DUAL IMAGE WATERMARKING BASED ON HUMAN VISUAL CHARACTERISTICS FOR AUTHENTICATION AND COPYRIGHT PROTECTION

WONG SHU JIE

Bachelor Degree

UNIVERSITI MALAYSIA PAHANG

UNIVERSITI MALAYSIA PAHANG

DECLARATION OF THESIS AND COPYRIGHT

Author's Full Name : WONG SHU JIE

Date of Birth

Title : DUAL IMAGE WATERMARKING BASED ON HUMAN VISUAL CHARACTERISTICS FOR AUTHENTICATION AND COPYRIGHT PROTECTION

Academic Session : SEM1 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)

Name of Supervisor:
FERDA ERNAWAN
Date:

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 informed that the following thesis is classified as RESTRICTED for a period of three (3) years from the date of this letter. The reasons for this classification are as listed below.

Author's Name
Thesis Title

Reasons (i)

(ii)

(iii)

Thank you.

Yours faithfully,

____
(Supervisor's Signature)

Date:

Stamp: TS. DR. FERDA ERNAWAN
SENIOR LECTURER
FACULTY OF COMPUTING
COLLEGE OF COMPUTING & APPLIED SCIENCES
UNIVERSITI MALAYSIA PAHANG
26600 PEKAN, PAHANG DARUL MAKMUR
TEL : 09-424 4648 FAX : 09-424 4666

Note: This letter should be written by the supervisor, addressed to the Librarian, *Perpustakaan Universiti Malaysia Pahang* with its copy attached to the thesis.

UMP Universiti Malaysia PAHANG
Engineering • Technology • Creativity

SUPERVISOR'S DECLARATION

I/We* hereby declare that I/We* have checked this thesis/project* and in my/our* opinion, this thesis/project* is adequate in terms of scope and quality for the award of the degree of *Doctor of Philosophy/ Master of Engineering/ Master of Science in …………………………..

(Supervisor's Signature)

Full Name : Profesor Madya Ts. Dr. Ferda Ernawan

Position : Senior Lecturer

Date : 10/07/2023

(Co-supervisor's Signature)

Full Name :

Position :

Date :

UMP
Universiti
Malaysia
PAHANG
Engineering • Technology • Creativity

STUDENT'S DECLARATION

I hereby declare that the work in this thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at Universiti Malaysia Pahang or any other institutions.

(Student's Signature)

Full Name : WONG SHU JIE
ID Number : CD20137
Date : 2nd JULY 2023

DUAL IMAGE WATERMARKING BASED ON HUMAN VISUAL SYSTEM CHARACTERISTICS FOR AUTHENTICATION AND COPYRIGHT PROTECTION

WONG SHU JIE

Thesis submitted in fulfillment of the requirements

for the award of

Bachelor's Degree Graphics and Multimedia Technology

Faculty of Computing

UNIVERSITI MALAYSIA PAHANG

July 2023

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude and appreciation to all those who have contributed to the successful completion of my final year project. Their guidance, support, and encouragement were invaluable throughout this journey.

First and foremost, I would like to extend my deepest thanks to my project supervisor, Associate Professor Ts. Dr. Ferda Ernawan , for his exceptional guidance and continuous support. Their expertise, valuable insights, and unwavering commitment have been instrumental in shaping this project and pushing it towards excellence.

I would also like to thank the faculty members and professors at Faculty of Computing, Universiti Malaysia Pahang who have provided me with an enriching academic environment and invaluable resources. Their dedication to teaching and commitment to fostering intellectual growth have greatly contributed to the development of this project.

In addition, I would like to express my appreciation to my peers who have been an endless source of inspiration, collaboration, and encouragement. Their willingness to share ideas, engage in discussions, and offer constructive feedback has significantly enhanced the quality of my work.

Furthermore, I am grateful to my family and friends for their unwavering support, understanding, and encouragement throughout this project. Their belief in my abilities and their constant motivation have been the driving force behind my perseverance.

Lastly, I would like to acknowledge the numerous research articles, academic papers, and online resources that have provided valuable insights and knowledge, serving as the foundation for this project.

In conclusion, I am immensely grateful to all the individuals and organizations who have played a part in the completion of this final year project. Your contributions, support, and guidance have been invaluable, and I am truly honored to have had the opportunity to work on this project with such incredible individuals.

ABSTRAK

Kini, kandungan multimedia seperti gambar mudah diedarkan secara global kerana penggunaan teknologi maklumat dan komunikasi yang meluas. *Digital Watermarking* ialah pendekatan untuk mencegah serangan atau perubahan pada gambar yang mungkin membawa kepada masalah kritikal seperti penyebaran berita palsu, cetak rompak gambar dan pengedaran gambar secara haram. Penyelidikan ini membentangkan skema Penanda Air Imej Duaan berdasarkan ciri visual manusia untuk pengesahan dan perlindungan hak cipta. Objektif skim yang dicadangkan ini adalah untuk membangunkan algoritma penanda air yang dipertingkatkan yang mencapai ketidakjelasan dan keteguhan yang tinggi dengan memanfaatkan prinsip ciri sistem visual manusia. Skim ini bertujuan untuk membenamkan dua tera air ke dalam imej dengan herotan yang minimum, menjadikannya tidak dapat dilihat oleh mata manusia. Tambahan pula, tera air boleh diekstrak dengan tepat walaupun selepas serangan pemprosesan imej seperti hingar Gaussian atau hingar garam dan lada. Selain itu, skema ini menunjukkan penyetempatan gangguan yang cekap, membolehkan pengesanan pengubahsuaian yang dibuat pada imej asal dengan ketepatan tinggi, ketepatan dan skor F1. Keputusan eksperimen mengesahkan keberkesanan skim yang dicadangkan, mempamerkan prestasi unggul dari segi ketidakjelasan, keteguhan dan penyetempatan gangguan berbanding skim penanda air sedia ada yang tertakluk kepada serangan yang sama. Keupayaan skema untuk membenamkan tera air yang tidak dapat dikesan memastikan perlindungan hak cipta dan pengesahan ketulenan, manakala keteguhannya terhadap pelbagai serangan pemprosesan imej meningkatkan kepraktisannya dalam senario dunia sebenar. Kesimpulannya, cadangan skim Penanda Air Dwi Imej berdasarkan ciri visual manusia menyediakan penyelesaian yang berkesan untuk pengesahan dan perlindungan hak cipta. Dengan memastikan ketidakjelasan, keteguhan dan penyetempatan gangguan, skim ini menawarkan pendekatan yang boleh dipercayai untuk mendapatkan kandungan multimedia digital dalam era pengedaran maklumat yang meluas dan kemajuan teknologi.

ABSTRACT

Nowadays, multimedia content like images are easily to be distributed globally because of the widespread usage of information and communication technologies. Digital watermarking is an approach to prevent attacks or modification on images that might lead to serious problems like spreading of fake news, image piracy and illegal distribution of images. This research presents a novel Dual Image Watermarking scheme based on human visual characteristics for authentication and copyright protection. The objective of this proposed scheme is to develop an enhanced watermarking algorithm that achieves high imperceptibility and robustness by leveraging the principles of human visual system characteristics. The scheme aims to embed two watermarks into an image with minimal distortion, rendering them imperceptible to the human eye. Furthermore, the watermarks can be extracted accurately even after image processing attacks such as Gaussian noise or salt and pepper noise. Additionally, the scheme demonstrates efficient tamper localization, enabling the detection of modifications made to the original image with high accuracy, precision, and F1-score. Experimental results validate the effectiveness of the proposed scheme, showcasing superior performance in terms of imperceptibility, robustness, and tamper localization compared to existing watermarking schemes subjected to the same attacks. The scheme's ability to embed undetectable watermarks ensures copyright protection and authenticity verification, while its robustness against various image processing attacks enhances its practicality in real-world scenarios. In conclusion, the proposed Dual Image Watermarking scheme based on human visual characteristics provides an effective solution for authentication and copyright protection. By ensuring imperceptibility, robustness, and tamper localization, the scheme offers a reliable approach for securing digital multimedia content in the era of widespread information distribution and technological advancements.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ARE	Absolute Reconstruction Error
Avg	Average
BER	Bit Error Rate
DCT	Discrete Cosine transform
DRM	Digital Rights Management
DWT	Discrete Wavelet Transform
FNR	False-Negative Rate
FPR	False-Positive Rate
HH	Higher Highs
HL	Higher Lows
HVS	Human Visual System
JPEG	Joint Photographic Experts Group
LH	Lower Highs
LL	Lower Lows
LSB	Least-Significant Bit
MSE	Mean Squared Error
NC	Normalized Corelation
NCML	Nested Chaotic Map Lattice
PSNR	Peak Signal-To-Noise Ratio
RDWT	Redundant Discrete Wavelet Transforms
RGB	Red-Green-Blue
RHFM	Radial Harmonic Fourier Moments
ROI	Region of Interest
SSIM	Structural Similarity Index
SVD	Singular Value Decomposition
TNR	True-Negative Rate
TPR	True-Positive Rate
VCS	Visual Cryptography

CHAPTER 1

INTRODUCTION

1.1 Introduction

Nowadays, multimedia contents like video, audio and images are easily to be distributed globally because of the widespread usage of information and communication technologies (Bhinder et al., 2020) . Therefore, to prevent attacks or modification on image, digital watermarking is a significant method to for copyright protection and authentication (SINGH et al., 2014). Digital watermarking is an action of inserting information into digital multimedia, where the process must not cause any perceptual damage to the original content and could not be removed by unauthorized parties, and additionally is resistant to intentional and unintentional attacks (Singh & Kumar, 2011) or manipulations like scaling, cropping, compression, rotating, and filtering. (Al-Haj, 2007) These criteria are also known as imperceptibility and robustness. With these two criteria, the watermarking techniques are divided into three which are robust, fragile and semi-fragile. These three categories have their own concerns and neglects. Robust watermarking is made to withstand attacks that aim to destroy or remove the watermark without significantly lowering the visual quality of the watermarked image. Hence, robust watermarking is always used for ownership verification and copyright protection. On the other hand, fragile watermarking is utilized to maintain the integrity and authenticity of an image. It is designed for modification detection where any tamper on the image could be identified. Lastly, semi-fragile watermarking is a combination of characteristics of robust and fragile watermarking where it could detect unauthorized manipulations but still being robust. (Mishra et al., 2014)

Watermarking is categorised into two groups including spatial domain and transform domain approaches (F. Liu & Liu, 2008) . Transform domain methods are more robust as the transformed coefficients are not easy to be manipulated (Bhinder et al., 2020).

1.2 Problem Statement

Digital image watermarking approaches are researched to achieve robustness, imperceptibility with the function of authentication and copyright protection. In this context, authentication is to embed extracted information of image into the image and to utilize ability of the watermark to detect area that has been tampered. Moreover, copyright protection is to embed watermark image into original image without perceptual damage.

According to Rakhmawati et al. (2019), a dual watermarking scheme consists of robust watermarking scheme and fragile watermarking scheme. The robust watermarking scheme is responsible for copyright protection while the fragile watermarking scheme is responsible for authentication and content recovery. The proposed watermarking scheme, the robust watermarking scheme is optimised on its embedding strengths and reference pattern. Additionally, the fragile watermarking scheme is able to implement tamper verification, content identification, tamper localization, and image recovery.

However, the imperceptibility is not a focus of the mentioned solution. Human Visual System (HVS) Characteristics is a useful algorithm to improve the imperceptibility of the watermark. It is used to identify the region in the host image that is suitable to embed the watermark without much distortion.

Therefore, a dual image watermarking according to human visual system characteristics is proposed to accomplish copyright protection and authentication watermarking techniques with high imperceptibility and robustness.

1.3 Objectives

- To study on existing dual watermarking scheme for copyright protection and authentication.

- To propose an enhanced watermarking scheme based on human visual system characteristics for copyright protection and authentication.

- To evaluate the proposed watermarking scheme based on imperceptibility, robustness and tamper localization ability in comparison with existing standard of watermarking scheme.

1.4 Scope of Project

1. A coloured host image in size 512 × 512 pixels and the watermark image is 32 × 32 pixels will be used.

2. The imperceptibility of the watermarked image will be evaluated by using Peak Signal-To-Noise Ratio (PSNR), Structural Similarity Index (SSIM), Absolute Reconstruction Error (ARE).

3. The robustness of the watermark was evaluated by Normalized Corelation (NC) value and Bit Error Rate (BER) with various attacks to the image.

4. The tamper localization ability of the watermark is evaluated using the Confusion Matrix including True-Positive Rate (TPR), False-Negative Rate (FNR), False-Positive Rate (FPR) and True-Negative Rate (TNR) and F1 Score.

5. The experiments were conducted using MATLAB R2022a© with Acer workstation, Intel(R) Core (TM) i5-8265U CPU @ 1.60GHz 1.80 GHz.

1.5 Thesis organization

The thesis consists of 5 chapters.

Chapter 1 is discussing the introduction of this research. It consists of the introduction, problem statement of the research, objectives, scope of the research and lastly the thesis organization.

Chapter 2 is discussing about the study of the research. This chapter explains the existing and related solutions to solve the overlap issues. Nevertheless, the chapter is discussing the critical review of comparison including the advantages and disadvantages of the techniques to research for suitable techniques to adapt to the research.

Chapter 3 is discussing the methodology used to carry out the research.

Chapter 4 is discussing the result and the analysis of the finding based on the experiment.

Chapter 5 contains the conclusion of the research findings and the future work of the research.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

Chapter 2 discusses the collected information related to dual image watermarking scheme. First, current situation of digital image watermarking for copyright protection and authentication is discussed. Next, the embedding region and watermark pre-processing are discussed. Furthermore, the watermarking methods are discussed. Lastly the existing dual image watermarking scheme are discussed with a summary table of the existing scheme.

2.2 Digital Image Watermarking for Copyright Protection and Authentication

Digital image watermarking is a process of embedding information into an image. There are two categories of watermarks which are visible watermark and invisible watermark. Visible watermark could be a meaningful logo or text that could represent the owner of the image. While invisible watermark embeds the data into the original image and is not easy to discover by human's eyes. The data could be extracted from the watermarked image and the information of the copyright could be retrieved. A watermark could be used to verify the copyright and authenticity of a copyrighted image. Copyright protection allows the ownership of the image to be identified. This is commonly performed by robust watermarking. On the other hand, the authentication of the image can determine whether the image is original or has been modified or tampered. A fragile watermarking could detect modifications on images.

