 8(F) which is sharpening attack, with threshold values ranging from 0.1 to 0.9 with a step of 0.1. The NC values for the small and medium watermark sizes remain stable and higher than or equal to 0.96, even when the threshold value is as high as 0.9. However, the big watermark size exhibits poor robustness with an NC value dropping significantly to 0.82 when the threshold value is increased to 0.7 and 0.9.

A high NC number denotes strong resistance to various attacks, such as the sharpening attack, JPEG compression, and JPEG2000 compression, regardless of the watermark size. However, the biggest watermark size showed some weakness in terms of robustness against certain attacks, such as JPEG2000 compression, Gaussian Noise, and sharpening attack. Therefore, it is recommended to use smaller watermark sizes to ensure high robustness. Overall, the proposed watermarking method demonstrated good invisibility and robustness against various attacks.

4.5 Performance comparison with existing research

The attacks mentioned earlier were also performed on the watermarked Lenna image using another watermark named 'W2'. This was done to maintain fairness when comparing the proposed scheme with other papers that use the commonly used 'cameraman' image as their watermark. The 'W2' watermark that was retrieved from the attacked photos is shown in Table 10. The proposed system displayed great robustness against multiple attacks while using a distinct watermark picture.

Table 10: Extracted watermarks of W2

WF [3 3]	GLF [3 3]	MF [3 3]	AF [3 3]
SH08	GN001	GN005	SPN001
SPN005	SN005	AD	HE
MB	JPEG Q50	JPEG Q70	JPEG2000

4.5.1 Various attacks comparison

4.5.1.1 Comparison with schemes in IWT-SVD research

Table 11 compares the effectiveness of various picture watermarking techniques, including IWT-SVD-ABC, DWT-SVD-DE, IWT-SVD, and the suggested technique, against a variety of attacks. WF[2,2], AF[3,3], MF[3,3], GLF[3,3], SPN001, GN001, GN005, JPEG Q40, JPEG Q50, SH08, Rotation20, AD, and HE are among the assaults. A value of 1.0 indicates perfect retrieval.

Table 11: Comparison with schemes in IWT-SVD research paper

Attacks	IWT-SVD-ABC [17]	DWT-SVD-DE [30]	IWT-SVD [31]	Proposed scheme
	NC	NC	NC	NC
No attack	1.0000	1.0000	1.0000	1.0000
WF[2,2]	0.9968	0.9250	0.9948	0.9974
AF[3,3]	0.9651	0.9191	0.9716	0.9449
MF[3,3]	0.9734	0.9495	0.9838	0.9843
GLF[3,3]	0.9356	0.9592	0.9354	0.9462
GN001	0.9442	0.8578	0.9360	0.9908
GN005	0.8856	0.8212	0.8854	0.9388
SPN001	0.9976	0.9229	0.9970	0.9990
JPEG Q40	0.9996	0.9641	0.9990	0.9997
JPEG Q50	0.9996	0.9583	0.9990	0.9998
SH08	0.9485	0.8856	0.9470	0.9728
Rotation20	0.9076	0.9478	0.9842	0.9424
AD	0.9699	0.9496	0.9732	0.9288
HE	0.9739	0.9335	0.9142	0.9001
Average	0.9641	0.9281	0.9658	0.9675

Analyzing the results, the proposed scheme (IWT-HD-SVD) consistently outperforms the other schemes in terms of watermark retrieval accuracy. The average similarity index for the proposed scheme is 0.9675, which is higher than the indices for IWT-SVD-ABC (0.9641), DWT-SVD-DE (0.9281), and IWT-SVD (0.9658). This indicates that the proposed scheme is more robust against a variety of attacks and provides better protection for the embedded watermarks.

It is clear from the specific attacks that, on average, the proposed scheme outperforms the other schemes in terms of similarity indices. For example, under the WF[2,2] attack, the proposed scheme achieves a similarity index of 0.9974, while the

other schemes range from 0.9250 to 0.9968. Similarly, under attacks such as GN001, SPN001, JPEG Q40, JPEG Q50, and SH08, the proposed scheme consistently outperforms the others, with similarity indices ranging from 0.9388 to 0.9998.

However, It is important to note that the suggested scheme does exhibit slightly lower performance under some attacks, such as AF[3,3], MF[3,3], and Rotation20, compared to DWT-SVD-DE and IWT-SVD. This suggests that the proposed scheme may have certain limitations when faced with these specific types of attacks. In conclusion, considering the outcomes shown in the table, the proposed scheme (IWT-HD-SVD) demonstrates superior performance in terms of watermark retrieval accuracy compared to the other schemes evaluated.

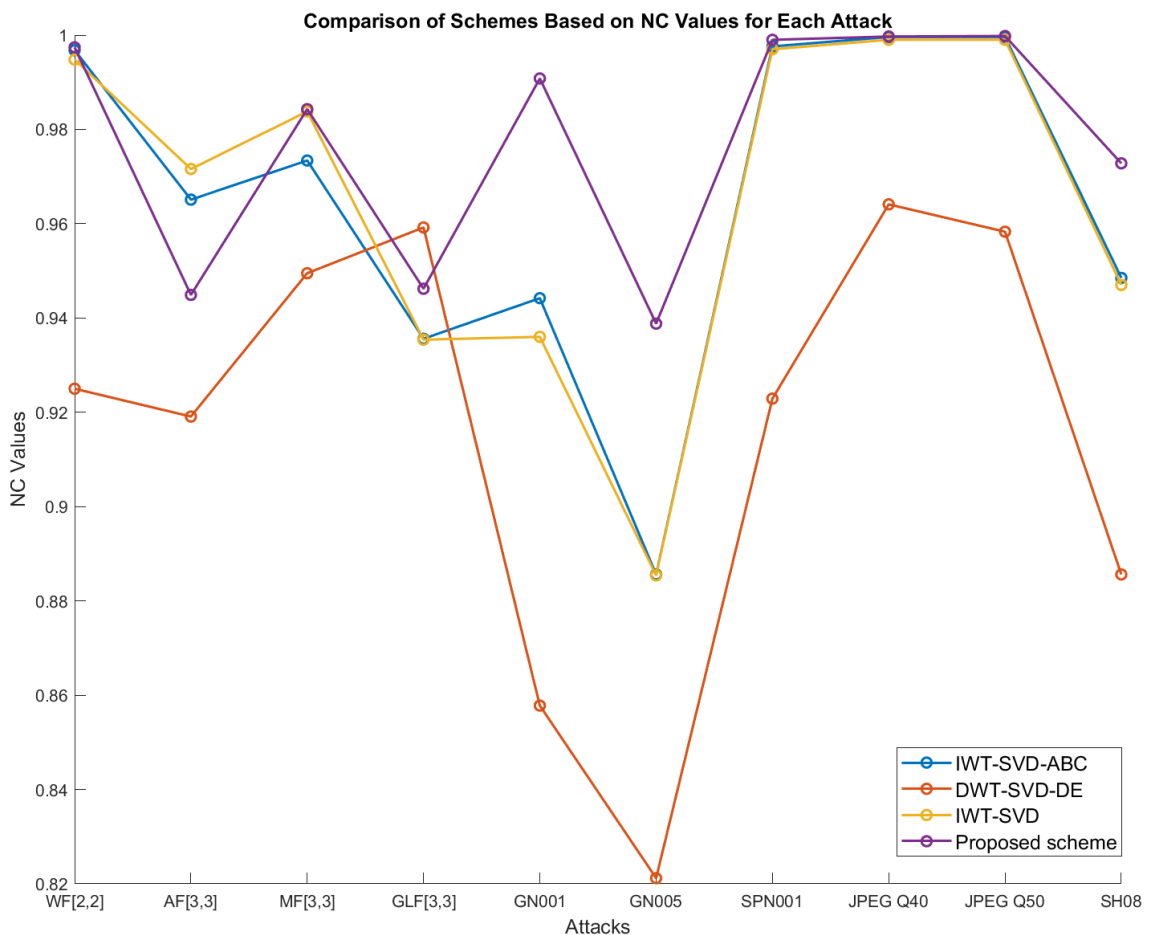


Figure 8: Line graph comparison with schemes in IWT-SVD research

4.5.1.2 Comparison with schemes in IWT-SVD-MOACO research

The table 12 offers a comparison of three image watermarking schemes: DWT-SVD-SC, IWT-SVD-MOACO, and the proposed scheme (IWT-HD-SVD). The schemes are evaluated under different attacks, with the "No attack" column representing the performance without any attack applied.