2.3 Human Visual System Characteristics

Human Visual System Characteristics are utilized in watermarking methods to improve the imperceptibility of watermark. It is used to identify an appropriate region to embed the watermark that does not cause significant distortion in the original image. Entropy and edge entropy are used to apply the Human Visual System Characteristics which could select a region which has less distortion after watermark embedding but perceptually significant, to ensure the robustness of the watermark. Entropy is a statistical measure of randomness that can be used to distinguish the texture of an input image. The equation of entropy is:

$$E = -\sum_{i=1}^{N} p_i \, log_2(p_i)$$

Image edge entropy provides useful data about the image properties. The equation of edge entropy is:

$$E_{edge} = -\sum_{i=1}^{N} p_i \, e^{1-p_i}$$

The average summation of entropy and edge entropy is defined as:

$$E_{HVS} = -\sum_{i=1}^{N} (p_i \, log_2(p_i) + p_i \, e^{1-p_i})/2$$

2.4 Watermarking Methods

2.4.1 Discrete Cosine Transform (DCT)

Discrete Cosine Transform (DCT) is a widely used mathematical transformation technique in signal processing and image compression. It converts a finite sequence in the spatial domain, into a set of frequency coefficients in the frequency domain. In image compression applications, the DCT is widely employed to transform image blocks or patches into the frequency domain. By utilizing the fact that many natural images have most of their energy concentrated in the lower-frequency components, the DCT allows for efficient representation and compression of images. The high-frequency components, which contain less perceptually important information, can be quantized or discarded to achieve compression. The DCT is commonly used in image and video compression standards such as JPEG (Joint Photographic Experts Group) and MPEG (Moving Picture Experts Group). It provides a compact representation of image data that allows for significant compression while maintaining visual quality to an acceptable level. The formula of 2D forward DCT is as follow:

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

Inverse DCT is used to reconstruct image from the frequency coefficients. the frequency-domain representation can be converted back into the time or spatial domain, allowing for the retrieval of the original signal or image. The formula of inverse DCT is as follows:

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

where u, v = 0, 1, …, N-1, and α is defined as:

$$\alpha(\mathrm{u}) = \begin{cases} \sqrt{\frac{1}{n}}, for\ u = 0, \\ \sqrt{\frac{2}{n}}, otherwise. \end{cases}$$

2.4.2 Singular Value Decomposition (SVD)

The watermark can embed to the host image by considering the $U_{2,1}$ and $U_{3,1}$ in the first column of orthogonal matrix U. The relationship between these coefficients can be used to define whether the watermark bit is 0 or 1. SVD of A is defined as:

$$A = USV^T$$

$$A = \begin{bmatrix} U_{1,1} & U_{1,2} & \cdots & U_{1,n} \\ U_{2,1} & U_{2,2} & \cdots & U_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ U_{n,1} & U_{n,2} & \cdots & U_{n,n} \end{bmatrix} \begin{bmatrix} \sigma_{1,1} & 0 & 0 & 0 \\ 0 & \sigma_{2,2} & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & \sigma_{n,n} \end{bmatrix} \begin{bmatrix} V_{1,1} & V_{1,2} & \cdots & V_{1,n} \\ V_{2,1} & V_{2,2} & \cdots & V_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ V_{n,1} & V_{n,2} & \cdots & V_{n,n} \end{bmatrix}^T$$

where U is an orthonormal matrix, S is a diagonal matrix made up of the squares of A's eigenvalues in descending order and V is an orthonormal matrix.

2.5 Existing Dual Watermarking Scheme

2.5.1 An Image Tamper Detection and Recovery Method Based on Self-Embedding Dual Watermarking (Kiatpapan & Kondo, 2015)

This paper proposed a dual watermarking method to detect tamper and recover image to original. By using this watermarking method, two same watermark image is divided into bit planes and is embedded on the original image with the determination of least-significant bit (LSB) plane. The proposed watermarking method arrange the bit planes of two identical watermarks with a centre-point-symmetric manner so that the information of the image is distributed uniformly as watermarks. This allows for the recovery of a sizable area of tampering. The evaluation experiment is done by using original image of size 512×512 pixels and watermark image of 128×128 pixels.

The process flow starts with the resizing the host image into a watermark. There are two sets of watermarks to be prepared as the proposed method is a dual image watermarking method. The watermarks are embedded at the upper part and lower part of the least significant bit plane of the original image. Below is the flowchart of the watermark embedding process.

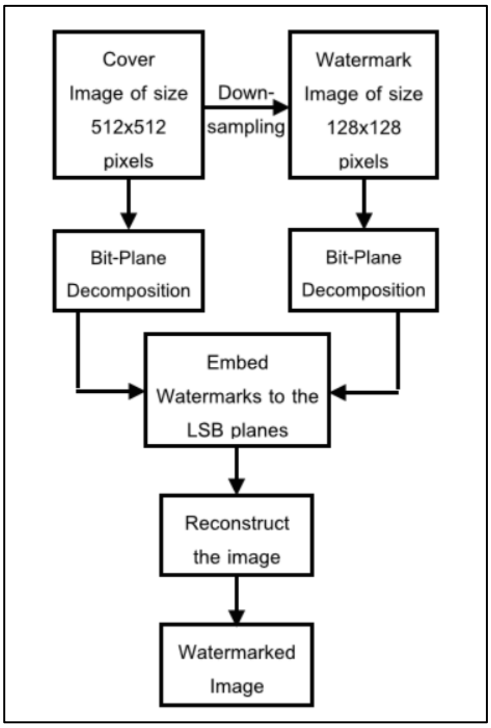
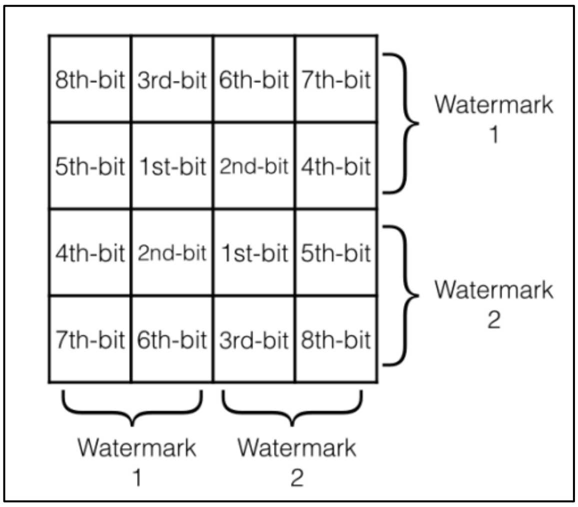

Cover Image of size 512x512 pixels
Down-sampling
Watermark Image of size 128x128 pixels
Bit-Plane Decomposition
Bit-Plane Decomposition
Embed Watermarks to the LSB planes
Reconstruct the image
Watermarked Image

Figure 1: Watermark Embedding Process

Figure 2 shows the actual arrangement of two watermarks on the host image.



8th-bit	3rd-bit	6th-bit	7th-bit
5th-bit	1st-bit	2nd-bit	4th-bit
4th-bit	2nd-bit	1st-bit	5th-bit
7th-bit	6th-bit	3rd-bit	8th-bit

Figure 2: Watermark Arrangement in LSB Plane

Next, for tamper detection and image recovery, the algorithm compares pixel-by-pixel of the tampered image and the watermark image colour intensities. If the algorithm does not detect any difference of the colour intensity of two images, it means the image is not tampered. However, if the colour intensity of the pixels is different, the tampered pixel will be replaced with the pixel from the watermark image. Figure 3 illustrates the tamper detection and image recovery process.

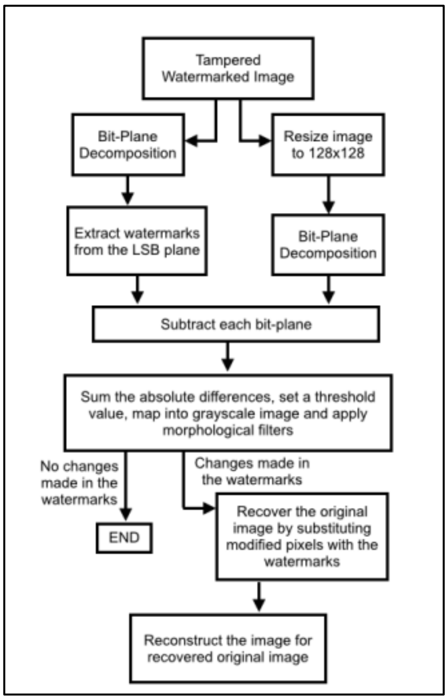

Tampered Watermarked Image
Bit-Plane Decomposition
Resize image to 128x128
Extract watermarks from the LSB plane
Bit-Plane Decomposition
Subtract each bit-plane
Sum the absolute differences, set a threshold value, map into grayscale image and apply morphological filters
No changes made in the watermarks
Changes made in the watermarks
END
Recover the original image by substituting modified pixels with the watermarks
Reconstruct the image for recovered original image

Figure 3: Tamper Detection and Image Recovery Flowchart

The proposed method with LSB implementation is exceptionally sensitive to the tamper on image. Additionally, the arrangement of watermark which is a centre-point-symmetric pattern ensures the image information is distributed evenly on the image. In conclusion, this proposed method is simple and easy to implement but with high effectiveness to detect image tamper and recover tampered image. The limitation of the watermarking method is it is unable to recover image that has been tampered globally across the whole original image.

2.5.2 An Analysis of Wavelet Based Dual Digital Image Watermarking Using SVD (Deepa B. Maheshwari, 2018)

This paper proposed a watermarking scheme based on DWT and SVD. The primary watermark is divided into 4 bands, then each band is applied with SVD. Moreover, the secondary watermark is embedded after modifying the singular values. The watermarking scheme is evaluated by various attacks like noise such as Gaussian and Poisson, rotation and average filtering. It demonstrates this watermarking scheme is more effective than solely DWT or SVD method.

In this watermarking scheme, an image is chosen as the primary watermark and a significant logo is selected as the secondary watermark. The generation or primary and secondary watermarks are inter-related. Firstly, the primary watermark is transformed using DWT algorithm and followed by SVD algorithm. Next, the singular values of the primary watermark are add up to the secondary watermark. The sum is used to modify the DWT transformation of the primary watermark. Next, the processed primary watermark is obtained and is embedded on the host image.

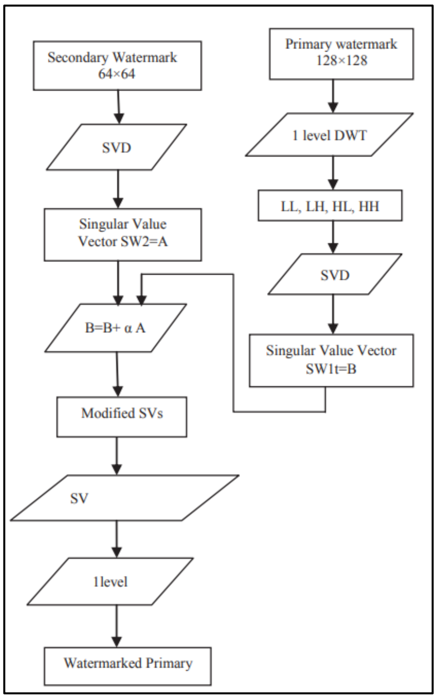

Secondary Watermark 64×64
Primary watermark 128×128
SVD
1 level DWT
LL, LH, HL, HH
Singular Value Vector SW2=A
SVD
B=B+ α A
Singular Value Vector SW1t=B
Modified SVs
SV
1level
Watermarked Primary

Figure 4: Process of Adding Secondary Watermark to Primary Watermark

In conclusion, the hybrid DWT and SVD watermarking scheme has both benefit properties of DWT and SVD algorithms in term of robustness and imperceptibility. This watermarking scheme is proven more effective than solely DWT or SVD watermarking method.

2.5.3 DWT-domain Dual Watermarking Algorithm of Colour Image based on Visual Cryptography (Y. Han et al., 2013)

The proposed watermarking scheme is a dual watermarking algorithm of colour image where the first watermark is embedded into the DWT's high-frequency segment. Moreover, for the secondary watermark, visual cryptography is used to create two shares, one shares is embedded into the DWT's low-frequency segment, while another share is protected by copyright.

Based on the paper, the embedded position of the watermark is determined based on a few factors including Human Visual System (HVS) characteristics, invisibility of watermark, and robustness of the watermark. According to these factors, it is concluded that the watermark should embed in blue components, the watermark should be embedded in texture or edge which is the high-frequency segment of the image after DWT and lastly the watermark should embed into the low-frequency segment after DWT. As mentioned in the analysis above, human eyes are sensitive to horizontal than vertical, the primary watermark is embedded into the vertical component of the high-frequency segment after DWT. The first watermark is also known as confirmable watermark as it is used to ensure the presence of the watermark. Next, the second watermark is embedded into the lower-frequency segment after DWT to enhance the robustness of the watermark. The second watermark image is named as a distinguishable watermark. The first watermark image is a straightforward but meaningful binary image, whereas the second is a complex but significant binary image.

In conclusion, the dual watermarking system make use of the advantages of DWT and VCS to propose a watermarking scheme with high security, robustness and imperceptibility.

2.5.4 A New Blind Image Watermarking Technique for Dual Watermarks Using Low-Frequency Band DCT Coefficients (Al-Gindy et al., n.d.)

This paper proposes a blind watermarking technique which embeds watermark data in 16 low-frequency band coefficients of DCT sub blocks. The embedding process is carried out by modifying the original image's selected DCT-coefficients to even or odd based on the binary bit value of the watermark. Blind watermarking is a technique which the information of original image and original watermark image are not needed during the extraction process of the watermark. The low-frequency band of the DCT-domain is chosen as the location for watermark data to be positioned. Additionally, this watermarking scheme is based on the possibility of incorporating multiple copies of the two binary watermarks into the host image.