Table 12: Comparison with schemes in IWT-SVD-MOACO research paper

Attacks	DWT-SVD-SC [32]	IWT-SVD-MOACO [16]	Proposed scheme
	NC	NC	NC
No attack	1.0000	1.0000	1.0000
GN001	0.9681	0.9712	0.9993
SN001	0.9838	0.9903	0.9998
SN01	0.9541	0.9578	0.9999
AF[3,3]	0.9757	0.9796	0.9978
MF[3,3]	0.9817	0.9800	0.9843
SPN001	0.9823	0.9841	0.9999
SPN01	0.9113	0.9220	0.9999
JPEG Q30	0.9822	0.9930	0.9996
JPEG Q50	0.9841	0.9811	0.9998
Average	0.9723	0.9759	0.9980

Analyzing the results, it is evident that the proposed scheme consistently outperforms the other two schemes in terms of watermark retrieval accuracy. The average similarity index for the proposed scheme is 0.9980, which is higher than the indices for DWT-SVD-SC (0.9723) and IWT-SVD-MOACO (0.9759). This indicates that the suggested scheme offers improved resistance to a range of attacks and ensures a higher level of watermark preservation. Looking at the specific attacks, the proposed scheme consistently achieves higher similarity indices compared to the other schemes. For instance, under attacks like GN01, SN01, AF[3,3], and MF[3,3], the proposed scheme demonstrates superior performance with similarity indices ranging from 0.9978 to 0.9999, while the other schemes range from 0.9541 to 0.9903. This implies that the suggested system can successfully fend off various signal processing threats and maintain a higher fidelity of the embedded watermarks.

Moreover, the proposed scheme exhibits excellent performance under specific attacks like SPN01, SPN1, JPEG Q30, and JPEG Q50, with similarity indices ranging from 0.9843 to 0.9999. In comparison, the other schemes achieve lower indices in the range of 0.9113 to 0.9930. This indicates that the proposed scheme is particularly effective in scenarios where the watermarked images are subjected to noise, compression, or quantization-based attacks. In summary, judging from the outcomes in the table, the proposed scheme demonstrates superior performance in terms of watermark retrieval accuracy compared to DWT-SVD-SC and IWT-SVD-MOACO. It showcases robustness against a wide range of attacks, as reflected by its high average similarity index of 0.9980. The proposed scheme excels in preserving watermarks even under challenging attack scenarios, such as noise and compression.

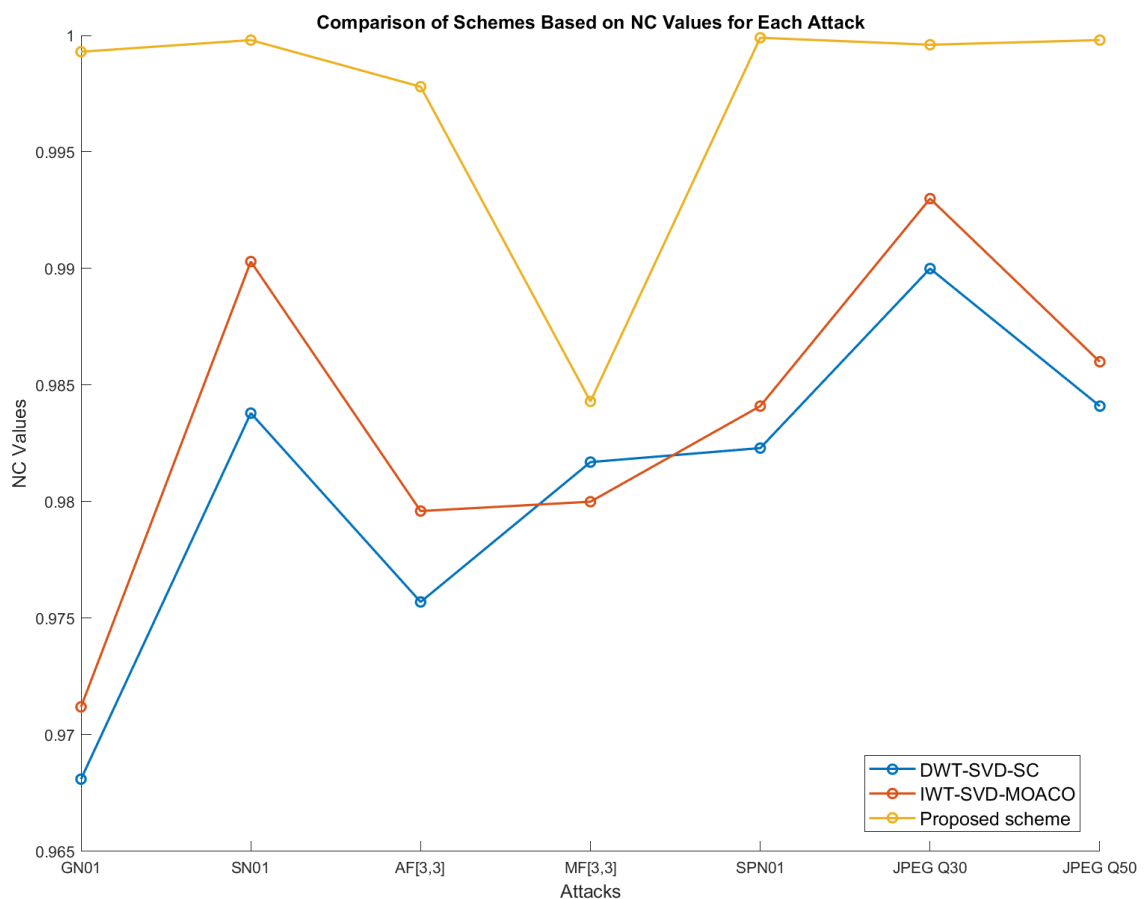


Figure 9: Line graph comparison for schemes in IWT-SVD-MOACO research

4.5.1.3 Comparison with DWT-HD-SVD

. Table 13 presents the performance evaluation of two image watermarking schemes: DWT-HD-SVD and the proposed scheme. The schemes are tested under various attacks.

Table 13: Comparison with DWT-HD-SVD research paper

Attacks	DWT-HD-SVD [28]	Proposed scheme
	NC	NC
No attack	1.0000	1.0000
MF [3,3]	0.9685	0.9843
GLF[3,3]	0.9749	0.9462
SPN001	0.9985	0.9990
JPEG Q25	0.9994	0.9996
JPEG Q40	0.9998	0.9998
JPEG Q50	0.9998	0.9998
JPEG Q70	0.9999	0.9999
SH02	0.9992	0.9967
GN005	0.9286	0.9388
SPN001	0.9897	0.9990
Average	0.9882	0.9886

Upon analysis of the results, it can be observed that both the DWT-HD-SVD and the proposed scheme exhibit high watermark retrieval accuracy. The average similarity indices for the two schemes are 0.9882 and 0.9886, respectively. This indicates that both schemes are effective in preserving the embedded watermarks, with the proposed scheme showing a **slightly higher** overall performance.

When considering specific attacks, the proposed scheme consistently demonstrates superior performance compared to DWT-HD-SVD. For example, under attacks such as MF [3,3], GLF[3,3], SPN001, JPEG Q25, and SH02, the proposed scheme achieves higher similarity indices ranging from 0.9462 to 0.9996, while DWT-HD-SVD achieves indices ranging from 0.9286 to 0.9992. This indicates that the proposed scheme is more robust and ability to resist a wider variety of assaults while preserving the watermarks with higher fidelity. Also, both schemes achieve high similarity indices even under challenging attacks such as JPEG compression at various quality levels (Q25, Q40, Q50, and Q70). The similarity indices for both schemes remain consistently high,

indicating their ability to maintain the integrity of the watermarked images even after compression.

Overall, based on the data shown in table 13, the proposed system performs marginally better than DWT-HD-SVD. It showcases higher robustness against a variety of attacks, as reflected by its average similarity index of 0.9886.