The embedding algorithm is dividing the original image into an 8×8 blocks. These blocks are transformed using DCT and 16 coefficients of DCT are identified. Then, each DCT coefficient will undergo a zigzag process from low-frequency to high-frequency terms, here, the first lowest sixteen frequency not including the DC coefficient will be chosen. These selected coefficients will be displayed to preserve the robustness and imperceptibility of the watermark. Then, a secret key is applied to shuffle the binary watermark and convert them into vector of $1 \times N_{w1}$ and $1 \times N_{w2}$ size. The two vectors are finally combined into one vector of $1 \times N_w$ size. Later, the combined vector is separated into 16 sub blocks and each sub block is embedded into the original image by selecting one of sub block of the 8×8. Next, a shuffle is applied to shuffle the merged vectors and the previous step is repeated for every sub block of the original image. The shuffle could improve the watermark robustness from cropping attack. Finally, inverse DCT is used to acquire the watermarked image.

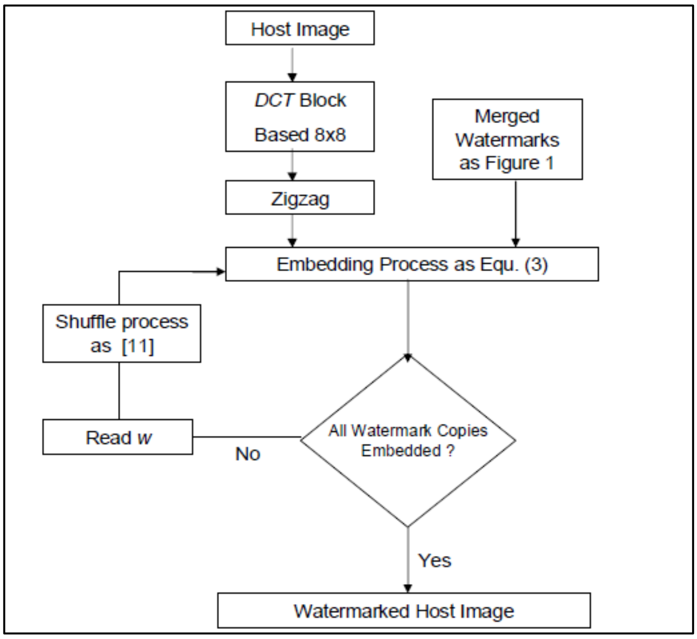


Figure 5: Flowchart of Embedding Process

The algorithm is tested by using “Lena”, a grayscale, 512×512 size as the host image and two 96×64 watermarks which are a handwritten binary signature and a binary text info image. It is proven that this watermarking scheme has high imperceptibility. Besides that, the robustness is tested with cropping and JPEG compression attack, the result is also satisfying.

In conclusion, this watermarking algorithm embeds multiple copies of two watermarks into the original image's low-frequency DCT coefficients. It is proven that this technique has high imperceptibility and robustness.

2.5.5 Dual Watermarking Method for Integrity of Medical Images (Lim et al., 2008)

This proposed watermarking scheme is a dual watermarking method which utilizes robust and fragile watermarking methods. The watermark could ensure the authenticity of the medical images which are transmitted across the Internet or store in the database. Additionally, the embedding region of the watermark is coded to ensure the watermark is out of the Region of Interest (ROI) areas to guarantee the watermark would not be embedded on the important part of the medical images. In this watermarking scheme, robust watermarking technique is used to embed data such as the hospital logo to identify any image leakage from the hospital’s server. Next, fragile watermarking technique is used to embed information like challenge-response information or timestamp. Furthermore, to ensure the watermark quality, the interference between robust and fragile watermarking is avoided by considering the edge information.

The embedding process is begun with the robust watermarking, following by fragile watermarking to examine the integrity of image after the robust watermarking. On the other side, to verify the watermarked image, the process is carried out in reverse. It means that the fragile watermark will be detected first before detecting the information in the robust watermark.

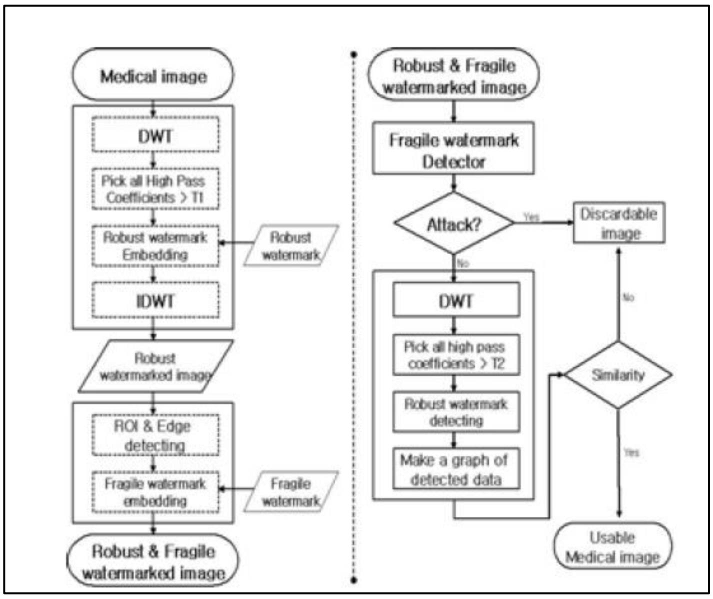

Medical image
DWT
Pick all High Pass Coefficients > T1
Robust watermark Embedding
Robust watermark
IDWT
Robust watermarked image
ROI & Edge detecting
Fragile watermark embedding
Fragile watermark
Robust & Fragile watermarked image
Robust & Fragile watermarked image
Fragile watermark Detector
Attack?
Yes
Discardable image
No
DWT
Pick all high pass coefficients > T2
Robust watermark detecting
Make a graph of detected data
Similarity
No
Yes
Usable Medical image

Figure 6: Block Diagram of Proposed Scheme

From the experimental result, the robustness is tested using various attacks which are median filter, JPEG compression, blur filter and cut and is represented using PSNR value. It is shown that the robustness to median filter attack is higher than other attacks.

In conclusion, this dual watermarking technique for medical images is a combination of fragile and robust watermarking, in addition, has the mechanism to avoid interference of two watermarks and the ROI is considered to avoid hiding any important information of the medical images by the watermarks.

2.5.6 Applying Dual Digital Watermarking Technology in Digital Rights Management (Liao & Liu, 2010)

In this paper, a Discrete Cosine Transform (DCT) dual watermarking scheme is proposed and to be utilised in Digital Rights Management system. This system could manage private performances and exhibits digital content. The two watermarks to be embedded are the owner’s watermark and the customer’s/buyer’s watermark. The owner’s watermark will be first embedded in the low and middle frequency DCT coefficients and the customer’s/buyer’s watermark is embedded in the DC coefficients after they buy/obtain the digital media from the Digital Rights Management (DRM) system. The purpose of the proposed watermarking scheme is to protect the digital media, allow the tracing of primary source and identify pirated digital media.

First, the owner’s watermark is embedded. A binary image is chosen as the owner’s watermark and is pre-processed using Arnold transform and reshaped to a one-dimension sequence. Arnold transform could shuffle the binary image and increase the security of the watermark. A transform key is sent and stored in the DRM system. Next, the original image is separated to an 8×8 block without overlapping and each block is transformed using DCT. After that, the coefficients of the blocks are compared and 15 blocks with low-frequency coefficients are chosen to embed the one-dimension watermark sequence based on predefined rules. After embedding the watermark, inverse DCT Transform is utilized to obtain the watermarked image.

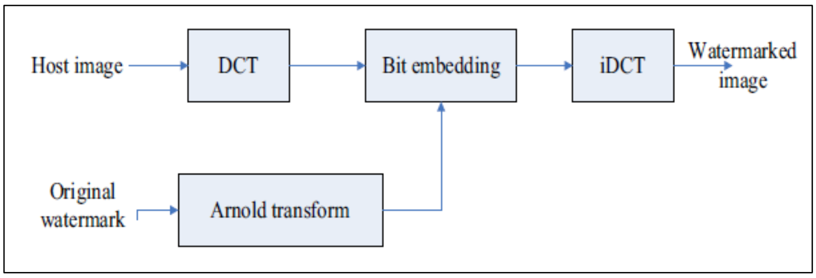


Figure 7: Owner’s Watermark Embedding Process

Then, the customer’s watermark is a 48-bit string of MAC address of the customer. The original image here is the owner-watermarked image from the previous step. Similarly, the watermarked image is separated to 8×8 blocks without overlapping and each block is transformed with DCT. 48 DC coefficients are selected based on the customer’s watermark as the embedding bit and is embedded using predefined rules. Lastly, using inverse DCT transform, the final watermarked image is obtained.

The experimental result of this paper is done with a grayscale “Lena” picture, it is shown that the watermark is not easy to be discovered by eyes easily. In conclusion, this watermarking scheme utilizes DCT Transform for both watermark and is useful to assist in managing the digital medias in DRM system.

2.5.7 **Dual Watermarking for Image Tamper Detection and Self-recovery** (Q. Han et al., 2013)

This paper proposed a dual watermarking method that has the function of tamper location and self-recovery. Robust and fragile watermarking techniques are combined and used in this proposed method. Besides that, eigenface information is utilised in robust watermarking to be embedded in the original image as watermark. The restoration of tampered region is achieved by using the embedded eigenface to low frequency sub band.

The fragile watermarking is applied using Least Significant Bits (LSB) algorithm which the watermark is embedded to the lowest level of pixel value to ensure the image quality is not significantly affected. First, the watermark information is converted into binary vector. Then, the binary vector is substituted into the least significant bit of the image. Finally, the binary data is converted back to decimal data.

Next, for robust watermarking, the watermark is the eigenface generated from the original face image. The original image is divided in LL, LH, HL and HH, four sub-bands. LL is selected to be the embedding region because the wavelet conversion characteristic states that the low frequency sub band contains the majority of the wavelet image decomposition's energy. Lastly, the image is applied with inverse wavelet transform to obtain the watermarked image.

The proposed method is examined using a random face image from ORL face database, by tampering the nose of the image with regular square and the result shows that the tampered region is able to be detected and recovered.

2.5.8 Blind and safety-enhanced dual watermarking algorithm with chaotic system encryption based on RHFM and DWT-DCT (Li et al., 2021)

This paper proposed a dual watermarking method for copyright protection based on Radial Harmonic Fourier Moments (RHFMs), Discrete Wavelet Transform and Discrete Cosine Transform (DWT-DCT). Additionally, to increase the security of the watermark embedding process, a non-adjacent linked map lattice chaotic system was employed. First, the original image is DCT transformed. Then, the origin's direction information is computed and embedded in RHFM domain. Next, this image that is embedded with direction information is transform with DWT and a low-frequency sub band is identified and separated into 8×8 blocks without overlapping. After that, each block is DCT transformed and two blocks with lowest frequency coefficients are selected as the watermark embedding region.

This research paper has a few major contributions. First, the watermarking process is encrypted to achieve security purpose. Next, secret sequences used for watermarking is generated using NCML chaotic system could help to achieve security purpose also. Furthermore, to avoid rotation attacks, the direction information is embedded into RHFMs, this helps the watermarked image to return to their original direction after any rotation attacks. Nevertheless, to prevent unauthorised watermark embedding, a standard watermark is encrypted using zero-watermarking to provide a distinctive watermark for each carried image. Lastly, the two watermarks including zero-watermark and normal watermark are both useful for copyright protection.

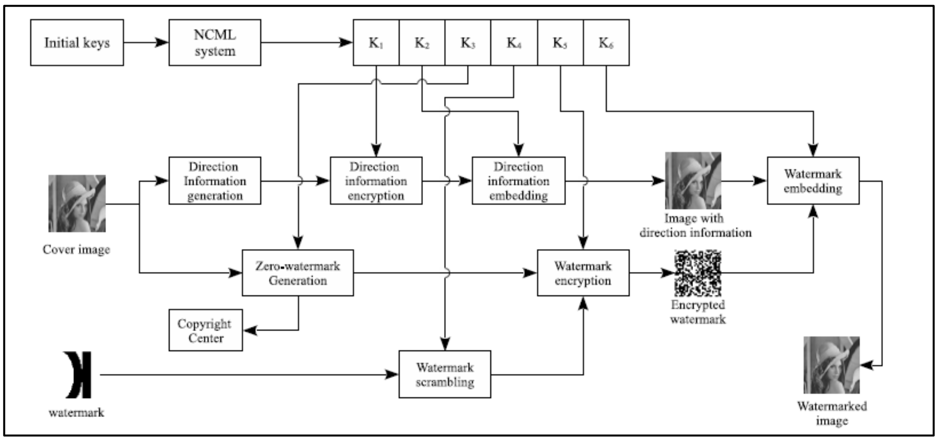


Figure 8: Flowchart of Proposed Watermarking Algorithm

To evaluate the proposed watermarking scheme, different kind of attacks are tested on the watermarked image including noise attack, cropping attack and rotation attack, the result shows that the watermarking scheme has good availability and has high imperceptibility. There are some limitations of the watermarking scheme which are inaccurate direction information and time-consuming direction information process.

2.6 Summary of Existing Watermarking Schemes

Table 1: Summary of Existing Watermarking Scheme

	(Kiatpapan & Kondo, 2015)	(Deepa B. Maheshwari, 2018)	(Han et al., 2013)	(Al-Gindy et al., n.d.)	(Lim et al., 2008)	(Liao & Liu, 2010)	(Q. Han et al., 2013)	(Li et al., 2021)
Watermarking Method	-	DWT-SVD	DWT	DCT	DWT	DCT	Wavelet Transform	RHFM and DWT-DCT
Embedding region	LSB plane	-	LH_1, LL_1	16 low-frequency band	Pseudorandom number generator initialized with secret key	15 low-frequency band	LL	LL_1
Watermark Action before Embedding	Convert to binary	DWT & SVD	Arnold Transform & DWT	Shuffle with secret key	-	Arnold Transform	Eigenfaces	Encryption RHFM DWT-DCT
Host Image Size	512×512	512×512	256×256	512×512	-	384×384	-	512×512
Watermark Size	128×128	128×128 64×64	75×75 64×64	96×64	200 bits	64×64 48 bits	-	32×32

Watermark Image Type	Binary	Grayscale	Binary & Complex Binary	Binary & Grayscale	Binary	Binary	Grayscale	Grayscale
Psychovisual Threshold	-	-	VCS	-	ROI	-	-	-
Advantages	Sensitive to image tamper	Better robustness and imperceptibility compared to solely DWT or SVD solution.	Improved the security, robustness and imperceptibility.	Watermarks can be extracted independently of the original image.	Implementation of edge information avoid the interference of two watermarks.	Embed watermark from two parties: owner and customer.	Satisfying ability for tamper localization and self-recovery.	Direction information is embedded to prevent rotation attack.
Disadvantages	Unable to recover image that is tampered across the whole image.	-	-	-	-	-	Implementation of Eigenface is suitable for image with faces only.	The direction correction process could be enhanced to consume less time.