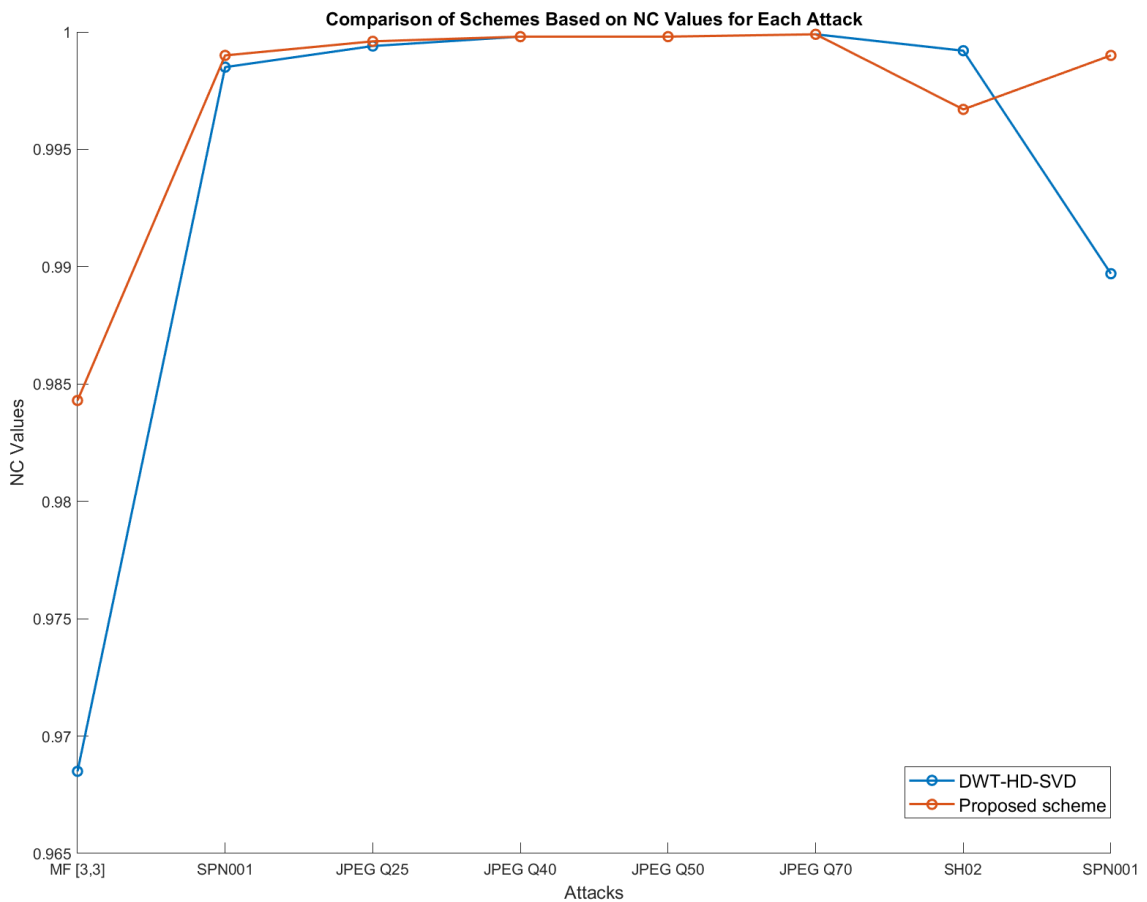


Figure 10: Line graph comparison with DWT-HD-SVD research

4.6 Summary

In this chapter, The overall results and discussion of the suggested watermarking method are presented. The performance of the scheme's imperceptibility for various watermark images is demonstrated in detail, with different sizes of watermark images. The chapter also showcases the invisibility performance and the level of the extracted watermark's quality, which yielded excellent results. Furthermore, the suggested

watermarking systems are evaluated against image processing attacks and compared with related works. Finally, Chapter 5 presents the conclusion of the proposed scheme.

CHAPTER 5

CONCLUSION

5.1 Introduction

This study set out to examine scaling factor optimisation in picture watermarking and assess how well the suggested scheme performed in contrast to other methods. Although the proposed scheme may not outperform other schemes in certain specific attacks, it consistently achieved higher average NC values than the competing schemes. It is important to note that achieving optimal robustness and imperceptibility across all types of attacks using optimized scaling factors can be challenging. The inclusion of hybrid and optimization methods in the proposed scheme resulted in increased computational time, particularly during the scaling factor optimization process.