CHAPTER 3

METHODOLOGY

3.1 Introduction

Chapter 3 discussed the software and hardware requirement to develop and test the proposed watermarking scheme. Besides, it discussed in details the proposed embedding watermarking scheme for both robust watermark and fragile watermark. Next, proposed watermark extraction scheme is discussed. Furthermore, this chapter also consists the evaluation plan and Gantt chart.

3.2 Software & Hardware Requirement

Table 2: Software and Hardware Requirement

Software Requirement		
MatLab R2022a©	For codes development and testing	
Hardware Requirement		
Computer	Operating Systems	• Windows 10 (version 1709 or higher) • Windows 7 Service Pack 1 • Windows Server 2019 • Windows Server 2016
	Processors	• **Minimum**: Any Intel or AMD x86-64 processor • **Recommended**: Any Intel or AMD x86-64 processor with four

		logical cores and AVX2 instruction set support
	Disk	• **Minimum**: 3 GB of HDD space for MATLAB only, 5-8 GB for a typical installation • **Recommended**: An SSD is recommended
	RAM	• **Minimum**: 4 GB • Recommended: 8 GB

3.3 Proposed Embedding Watermark Scheme

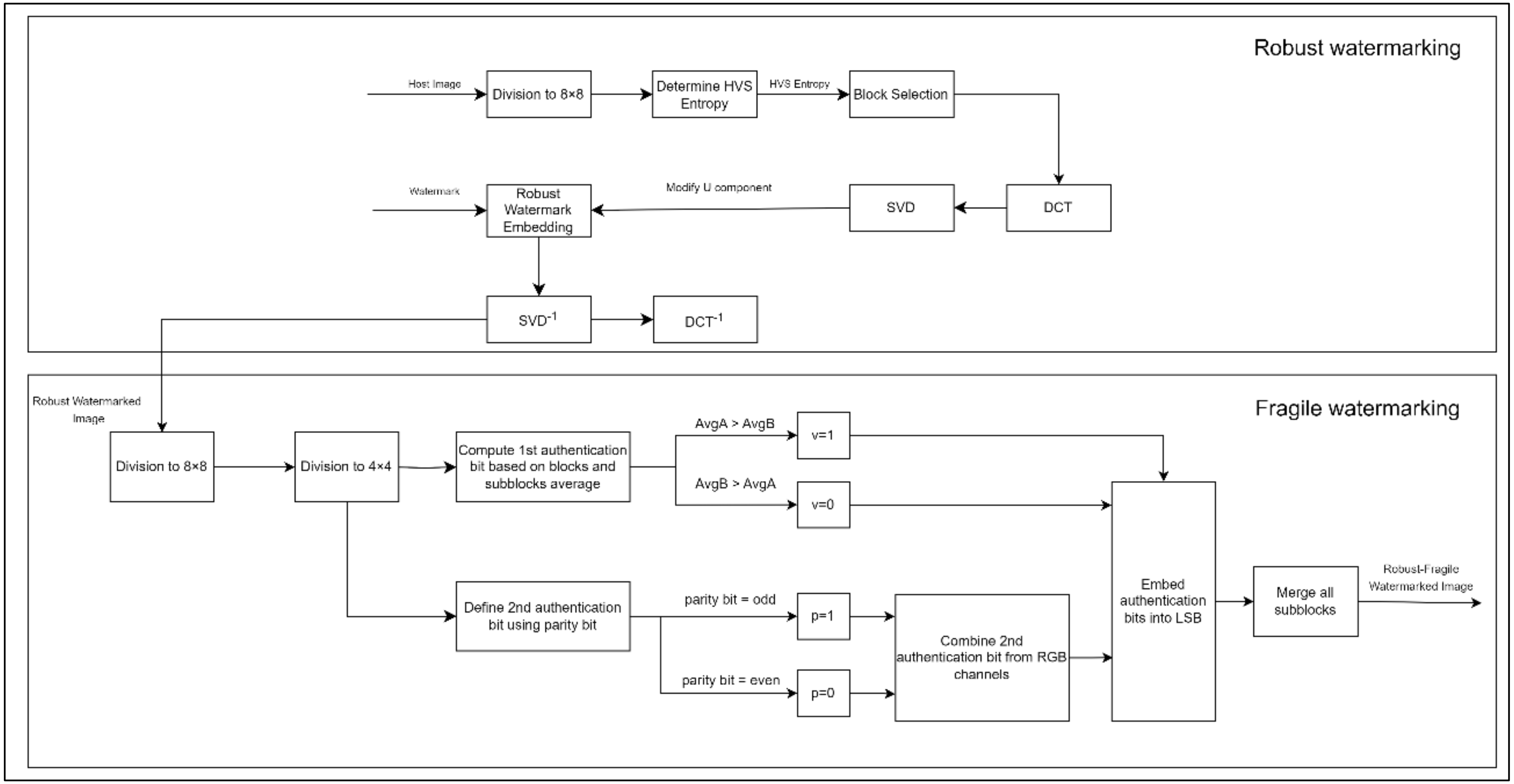


Figure 9: Proposed Embedding Watermark Block Diagram

3.3.1 Robust Watermark Embedding Algorithm

Step 1: Separate the cover image into 4×4 non-overlapping blocks.

Step 2: Calculate the HVS entropy value for every non-overlapping block.

Step 3: Choose the blocks with the lowest HVS entropy values and record the x and y coordinates.

Step 4: For each non-overlapping selected block, use DCT, to obtain DCT domain frequency bands.

Step 5: Apply SVD to all blocks that have transformed with DCT.

Step 6: Each binary watermark bit is embedded by modifying orthogonal matrix U.

Step 7: Implement the inverse SVD on every selected block, followed by the inverse DCT.

Step 8: Reassemble the watermarked image by combining all of the modified selected blocks.

3.3.2 Authentication Bit Embedding

Step 1: Separate the cover image into 8×8 non-overlapping blocks. Next, every block is split into four sub-blocks of 4×4 pixels each.

Step 2: The average pixel value of every image block and sub-block is calculated.

Step 3: The first authentication bits, v were calculated by assessing the average image block, AvgA to each of its sub-block, AvgB. Embed first authentication bit in Least Significant Bit (LSB).

$$\text{If } AvgA > AvgB,\ v = 1,$$

$$\text{If } AvgB > AvgA,\ v = 0,$$

Step 4: Each sub-block's parity bits are used for the creation of the second authentication bits, p. Combine parity bits frm RGB channels. Embed parity bit into LSB.

If parity number is odd, then p = 1,

If parity number is even, then p = 0.

Step 6: The embedding steps are repeated for all subblocks.

Step 7: Merge all subblocks.

3.4 Proposed Watermark Extraction Scheme

3.4.1 Fragile Watermark Extraction

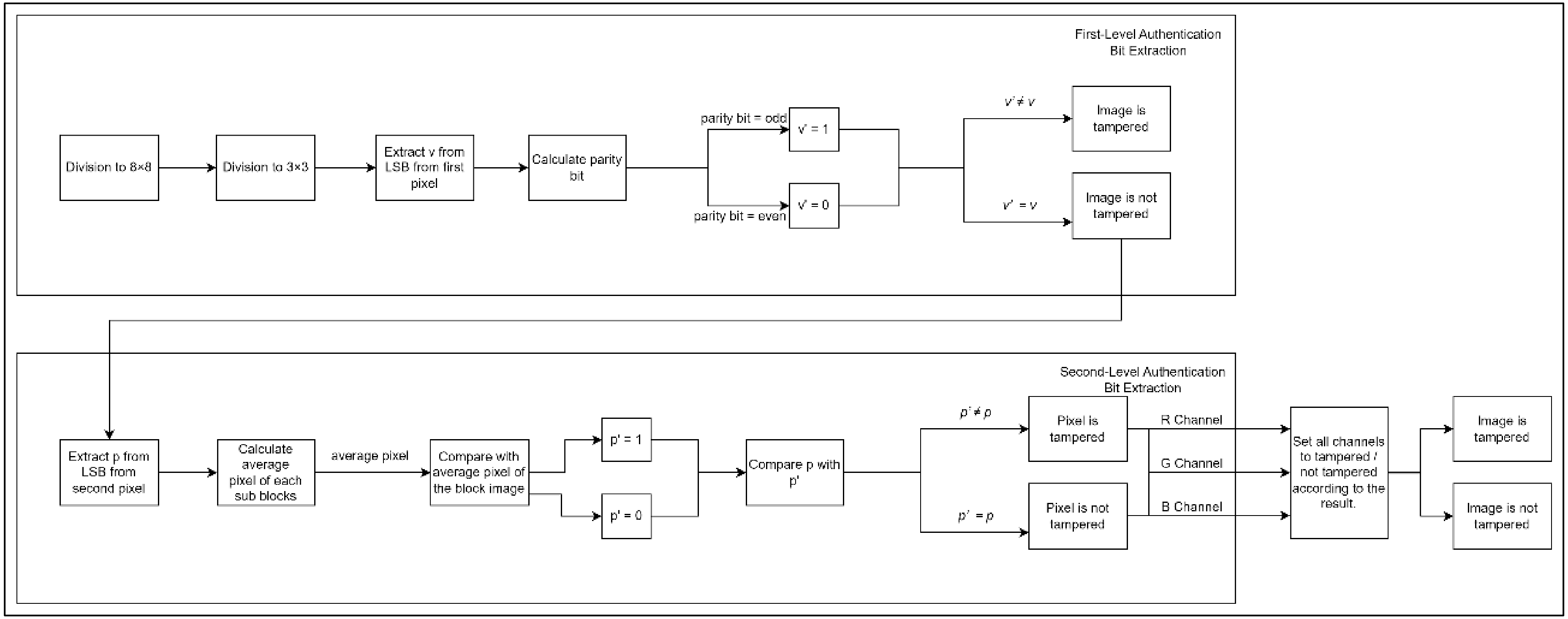

First-Level Authentication Bit Extraction
Division to 8×8
Division to 3×3
Extract v from LSB from first pixel
Calculate parity bit
parity bit = odd
v' = 1
parity bit = even
v' = 0
v' ≠ v
Image is tampered
v' = v
Image is not tampered
Second-Level Authentication Bit Extraction
Extract p from LSB from second pixel
Calculate average pixel of each sub blocks
average pixel
Compare with average pixel of the block image
p' = 1
p' = 0
Compare p with p'
p' ≠ p
Pixel is tampered
p' = p
Pixel is not tampered
R Channel
G Channel
B Channel
Set all channels to tampered / not tampered according to the result.
Image is tampered
Image is not tampered

Figure 10: Fragile Watermark Extraction Block Diagram

First-level Authentication Bit Extraction:

Step 1: Divide tampered image to 8×8 pixels non-overlapping image blocks.

Step 2: Divide each block to four 4×4 pixels sub blocks.

Step 3: Extract bit v from LSB of first pixel in sub blocks.

Step 4: Calculate the parity bit and determine v’ with the rules:

If parity is odd, then v’ = 1,

If parity is even, then v’ =0

Step 5: Determine image tamper with the rules:

If v’ ≠ v, then image is tampered,

If v’ = v, then image is not tampered.

Step 6: If v’ and v has same bit value, proceed to second-level authentication.

Second-level Authentication Bit Extraction:

Step 1: Extract bit p from LSB plane from LSB on the second pixel in the sub block.

Step 2: Calculate average pixel of each sub blocks, A and compare them with average pixel of the block image, A’ to determine p’ with the rules:

If A > A’, then p’ = 1,

If A’>A, then p’ = 0.

Step 3: Compare p with p’. p’ denotes the algebraic relationship between 4×4 pixels sub blocks and 8×8 pixels sub blocks.

Step 4: Determine image tamper with:

If p’ ≠ p, then image is tampered,

If p’ = p, then image is not tampered.

Step 5: Repeat for RGB channels. Align the result for all the RGB channels.

Step 6: Mark the pixel if it is tampered.

3.4.2 Robust Watermark Extraction

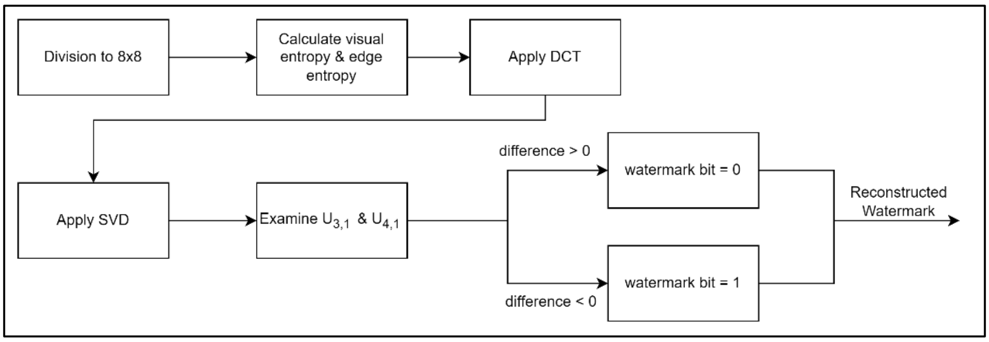


Figure 11: Watermark Extraction Block Diagram

Step 1: The image is divided into 8×8 pixels.

Step 2: The visual entropy and edge entropy is calculated, to determine the area where the watermark is embedded.

Step 3: Apply DCT Transformation to the selected blocks to obtain the n DCT domain frequency bands.

Step 4: Apply SVD to the DCT transformed blocks.

Step 5: Examine the $U_{3,1}$ and $U_{4,1}$ of the U matrix, compute the absolute difference of $U_{3,1}$ and $U_{4,1}$, d.

Step 6: Determine the watermark bit based on the rules below:

If d > 0, then binary watermark bit = 1,

If d<0, then binary watermark bit = 0.

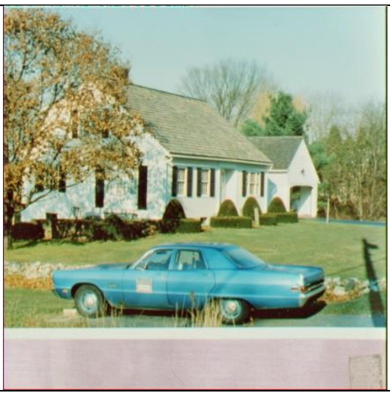
Step 7: Use the obtained watermark bit to reconstruct the watermark.

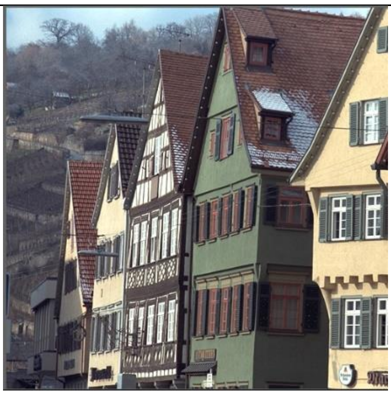
3.5 Evaluation Plan

The watermarking scheme is evaluated based on the quality of the watermark and tamper localization ability.

3.5.1 Host Images & Watermark Image

The host image is obtained from the database of USC Viterbi School of Engineering (*SIPI Image Database - Misc*, n.d.). 8 random images are selected to do the experiment without considering the image color or characteristics to ensure a fair result. The host images are of size of 512 × 512 pixels.

 (a) Parrot	 (b) Lighthouse
 (c) Ball	 (d) Kid
	

(e) Car	(f) Lady
 (g) Sailboat	 (h) Houses

The watermark image is a Chinese character that is famous in digital watermarking scheme experiment. The watermark is in size of 32 × 32 pixels.

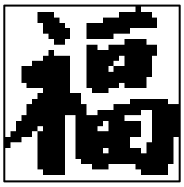


Figure 12: Watermark Logo

3.5.2 Attack Analysis

The proposed scheme will be tested under various attacks. The following are the brief description of each attack.

1. Cropping – Crop away 12.5% and 50% of the centre of a host image, 12.5%, 25% and 50% of row of the host image and 12.5%, 25% and 50% of column of the host image.

2. Gaussian Low-pass Filter – Gaussian Low-pass Filter removes the high frequency characteristics of the images on either X or Y axis. It will cause losing of clarity on the image or a blurring effect on the image. The size of filter used are 3×3, 5×5 and 7×7.

3. Salt-and-Pepper Noise – Salt-and-Pepper noise is also referred as impulse noise. It makes some pixels in the image to be noisy. The noise density are 0.01% and 0.001%.

4. Regular Shape Tamper – The proposed scheme will be tampered using regular shape including rectangle and square. The percentage of the shape coverage are 12.5% centre, 50% centre, 12.5% row, 25% row, 50% row, 12.5% column, 25% column and 50% column.

5. Irregular Shape Tamper – The image is tampered with copy and move and color modfication.

3.6 Watermarking Scheme Performance Metrics

3.6.1 Watermark Quality Evaluation

The watermarked image quality is evaluated twice that are on robust watermark and robust-fragile watermark. The evaluation of robust watermark will be done after the first watermark is embedded and before the second watermark is embedded. Moreover, the evaluation of robust-fragile watermark will be done after both watermarks are embedded. The parameters that will be used for imperceptibility evaluation are Peak Signal-To-Noise Ratio (PSNR), Absolute Reconstruction Error (ARE) and Structural Similarity Index Measure (SSIM), and evaluation for robustness are measured with Normalized Correlation (NC) value and Bit Error Rate (BER).

PSNR is defined as the ratio of a signal's maximum possible value (power) to the power of distorting noise that impacts the quality of its representation. It is commonly used in assessing the quality of image compression by comparing the original and a compressed image. The higher the PSNR, the higher the quality of the image after embedding with watermark. The formula of PSNR is:

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

where the formula of Mean Squared Error (MSE) is:

$$MSE = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(f(k,l) - g(k,l))^2$$

SSIM is a parameter used to measure the similarity of two pictures. In the evaluation, it is used to compare the watermarked image and the original image. The formula of SSIM is:

$$SSIM(x,y) = [l(x,y)]^{\alpha} \cdot [c(x,y)]^{\beta} \cdot [s(x,y)]^{\gamma}$$

where $\alpha > 0, \beta > 0, \gamma > 0$ are used to define the significance of the components of luminance (l), contrast (c) and structure (s).

ARE is parameter of the difference between the original and reconstructed image which is the image after watermark embedding. The formula of ARE is:

$$ARE = \frac{1}{MN}\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} |f(k,l) - g(k,l)|$$

The NC value is used to assess the similarity of extracted watermark and original watermark. The formula of NC value is:

$$NC = \frac{\sum_i w_i {w_i^*}^2}{\sum_i w_i^2}$$

Bit Error Rate (BER) is often used to evaluate the performance of the watermarking algorithm under various attacks or distortions. The BER measures the accuracy of watermark detection after the watermarked content has been subjected to different types of attacks or distortions. A lower BER indicates higher robustness, meaning that the watermark can withstand various attacks or distortions and still be accurately detected. It demonstrates the ability of the digital watermarking scheme to maintain the integrity and robustness of the embedded watermark in the presence of potential attacks or distortions.

3.6.2 Tamper Localization Ability

Tamper localization of the watermark is evaluated using the Confusion Matrix including True-Positive Rate (TPR), False-Negative Rate (FNR), False-Positive Rate (FPR) and True-Negative Rate (TNR) and F1 Score. TPR is the ratio of the detected area to the real tampered area. The higher the TPR, the more accurate the tamper detections in the tampered regions. On the other hand, FNR is the ratio of the undetected area to the actual tampered area. The higher the FNR indicates the more inaccurate the tamper detection in the tampered area of the images. The formula of TPR and FNR are defined as:

$$TPR = \frac{TP}{TP + FN} = \frac{TP}{P} = 1 - FNR$$

$$FNR = \frac{FN}{TP + FN} = \frac{FN}{P} = 1 - TPR$$

Where TP denotes the true-positive tampered pixels number, FN denote the false-negative tampered pixels number and P denotes real tampered pixels number.

Next, FPR is a ratio that of the false detected region to the untampered region. The FPR value range is from 0 to 1. The greater the FPR value, the larger the detection of the untampered region as tampered region or false detection. TNR is a ratio of non-detected region to untampered region. The formula of FPR and TNR are defined as:

$$FPR = \frac{FP}{FP + TN} = \frac{FP}{N}$$

$$TNR = \frac{TN}{FP + TN} = \frac{TN}{N}$$

where FP denotes the false-positive tampered pixels number, TN denotes the true-negative tampered pixels number, and N denotes the untampered pixels number. In short, the meaning of confusion matrix is summarized in the table below.

Table 3: Confusion Matrix Summary

Tampered?	Tamper localization	Confusion Matrix
Tampered	Detected	True-positive
Tampered	Not detected	False-positive
Not tampered	Detected	False-negative
Not tampered	Not detected	True-negative

F1-Score is an indicator that considers precision and recall together. It is commonly referred to as the harmonic mean, which is a kind of average calculation for ratios.

The formula of F1-Score is:

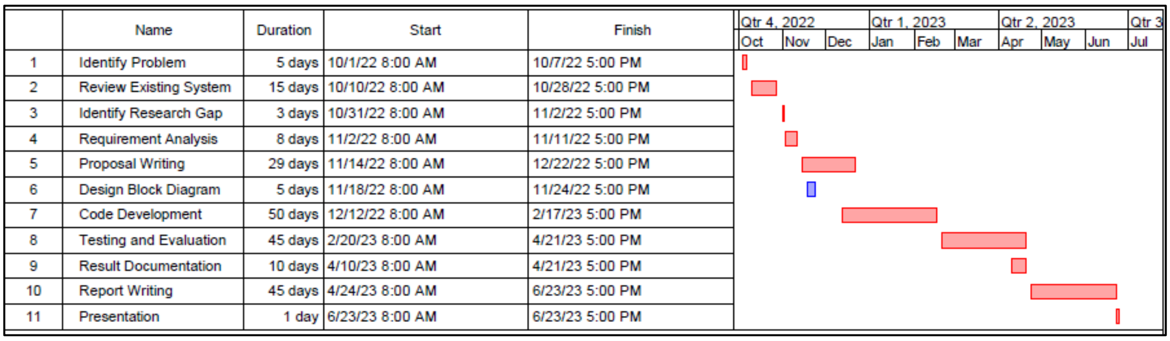
$$F1 - Score = 2 * \frac{Precision * Recall}{Precision + Recall}$$

where the formula of precision and recall are defined as:

$$Precision = \frac{TP}{TP + FP} = \frac{TPR}{TPR + FPR}$$

$$Recall = \frac{TP}{TP + FN} = \frac{TPR}{TPR + FNR}$$

3.7 Gantt Chart



	Name	Duration	Start	Finish
1	Identify Problem	5 days	10/1/22 8:00 AM	10/7/22 5:00 PM
2	Review Existing System	15 days	10/10/22 8:00 AM	10/28/22 5:00 PM
3	Identify Research Gap	3 days	10/31/22 8:00 AM	11/2/22 5:00 PM
4	Requirement Analysis	8 days	11/2/22 8:00 AM	11/11/22 5:00 PM
5	Proposal Writing	29 days	11/14/22 8:00 AM	12/22/22 5:00 PM
6	Design Block Diagram	5 days	11/18/22 8:00 AM	11/24/22 5:00 PM
7	Code Development	50 days	12/12/22 8:00 AM	2/17/23 5:00 PM
8	Testing and Evaluation	45 days	2/20/23 8:00 AM	4/21/23 5:00 PM
9	Result Documentation	10 days	4/10/23 8:00 AM	4/21/23 5:00 PM
10	Report Writing	45 days	4/24/23 8:00 AM	6/23/23 5:00 PM
11	Presentation	1 day	6/23/23 8:00 AM	6/23/23 5:00 PM

Figure 13: Gantt Chart

CHAPTER 4

RESULTS AND DISCUSSION

4.1 Introduction

Chapter 4 presents the results and discussion of the proposed watermarking algorithm. The chapter is divided into three main sections: imperceptibility performance, robustness performance, and tamper localization. In the imperceptibility performance section (section 4.2), the quality of the watermarked images is evaluated in terms of their visual quality and distortion level. The robustness performance section (section 4.3) evaluates the effectiveness of the proposed algorithm under various attacks, including regular tamper, irregular tamper combined with image processing attacks, and a comparison of robustness performance with other state-of-the-art methods. Specifically, section 4.3 includes three sub-sections: image processing attack with regular tamper (section 4.3.1), irregular tamper + image processing attack (section 4.3.2), and robustness comparison of normalized correlation (NC) values with other methods (section 4.3.3). Finally, in section 4.4, the tamper localization performance of the proposed algorithm is evaluated, with the results of the experiment presented and discussed. Overall, this chapter provides a comprehensive evaluation of the proposed algorithm's performance and its suitability for real-world applications.

4.2 Imperceptibility Performance

The imperceptibility of watermark is evaluated after embedding first watermark and after embedding both watermarks. The experiment was conducted on a set of eight images. The performance of the image reconstruction algorithm was evaluated using three different metrics: Absolute Reconstruction Error (ARE), Peak Signal-to-Noise Ratio (PSNR), and Structural Similarity Index (SSIM).The explanation of these parameters is mentioned in 3.5.3 Watermark Quality Evaluation. The imperceptibility performance of the proposed watermarking scheme is shown at **Error! Reference source not found.**.

Table 4: ARE, PSNR and SSIM of Various Host Images after Embedding Watermark for Copyright Protection and After Embedding Watermark for Copyright Protection and Authentication Bit

	After Embedding Watermark for Copyright Protection			After Embedding Watermark for Copyright Protection and Authentication Bit		
	ARE	PSNR	SSIM	ARE	PSNR	SSIM
Parrot	0.3204	49.9867	0.9936	0.3434	49.8258	0.9934
Lighthouse	0.3336	49.7177	0.9912	0.3531	49.5531	0.9911
Ball	0.3530	48.4600	0.9931	0.3731	48.3365	0.9930
Kid	0.2514	53.1876	0.9968	0.2712	52.7398	0.9967
Car	0.4688	46.1104	0.9834	0.4911	46.0613	0.9834
Lady	0.3242	50.5095	0.9935	0.3457	50.3172	0.9934
Sailboat	0.4312	47.1846	0.9840	0.4518	47.1043	0.9839
Houses	0.5327	43.4170	0.9894	0.5532	43.3803	0.9894
Average	0.3769	48.5717	0.9906	0.3978	48.4148	0.9905