The proposed scheme introduced an optimized scaling factor selection method that considered the impact of the selected diagonal matrix in the SVD process during watermark embedding. This approach demonstrated both high robustness against a range of attacks and high imperceptibility of the watermarked image. Moreover, the proposed scheme exhibited versatility in handling different sizes of watermark images, as it was successfully tested with various sizes. This further reinforced its effectiveness in achieving high robustness and imperceptibility compared to other existing schemes. This research successfully contributed to the field of image watermarking by introducing optimized scaling factors, improving the embedding method through consideration of the selected diagonal matrix in SVD. The suggested method performed more effectively in terms of robustness and imperceptibility, making it a valuable contribution to the field.

5.2 Research contributions

This study has made several significant contributions:

1. The proposed watermarking scheme introduces an innovative approach to generate optimized scaling factors by extensively testing various types of attacks.

By systematically selecting the best scaling factor for each attack, the scheme achieves enhanced performance and robustness.

2. The proposed scheme demonstrates good imperceptibility and robustness when subjected to various forms of visual attacks. The watermarking scheme exhibits high imperceptibility with a PSNR of 38dB and a SSIM of 0.99. Moreover, when tested against various types of attacks, including those targeting different sizes of watermark images, the scheme consistently achieves NC values. For a watermark size of 256x256, the average NC value is approximately 0.9794, for 128x128 it is around 0.9857, and for 64x64 it reaches approximately 0.9873.

5.3 Conclusion

The primary goal of this project is to develop an optimized image watermarking that achieves both high robustness and imperceptibility. This objective is supported by conducting comparisons with existing schemes to validate the effectiveness of the proposed approach. To accomplish this, the research delves into the detailed exploration of key concepts such as HD, SVD, IWT, and the optimized scaling factor.

By providing comprehensive explanations and analyses of HD, SVD, IWT, and the optimized scaling factor, the **first objective** of studying the current methods of optimized image watermarking using HD and SVD in the IWT domain is successfully achieved. This involved thoroughly examining the principles, techniques, and applications of these components, allowing for a deep understanding of their functionalities and potential for optimization.

The **second objective** of developing an optimized image watermarking scheme using HD, SVD, and IWT is fulfilled through the well-designed proposed scheme. The research focuses on optimizing the scaling factor, which plays a crucial role in balancing robustness and imperceptibility. By carefully considering the scaling factor for different types of attacks, the proposed scheme is refined to achieve optimal performance in terms of imperceptibility while maintaining robustness against various attacks.

To address the **final objective** of evaluating the results for the optimized image watermarking scheme, extensive experiments are conducted. The proposed scheme is subjected to a range of attack scenarios, and the outcomes are contrasted with similar strategies. This comprehensive evaluation allows for a thorough assessment of the scheme's imperceptibility and robustness, enabling researchers and practitioners to understand its effectiveness in real-world scenarios.

In summary, this research successfully achieves its objectives by thoroughly studying the current methods, developing an optimized scheme, and conducting a comprehensive evaluation of its performance regarding imperceptibility and robustness. Furthermore, there is potential for enhancing the performance of the watermarking technique in future research by exploring alternative optimization methods or embedding methods. By investigating different optimization approaches or refining embedding the watermark procedure, It is feasible to improve the resilience and imperceptibility of watermarking even further. This avenue of exploration opens up opportunities for further advancements and refinements in the field of optimized image watermarking.

5.4 Future recommendation

Several recommendations can be made for future research:

1. The proposed watermarking scheme shows potential for implementation with other optimization methods such as ACO, PSO, FA, GWO, and more. Currently, the optimization process requires significant computational time, and The necessary scaling factor is manually adjusted based on the type of attacks. Exploring alternative optimization methods can help address these issues and potentially improve the plan's effectiveness.
2. The proposed watermarking scheme has the potential to be applied in other domains, such as DCT, RDWT, and others. While the current scheme focuses on the IWT domain, it would be valuable to investigate its performance in other

transform domains. For example, Yuling Luo [28] explored the application of a similar scheme using FOA optimization in the DWT domain.

3. It is worth exploring various hybrid methods to further enhance its performance. Combining the proposed scheme with complementary techniques from different domains or methodologies can potentially lead to enhanced robustness and imperceptibility outcomes.

REFERENCES

- [1] C. I. Podilchuk and W. Zeng, "Image-adaptive watermarking using visual models," *IEEE J. Sel. Areas Commun.*, vol. 16, no. 4, pp. 525–539, May 1998, doi: 10.1109/49.668975.
- [2] "Copyright Explained: Definition, Types, and How It Works." <https://www.investopedia.com/terms/c/copyright.asp> (accessed Oct. 29, 2022).
- [3] "What is Digital Watermark? - Definition from Techopedia." <https://www.techopedia.com/definition/23373/digital-watermark> (accessed Oct. 29, 2022).
- [4] S. M. R. Haque, "Singular Value Decomposition and Discrete Cosine Transform Based Image Watermarking," 2008, Accessed: Oct. 29, 2022. [Online]. Available: www.bth.se/tek
- [5] "Integer Wavelet Transform (Advanced Signal Processing Toolkit) - NI." https://www.ni.com/docs/en-US/bundle/labview-advanced-signal-processing-toolkit-api-ref/page/lvasptconcepts/wa_iwt.html (accessed Dec. 06, 2022).
- [6] H. Seddik, M. Sayadi, F. Fnaiech, and M. Cheriet, "IMAGE WATERMARKING BASED on the HESSENBERG TRANSFORM," *Int. J. Image Graph.*, vol. 9, no. 3, pp. 411–433, Jul. 2009, doi: 10.1142/S0219467809003514.
- [7] "Understanding Singular Value Decomposition and its Application in Data Science | by Reza Bagheri | Towards Data Science." <https://towardsdatascience.com/understanding-singular-value-decomposition-and-its-application-in-data-science-388a54be95d> (accessed Jan. 19, 2023).
- [8] J. M. Guo and H. Prasetyo, "False-positive-free SVD-based image watermarking," *J. Vis. Commun. Image Represent.*, vol. 25, no. 5, pp. 1149–1163, Jul. 2014, doi: 10.1016/J.JVCIR.2014.03.012.
- [9] "How to Choose an Optimization Algorithm - MachineLearningMastery.com." <https://machinelearningmastery.com/tour-of-optimization-algorithms/> (accessed May 15, 2023).
- [10] "Why in DWT domain image watermarking techniques LL sub-band is preferred by the researcher? | ResearchGate." <https://www.researchgate.net/post/Why-in-DWT-domain-image-watermarking-techniques-LL-sub-band-is-preferred-by-the-researcher> (accessed May 15, 2023).
- [11] R. A. Alotaibi and L. A. Elrefaei, "Text-image watermarking based on integer wavelet transform (IWT) and discrete cosine transform (DCT)," *Appl. Comput. Informatics*, vol.

15, no. 2, pp. 191–202, Jul. 2019, doi: 10.1016/J.ACI.2018.06.003.

- [12] “(PDF) Reversible Digital Watermarking using Integer Wavelet Transform.” https://www.researchgate.net/publication/228411491_Reversible_Digital_Watermarking_using_Integer_Wavelet_Transform (accessed Dec. 02, 2022).
- [13] “Integer Wavelet Transform | Download Scientific Diagram.” https://www.researchgate.net/figure/Integer-Wavelet-Transform_fig1_342055763 (accessed Dec. 06, 2022).
- [14] “Singular value decomposition - Wikipedia.” https://en.wikipedia.org/wiki/Singular_value_decomposition (accessed Jan. 17, 2023).
- [15] N. Jose, M. Kuriakose, and S. Thomas, “Hybrid method for image watermarking,” *2017 Int. Conf. Energy, Commun. Data Anal. Soft Comput. ICECDS 2017*, pp. 1157–1162, Jun. 2018, doi: 10.1109/ICECDS.2017.8389623.
- [16] N. M. Makbol, B. E. Khoo, T. H. Rassem, and K. Loukhaoukha, “A new reliable optimized image watermarking scheme based on the integer wavelet transform and singular value decomposition for copyright protection,” *Inf. Sci. (Ny)*, vol. 417, pp. 381–400, Nov. 2017, doi: 10.1016/J.INS.2017.07.026.
- [17] I. A. Ansari, M. Pant, and C. W. Ahn, “Robust and false positive free watermarking in IWT domain using SVD and ABC,” *Eng. Appl. Artif. Intell.*, vol. 49, pp. 114–125, Mar. 2016, doi: 10.1016/J.ENGAPPAL.2015.12.004.
- [18] A. Mishra, C. Agarwal, A. Sharma, and P. Bedi, “Optimized gray-scale image watermarking using DWT–SVD and Firefly Algorithm,” *Expert Syst. Appl.*, vol. 41, no. 17, pp. 7858–7867, Dec. 2014, doi: 10.1016/J.ESWA.2014.06.011.
- [19] Y. Guo, B. Z. Li, and N. Goel, “Optimised blind image watermarking method based on firefly algorithm in DWT-QR transform domain,” *IET Image Process.*, vol. 11, no. 6, pp. 406–415, Jun. 2017, doi: 10.1049/IET-IPR.2016.0515.
- [20] N. K. Sharma, S. Kumar, A. Rajpal, and N. Kumar, “MantaRayWmark: An image adaptive multiple embedding strength optimization based watermarking using Manta Ray Foraging and bi-directional ELM,” *Expert Syst. Appl.*, vol. 200, p. 116860, Aug. 2022, doi: 10.1016/J.ESWA.2022.116860.
- [21] A. Mohan, A. Anand, A. K. Singh, R. Dwivedi, and B. Kumar, “Selective encryption and optimization based watermarking for robust transmission of landslide images,” *Comput. Electr. Eng.*, vol. 95, p. 107385, Oct. 2021, doi: 10.1016/J.COMPELECENG.2021.107385.
- [22] D. Golda, B. Prabha, K. Murali, K. Prasuna, S. Sri Vatsav, and S. Adepu, “Robust image