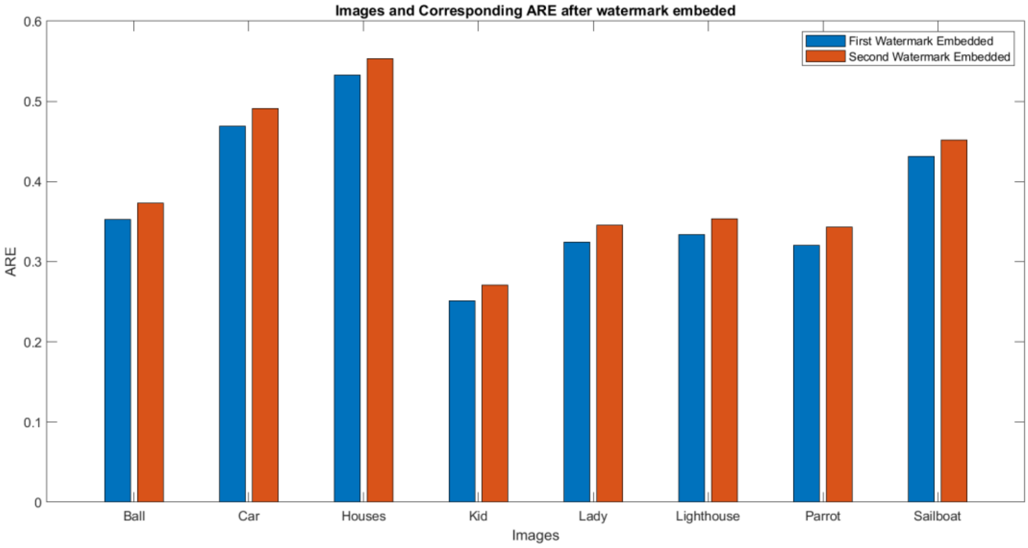


Figure 14: Images and Corresponding ARE after Watermark Embedded

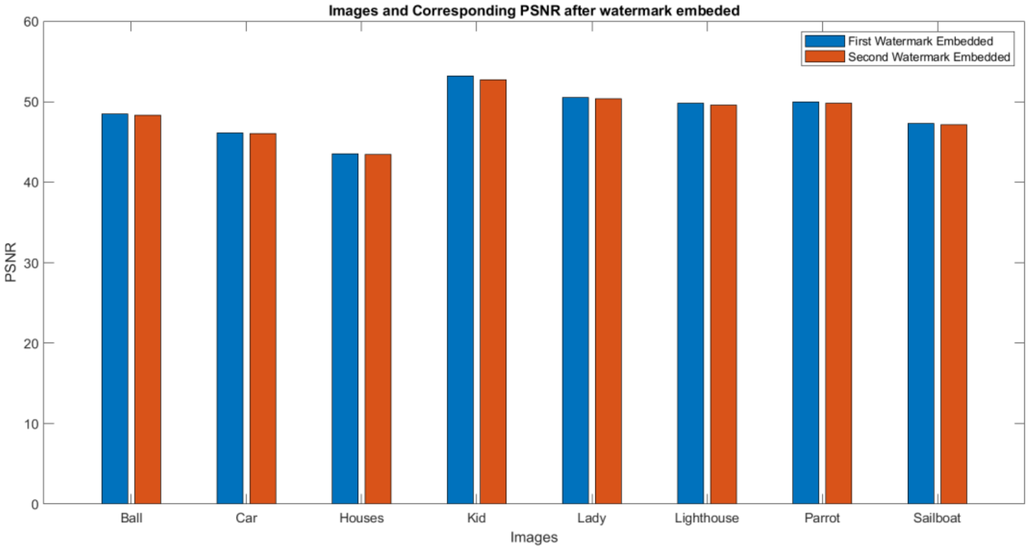


Figure 15: Images and Corresponding PSNR after Watermark Embedded

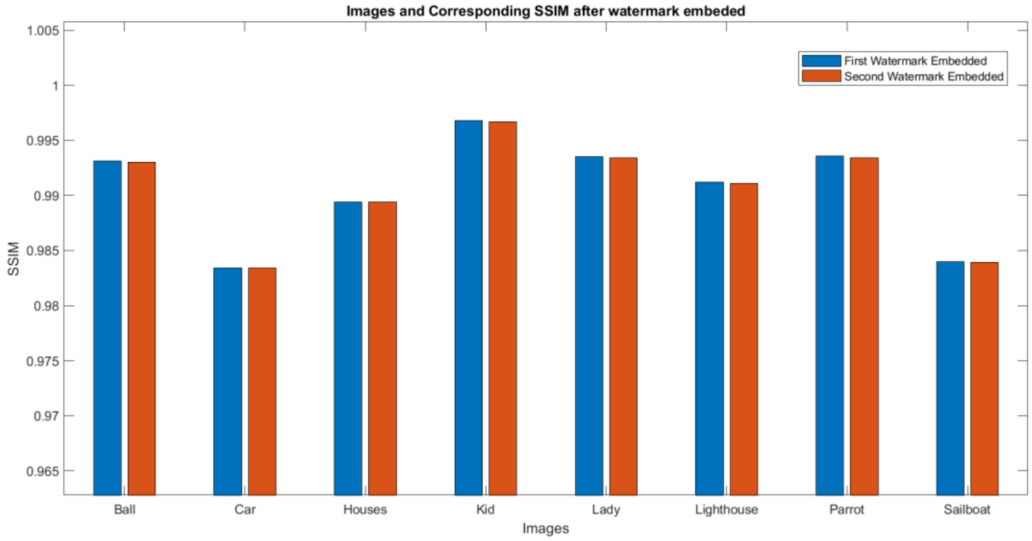


Figure 16: Images and Corresponding SSIM after Watermark Embedded

The experiment was conducted on a set of eight images to evaluate the performance of an image watermarking algorithm. Two different watermarks were embedded in each image and the quality of the resulting watermarked images was measured using three different metrics: Absolute Reconstruction Error (ARE), Peak Signal-to-Noise Ratio (PSNR), and Structural Similarity Index (SSIM).

After embedding the first watermark, the ARE values ranged from 0.2514 to 0.5327, with an average value of 0.3769. The PSNR values ranged from 43.4170 to 53.1876, with an average value of 48.5717. The SSIM values ranged from 0.9834 to 0.9968, with an average value of 0.9906. The image "kid" which has lower light intensity has the highest PSNR value wheareas the image “Houses” which has higher light intensity has lowest PSNR. Therefore, it is believed that an image with higher light intensity is harder to achieve high imperceptibility, and vide versa.

After embedding both watermarks, the ARE values ranged from 0.2712 to 0.5532, with an average value of 0.3978. The PSNR values ranged from 43.3803 to 52.7398, with an average value of 48.4148. The SSIM values ranged from 0.9834 to 0.9967, with an average value of 0.9905. The value performed slightly worse than after embedding first watermark only, it is because the second watermark embedding had made changes to the least significant bit of the image.

Overall, the results indicate that the algorithm was able to embed both watermarks into the images with relatively low ARE values and high PSNR and SSIM values, indicating good reconstruction quality and high similarity between the original and watermarked images.

4.2.1 Comparison of PSNR and SSIM Values with (LUSIA RAKHMAWATI et al., 2017) and (Al-Otum & Ellubani, 2022)

The data above represents the performance evaluation of a proposed scheme, conducted by Lusia Rakhmawati et al. in 2017, and a scheme developed by Al-Otum and Ellubani in 2022. The evaluation measures the quality of the watermarked images using two metrics: Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM).

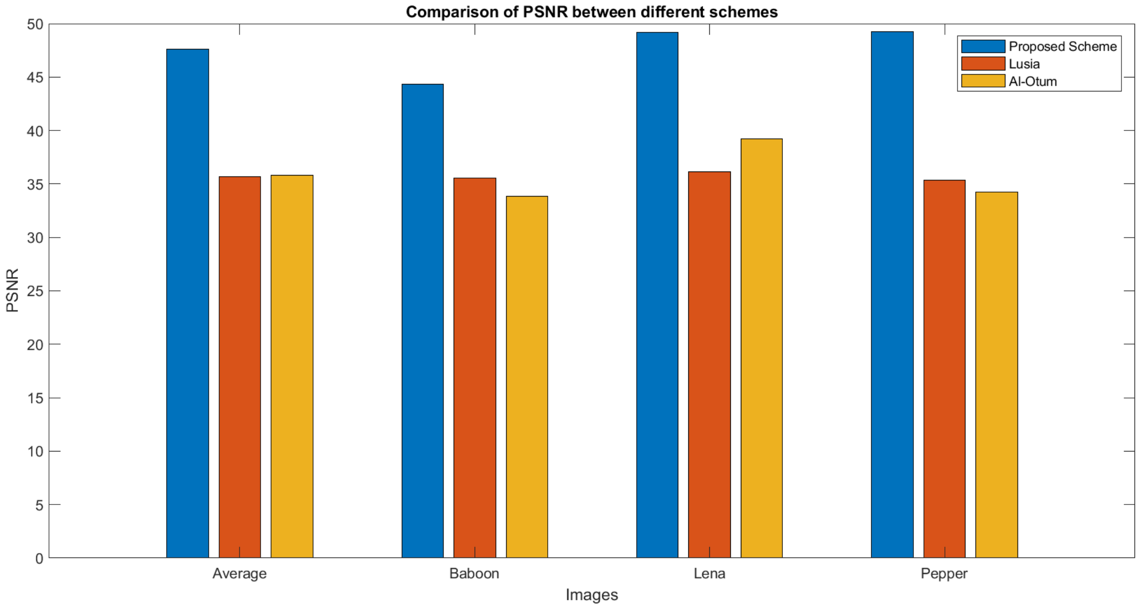
The table shows the PSNR and SSIM values for three different test images: Lena, Baboon, and Pepper. For each test image, the values are provided for the proposed scheme (Rakhmawati et al., 2017) and the scheme developed by Al-Otum and Ellubani(2022).

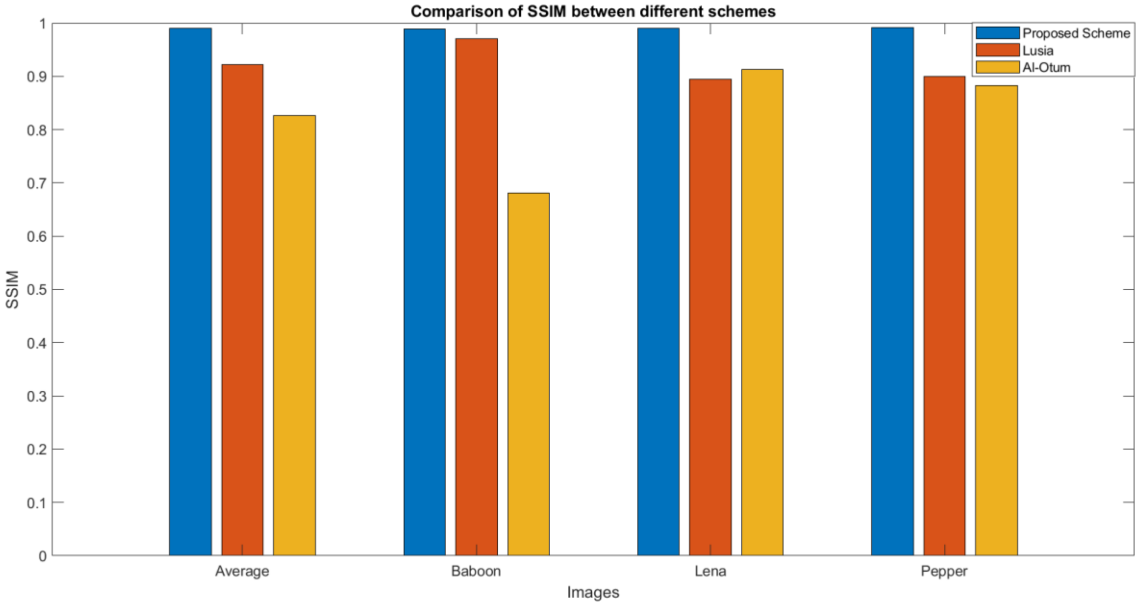
Looking at the results, we can see that for all three test images (Lena, Baboon, and Pepper), the proposed scheme (Rakhmawati et al., 2017) consistently achieves higher PSNR and SSIM values compared to the scheme developed by Al-Otum and Ellubani (2022). This indicates that the proposed scheme produces watermarked images with better overall quality and structural similarity to the original images.

The average values across all test images show that the proposed scheme has an average PSNR of 47.5781 and an average SSIM of 0.9900, while the scheme developed by Al-Otum and Ellubani has an average PSNR of 35.6753 and an average SSIM of 0.9217. These average values further support the conclusion that the proposed scheme performs better in terms of image quality and structural similarity.

Table 5: Comparison of PSNR and SSIM Values

	Proposed Scheme		(Lusia Rakhmawati et al., 2017)		(Al-Otum & Ellubani, 2022)	
	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
Lena	**49.1847**	**0.9900**	36.1340	0.8950	39.2500	0.9130
Baboon	**44.3339**	**0.9892**	35.5450	0.9700	33.8300	0.6810
Pepper	**49.2157**	**0.9909**	35.3470	0.9000	34.2600	0.8830
Average	**47.5781**	**0.9900**	35.6753	0.9217	35.7800	0.8257


Comparison of PSNR between different schemes
PSNR
0
5
10
15
20
25
30
35
40
45
50
Average
Baboon
Lena
Pepper
Images
Proposed Scheme
Lusia
Al-Otum


Comparison of SSIM between different schemes
SSIM
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
Average
Baboon
Lena
Pepper
Images
Proposed Scheme
Lusia
Al-Otum

4.3 Robustness Performance

Robustness of the watermark is evaluated by NC and BER. The watermarked images are applied with single attacks and combination attacks which are regular tamper + image processing attacks and irregular tamper + image processing attacks. NC and BER are calculated after the attacks to ensure the robustness of the embedded watermark.

4.3.1 Single Attack

The attacks including Gaussian Lowpass Filter, Gaussian Noise, Speckle Noise, Salt & Pepper Noise, Sharpening, Scaling, JPEG Compression and JPEG2000 Compression with different parameters. Table 6 shows the result of NC and BER of extracted wateramark after a single attack.

The table presents the results of various image processing techniques applied to different images, evaluated using the metrics of Normalized Cross-Correlation (NC) and Bit Error Rate (BER). Among the techniques analyzed, Gaussian Lowpass Filters with kernel sizes of (3,1) and (5,1) demonstrate strong performance, indicated by high NC values and low BER values. These filters effectively reduce noise and blur in the images, resulting in enhanced image quality and minimal distortion.

When Gaussian noise is added to the images, with noise levels of 0.003 and 0.001, the performance is slightly affected, as evidenced by the moderate NC and BER values. The presence of Gaussian noise introduces some degradation to the image quality, but the images remain recognizable. Similarly, the application of Speckle Noise with a noise level of 0.001 achieves notable results, with high NC values and low BER values. This technique effectively preserves the crucial details of the images while introducing a grainy texture.

On the other hand, the introduction of Salt & Pepper Noise, at noise levels of 0.003 and 0.001, leads to slightly lower performance compared to Gaussian and Speckle Noise. The NC values decrease, and the BER values increase, indicating a more significant impact on image quality. However, the images still retain their general features despite the presence of noise.

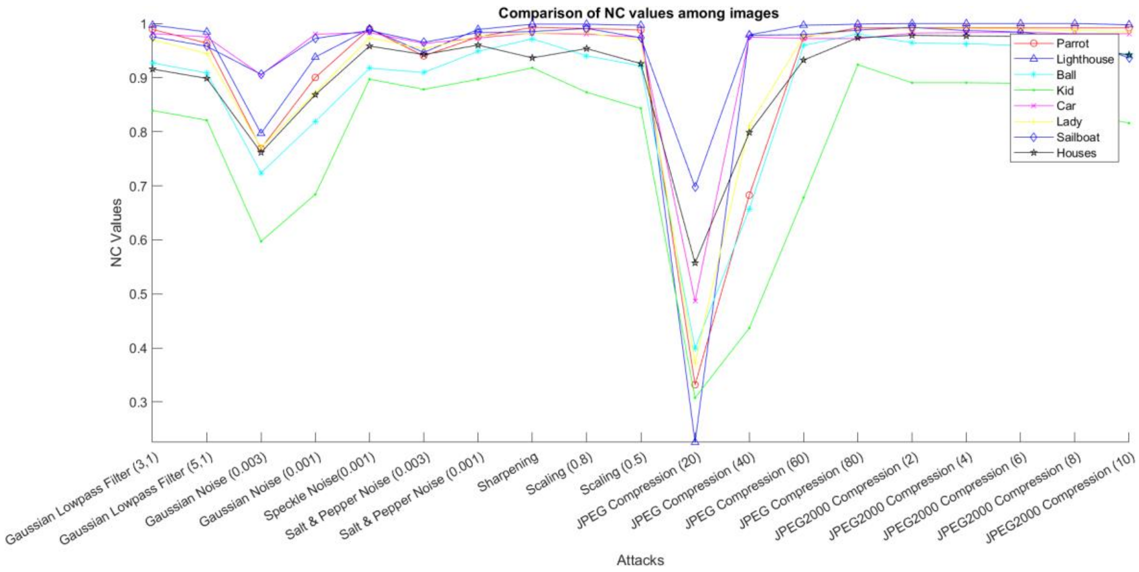
Furthermore, the application of image sharpening and scaling techniques demonstrates good performance, with high NC values and low BER values. These techniques enhance the sharpness and details of the images while maintaining their overall integrity.

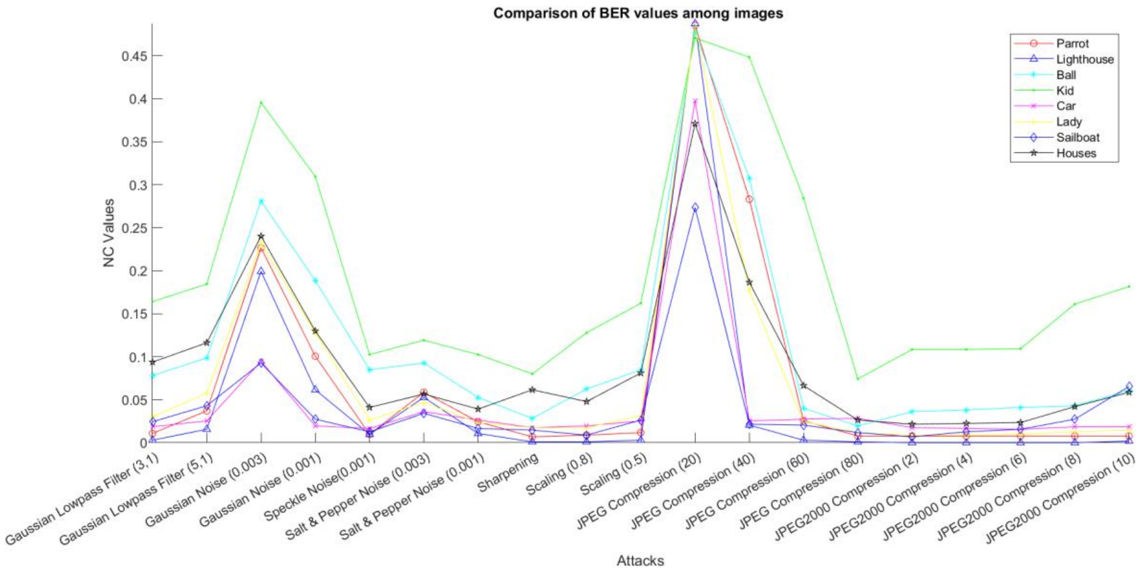
Lastly, the performance of JPEG and JPEG2000 compression techniques is evaluated. The results show that lower compression ratios, such as JPEG Compression (20), yield poorer performance in terms of NC and BER values. As the compression ratio increases, the NC values improve, and the BER values decrease, indicating better preservation of image quality. However, even at higher compression ratios, there is still some loss of image information and visible artifacts due to the compression process.

Overall, the analysis of the data highlights the effectiveness of different image processing techniques in improving or degrading image quality, based on the evaluated metrics. The choice of technique should consider the desired balance between preserving image details and reducing noise or artifacts, depending on the specific application or requirements.

Table 6: NC, BER of Extracted Watermark after Single Attack

	Parrot		Lighthouse		Ball		Kid		Car		Lady		Sailboat		Houses	
	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER
Gaussian Lowpass Filter (3,1)	0.9892	0.0107	0.9971	0.0029	0.9273	0.0781	0.8393	0.1641	0.9815	0.0186	0.9702	0.0303	0.9757	0.0244	0.9158	0.0938
Gaussian Lowpass Filter (5,1)	0.9639	0.0371	0.9847	0.0156	0.9087	0.0986	0.8213	0.1846	0.9751	0.0254	0.9447	0.0576	0.9581	0.0430	0.8986	0.1162
Gaussian Noise (0.003)	0.7690	0.2266	0.7969	0.1992	0.7237	0.2813	0.5971	0.3955	0.9052	0.0947	0.7708	0.2324	0.9061	0.0928	0.7617	0.2402
Gaussian Noise (0.001)	0.9003	0.1006	0.9381	0.0615	0.8190	0.1885	0.6841	0.3096	0.9804	0.0195	0.8717	0.1279	0.9726	0.0273	0.8685	0.1299
Speckle Noise (0.001)	0.9902	0.0098	0.9902	0.0098	0.9176	0.0850	0.8972	0.1025	0.9833	0.0166	0.9738	0.0264	0.9872	0.0127	0.9585	0.0410
Salt & Pepper Noise (0.003)	0.9403	0.0586	0.9467	0.0527	0.9095	0.0928	0.8784	0.1191	0.9632	0.0361	0.9534	0.0469	0.9655	0.0342	0.9427	0.0566
Salt & Pepper Noise (0.001)	0.9754	0.0244	0.9893	0.0107	0.9488	0.0527	0.8970	0.1025	0.9734	0.0264	0.9766	0.0234	0.9833	0.0166	0.9603	0.0391
Sharpening	0.9931	0.0068	0.9990	0.0010	0.9719	0.0283	0.9183	0.0801	0.9823	0.0176	0.9823	0.0176	0.9852	0.0146	0.9366	0.0615
Scaling (0.8)	0.9912	0.0088	0.9990	0.0010	0.9406	0.0625	0.8730	0.1279	0.9803	0.0195	0.9826	0.0176	0.9912	0.0088	0.9539	0.0479
Scaling (0.5)	0.9882	0.0117	0.9971	0.0029	0.9216	0.0850	0.8432	0.1621	0.9747	0.0254	0.9693	0.0313	0.9738	0.0264	0.9260	0.0811
JPEG Compression (20)	0.3318	0.4854	0.2254	0.4873	0.3992	0.4775	0.3077	0.4707	0.4863	0.3975	0.3721	0.4834	0.6976	0.2734	0.5573	0.3711
JPEG Compression (40)	0.6826	0.2832	0.9793	0.0205	0.6575	0.3076	0.4367	0.4482	0.9753	0.0254	0.8119	0.1768	0.9785	0.0215	0.7987	0.1865
JPEG Compression (60)	0.9744	0.0254	0.9971	0.0029	0.9596	0.0400	0.6780	0.2842	0.9722	0.0273	0.9757	0.0244	0.9793	0.0205	0.9325	0.0664
JPEG Compression (80)	0.9921	0.0078	0.9990	0.0010	0.9807	0.0195	0.9240	0.0742	0.9723	0.0283	0.9883	0.0117	0.9882	0.0117	0.9739	0.0264
JPEG2000 Compression (2)	0.9921	0.0078	1.0000	0.0000	0.9645	0.0361	0.8907	0.1084	0.9823	0.0176	0.9912	0.0088	0.9931	0.0068	0.9783	0.0215
JPEG2000 Compression (4)	0.9921	0.0078	1.0000	0.0000	0.9627	0.0381	0.8907	0.1084	0.9833	0.0166	0.9912	0.0088	0.9872	0.0127	0.9773	0.0225
JPEG2000 Compression (6)	0.9921	0.0078	1.0000	0.0000	0.9599	0.0410	0.8898	0.1094	0.9843	0.0156	0.9903	0.0098	0.9843	0.0156	0.9764	0.0234
JPEG2000 Compression (8)	0.9921	0.0078	1.0000	0.0000	0.9578	0.0430	0.8362	0.1611	0.9813	0.0186	0.9874	0.0127	0.9727	0.0273	0.9579	0.0420
JPEG2000 Compression (10)	0.9921	0.0078	0.9980	0.0020	0.9411	0.0605	0.8159	0.1816	0.9814	0.0186	0.9854	0.0146	0.9364	0.0654	0.9420	0.0586



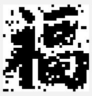
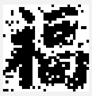
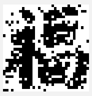
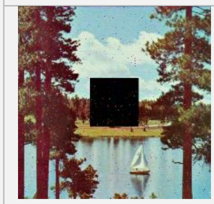
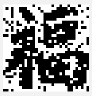
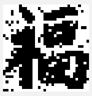
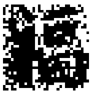
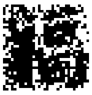
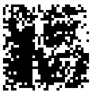
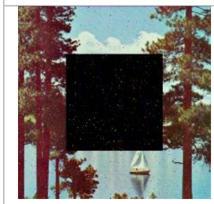
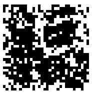
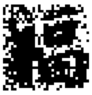
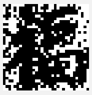
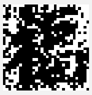
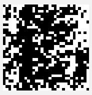


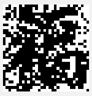
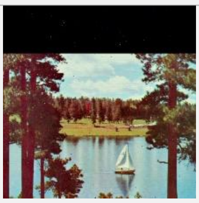
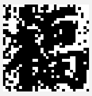
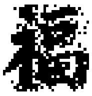
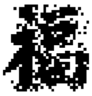
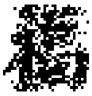
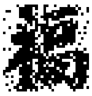
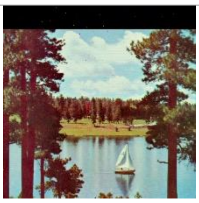
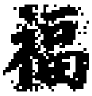
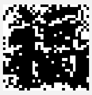
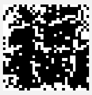
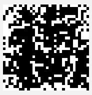
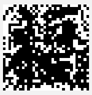
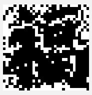
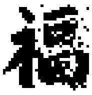
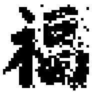
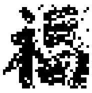
From the graph above, it is obvious that the watermarking scheme has stable performance among the images. It could withstand most of the attacks with high NC and low BER. JPEG Compression (20) attack has the highest BER values across most of the tested images which is an average of 0.4308. This suggests that the JPEG compression with a quality factor of 20 has a significant impact on the image quality and introduces a considerable amount of distortion. Thus, the watermarking scheme performed worst under JPEG Compression 20 attack. On the other hand, the watermarking scheme has the best value under JPEG Compression (80) attack which obtained an average of 0.9773 for NC and 0.0226 for BER. In short, the watermarking scheme could withstand JPEG Compression as long as the factor is not too high.

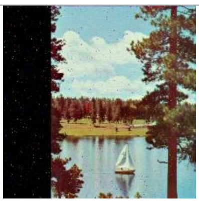
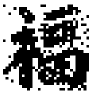
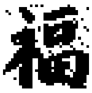
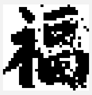
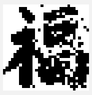
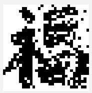
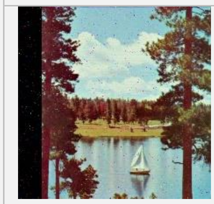
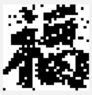
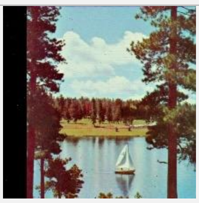
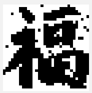
4.3.2 Regular Tamper + Image Processing Attacks

Table 7 shows NC and BER values of the extracted watermark after a series of combination attacks, which included various cropping techniques and the application of filters such as Gaussian lowpass filters and salt and pepper noise. Details of NC and BER value for all 8 images are shown in Appendix A. The average of NC and BER across all attacks for all images are 0.7678 and 0.2005 respectively.