- watermarking using the social group optimization algorithm,” *Mater. Today Proc.*, vol. 80, pp. 2819–2823, Jan. 2023, doi: 10.1016/J.MATPR.2021.07.045.
- [23] P. K. Muhuri, Z. Ashraf, and S. Goel, “A Novel Image Steganographic Method based on Integer Wavelet Transformation and Particle Swarm Optimization,” *Appl. Soft Comput.*, vol. 92, p. 106257, Jul. 2020, doi: 10.1016/J.ASOC.2020.106257.
- [24] “Peak signal-to-noise ratio - Wikipedia.” https://en.wikipedia.org/wiki/Peak_signal-to-noise_ratio (accessed Jan. 17, 2023).
- [25] “Structural similarity - Wikipedia.” https://en.wikipedia.org/wiki/Structural_similarity (accessed Jan. 17, 2023).
- [26] A. M. Alattar, “Watermarking Techniques,” *J. Inf. Secur. Appl.*, vol. 21, no. 3, pp. 174–183, 2014.
- [27] M. Tang and F. Zhou, “A robust and secure watermarking algorithm based on DWT and SVD in the fractional order fourier transform domain,” *Array*, vol. 15, p. 100230, 2022, doi: 10.1016/j.array.2022.100230.
- [28] J. Liu *et al.*, “An Optimized Image Watermarking Method Based on HD and SVD in DWT Domain,” *IEEE Access*, vol. 7, pp. 80849–80860, 2019, doi: 10.1109/ACCESS.2019.2915596.
- [29] P. W. Wong, “Image Quantization, Halftoning, and Printing,” *Handb. Image Video Process.*, pp. 925–937, Jan. 2005, doi: 10.1016/B978-012119792-6/50117-0.
- [30] M. Ali and C. W. Ahn, “An optimized watermarking technique based on self-adaptive DE in DWT–SVD transform domain,” *Signal Processing*, vol. 94, no. 1, pp. 545–556, Jan. 2014, doi: 10.1016/J.SIGPRO.2013.07.024.
- [31] N. M. Makbol and B. E. Khoo, “A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition,” *Digit. Signal Process.*, vol. 33, pp. 134–147, Oct. 2014, doi: 10.1016/J.DSP.2014.06.012.
- [32] A. Tareef and A. Al-Ani, “A highly secure oblivious sparse coding-based watermarking system for ownership verification,” *Expert Syst. Appl.*, vol. 42, no. 4, pp. 2224–2233, Mar. 2015, doi: 10.1016/J.ESWA.2014.09.055.

APPENDIX A
LIST OF TESTING IMAGES FROM INTERNET WITH SIZES OF 512X512



**APPENDIX B
RESEARCH GANTT CHART**