Table 7: Visualization of Attacked Images, Extracted Watermark and NC, BER value of Extracted Watermark after Combination Attacks

Cropping Area	Image Processing Attacks	Recovered Watermark	Image Processing Attacks	Recovered Watermark	Image Processing Attacks	Recovered Watermark
Centre 12.5%	 Gaussian Lowpass Filter (size=3×3, σ=1)	 NC=0.9290 BER=0.0693	 Gaussian Lowpass Filter (size=5×5, σ=1)	 NC=0.9148 BER=0.0840	 Gaussian Lowpass Filter (size=7×7, σ=1.4)	 NC=0.8836 BER=0.1191
	 Salt & Pepper (density= 0.01)	 NC=0.8667 BER=0.1289	 Salt & Pepper (density= 0.001)	 NC=0.9366 BER=0.0615		
Centre 50%	 Gaussian Lowpass Filter (size=3×3, σ=1)	 NC=0.7764 BER=0.1992	 Gaussian Lowpass Filter (size=5×5, σ=1)	 NC=0.7629 BER=0.2109	 Gaussian Lowpass Filter (size=7×7, σ=1.4)	 NC=0.7366 BER=0.2363
	 Salt & Pepper (density= 0.01)	 NC=0.7221 BER=0.2471	 Salt & Pepper (density= 0.001)	 NC=0.7823 BER=0.1943		
Row 25%		 NC=0.7734 BER=0.2012		 NC=0.7587 BER=0.2139		 NC=0.7152 BER=0.2549

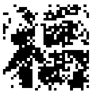
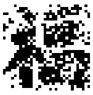
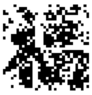
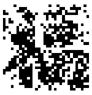
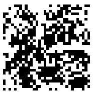
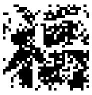
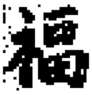
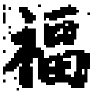
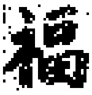
	Gaussian Lowpass Filter (size=3×3, σ=1)		Gaussian Lowpass Filter (size=5×5, σ=1)		Gaussian Lowpass Filter (size=7×7, σ=1.4)	
	 Salt & Pepper (density= 0.01)	 NC=0.7456 BER=0.2256	 Salt & Pepper (density= 0.001)	 NC=0.7767 BER=0.1982		
Row 12.5%	 Gaussian Lowpass Filter (size=3×3, σ=1)	 NC=0.8854 BER=0.1084	 Gaussian Lowpass Filter (size=5×5, σ=1)	 NC=0.8692 BER=0.1240	 Gaussian Lowpass Filter (size=7×7, σ=1.4)	 NC=0.8224 BER=0.1729
	 Salt & Pepper (density= 0.01)	 NC=0.8497 BER=0.1406	 Salt & Pepper (density= 0.001)	 NC=0.8991 BER=0.0957		
Column 50%	 Gaussian Lowpass Filter (size=3×3, σ=1)	 NC=0.7498 BER=0.2188	 Gaussian Lowpass Filter (size=5×5, σ=1)	 NC=0.7328 BER=0.2324	 Gaussian Lowpass Filter (size=7×7, σ=1.4)	 NC=0.6988 BER=0.2627
	 Salt & Pepper (density= 0.01)	 NC=0.7192 BER=0.2451	 Salt & Pepper (density= 0.001)	 NC=0.7663 BER=0.2061		
Column 25%	 Gaussian Lowpass Filter (size=3×3, σ=1)	 NC=0.9563 BER=0.0430	 Gaussian Lowpass Filter (size=5×5, σ=1)	 NC=0.9392 BER=0.0605	 Gaussian Lowpass Filter (size=7×7, σ=1.4)	 NC=0.8971 BER=0.1074

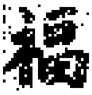
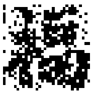
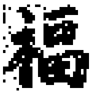
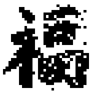
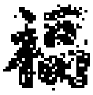
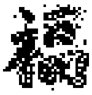
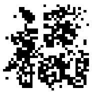
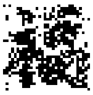
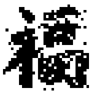
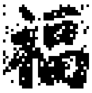
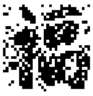
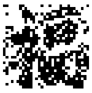
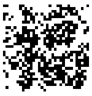
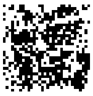
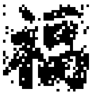
	 Salt & Pepper (density= 0.01)	 NC=0.9026 BER=0.0947	 Salt & Pepper (density= 0.001)	 NC=0.9642 BER=0.0352		
Column **12.5%**	 Gaussian Lowpass Filter (size=3×3, σ=1)	 NC=0.9585 BER=0.0410	ss Gaussian Lowpass Filter (size=5×5, σ=1)	 NC=0.9405 BER=0.0596	 Gaussian Lowpass Filter (size=7×7, σ=1.4)	 NC=0.8978 BER=0.1074
	 Salt & Pepper (density= 0.01)	 NC=0.9065 BER=0.0918	 Salt & Pepper (density= 0.001)	 NC=0.9702 BER=0.0293		

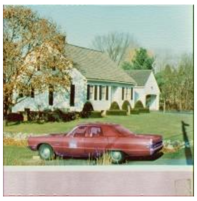
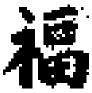
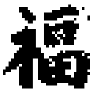
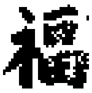
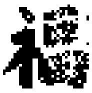
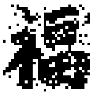
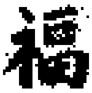
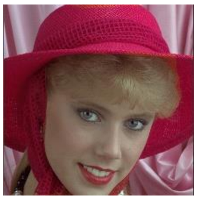
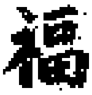
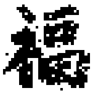
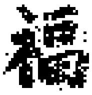
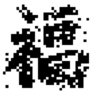
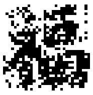
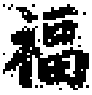
4.3.3 Irregular Tamper + Image Processing Attack

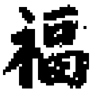
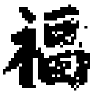
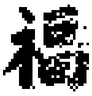
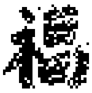
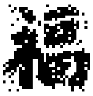
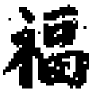
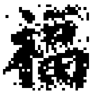
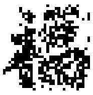
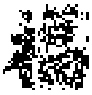
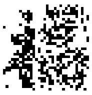
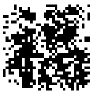
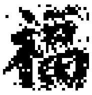
Table 6 shows NC and BER values of the extracted watermark after a series of combination attacks, which included irregular tamper and the application of filters such as Gaussian lowpass filters and salt and pepper noise.

Table 8: Visualization of Irregular Tampered Images, Extracted Watermark and NC, BER value of Extracted Watermark

Image Processing Attacks	**Recovered Watermark**	**Image Processing Attacks**	**Recovered Watermark**	**Image Processing Attacks**	**Recovered Watermark**
Parrot **Average NC=0.8179, Average BER=0.1841**					
 Tamper Attack only	 NC=0.8449 BER=0.1553	 Gaussian Lowpass Filter (size=3×3, σ=1)	 NC=0.8476 BER=0.1543	 Gaussian Lowpass Filter (size=5×5, σ=1)	 NC=0.8235 BER=0.1816
 Gaussian Lowpass Filter (size=7×7, σ=1.4)	 NC=0.8137 BER=0.1924	 Salt & Pepper (density= 0.01)	 NC=0.7468 BER=0.2510	 Salt & Pepper (density= 0.001)	 NC=0.8311 BER=0.1699
Light House **Average NC=0.9413, Average BER=0.0584**					
 Tamper Attack only	 NC=0.9723 BER=0.0273	 Gaussian Lowpass Filter (size=3×3, σ=1)	 NC=0.9704 BER=0.0293	 Gaussian Lowpass Filter (size=5×5, σ=1)	 NC=0.9561 BER=0.0439

 Gaussian Lowpass Filter (size=7×7, σ=1.4)	 NC=0.9413 BER=0.0596	 Salt & Pepper (density= 0.01)	 NC=0.8490 BER=0.1494	 Salt & Pepper (density= 0.001)	 NC=0.9585 BER=0.0410
Ball **Average NC=0.9011, Average BER=0.1045**					
 Tamper Attack only	 NC=0.9521 BER=0.0488	 Gaussian Lowpass Filter (size=3×3, σ=1)	 NC=0.9157 BER=0.0898	 Gaussian Lowpass Filter (size=5×5, σ=1)	 NC=0.8979 BER=0.1094
 Gaussian Lowpass Filter (size=7×7, σ=1.4)	 NC=0.8517 BER=0.1641	 Salt & Pepper (density= 0.01)	 NC=0.8492 BER=0.1543	 Salt & Pepper (density= 0.001)	 NC=0.9402 BER=0.0605
Kid **Average NC=0.8472, Average BER=0.1561**					
 Tamper Attack only	 NC=0.9307 BER=0.0693	 Gaussian Lowpass Filter (size=3×3, σ=1)	 NC=0.8603 BER=0.1426	 Gaussian Lowpass Filter (size=5×5, σ=1)	 NC=0.8300 BER=0.1748
 Gaussian Lowpass Filter (size=7×7, σ=1.4)	 NC=0.7808 BER=0.2324	 Salt & Pepper (density= 0.01)	 NC=0.7721 BER=0.2266	 Salt & Pepper (density= 0.001)	 NC=0.9095 BER=0.0908

Car **Average NC=0.9614, Average BER=0.0391**					
 Tamper Attack only	 NC=0.9823 BER=0.0176	 Gaussian Lowpass Filter (size=3×3, σ=1)	 NC=0.9815 BER=0.0186	 Gaussian Lowpass Filter (size=5×5, σ=1)	 NC=0.9742 BER=0.0264
 Gaussian Lowpass Filter (size=7×7, σ=1.4)	 NC=0.9398 BER=0.0645	 Salt & Pepper (density= 0.01)	 NC=0.9150 BER=0.0830	 Salt & Pepper (density= 0.001)	 NC=0.9753 BER=0.0244
Lady **Average NC=0.9339, Average BER=0.0679**					
 Tamper Attack only	 NC=0.9834 BER=0.0166	 Gaussian Lowpass Filter (size=3×3, σ=1)	 NC=0.9548 BER=0.0469	 Gaussian Lowpass Filter (size=5×5, σ=1)	 NC=0.9366 BER=0.0664
 Gaussian Lowpass Filter (size=7×7, σ=1.4)	 NC=0.9101 BER=0.0957	 Salt & Pepper (density= 0.01)	 NC=0.8619 BER=0.1387	 Salt & Pepper (density= 0.001)	 NC=0.9566 BER=0.0430

Sailboat **Average NC=0.9548, Average BER=0.0465**					
 Tamper Attack only	 NC=0.9912 BER=0.0088	 Gaussian Lowpass Filter (size=3×3, σ=1)	 NC=0.9729 BER=0.0273	 Gaussian Lowpass Filter (size=5×5, σ=1)	 NC=0.9544 BER=0.0469
 Gaussian Lowpass Filter (size=7×7, σ=1.4)	 NC=0.9132 BER=0.0947	 Salt & Pepper (density= 0.01)	 NC=0.9149 BER=0.0840	 Salt & Pepper (density= 0.001)	 NC=0.9824 BER=0.0176
Houses **Average NC=0. 8389, Average BER=0.1706**					
 Tamper Attack only	 NC=0.8913 BER=0.1074	 Gaussian Lowpass Filter (size=3×3, σ=1)	 NC=0.8516 BER=0.1621	 Gaussian Lowpass Filter (size=5×5, σ=1)	 NC=0.8393 BER=0.1797
 Gaussian Lowpass Filter (size=7×7, σ=1.4)	 NC=0.7960 BER=0.2363	 Salt & Pepper (density= 0.01)	 NC=0.7734 BER=0.2207	 Salt & Pepper (density= 0.001)	 NC=0.8819 BER=0.1172

4.3.4 **Robustness comparison of NC values with** (X. L. Liu et al., 2018) **and** (Duan et al., 2020)

The comparison experiment is carried using a Lena as host image with size 512×512 pixels and with size 32×32 pixels as watermark.

Figure 17: Lena

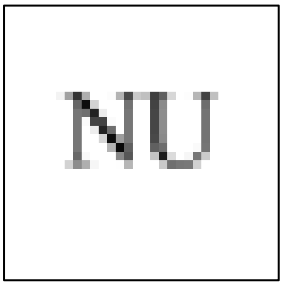


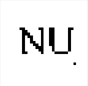
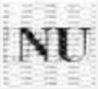
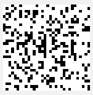
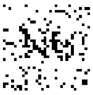
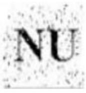
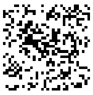
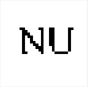
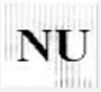
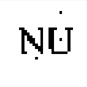
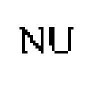
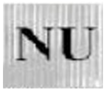
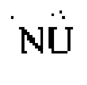
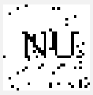
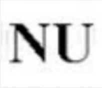
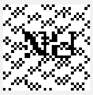
Figure 18: Watermark

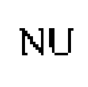
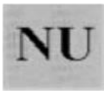
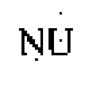
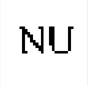
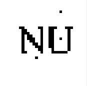
The proposed watermarking scheme has been compared with those proposed by Xiao-Long Liu and Shaohua Duan, based on the Normalized Correlation (NC) values obtained for various image processing operations such as brightening, darkening, blurring, contrast adjustment, JPEG compression and salt and pepper noise.

The results show that the proposed scheme outperforms both Liu's and Duan's schemes, with an average NC value of 0.9858, compared to 0.9825 and 0.8984, respectively. In particular, the proposed scheme achieves a high NC value of 0.9995 for JPEG compression (Q80), indicating its advantage in preserving the embedded watermark under this type of compression.

Although the proposed scheme obtains the highest NC values of 1.000 for brightening, darkening, blurring and contrast adjustment, it performs slightly lower with a value of 0.9274 for salt and pepper noise (0.02), compared to Liu's scheme which achieves a value of 0.9981. Nonetheless, the overall performance of the proposed scheme demonstrates its effectiveness and potential for use in practical applications that require robust watermarking techniques. (WITH JUSTIFICATION)

Table 9: Comparison of NC values among schemes

	Proposed	(X. L. Liu et al., 2018)	(Duan et al., 2020)
JPEG(Q80) 	 **0.9995**	 0.9842	 0.7333
Salt & Pepper (0.02) 	 0.9274	 **0.9981**	 0.6980
Brighten (50) 	 **1.0000**	 0.9904	 1.0000
Darken (50) 	 **1.0000**	 0.9655	 0.9971
Cropping (50%) 	 0.9735	 **0.9998**	 0.8605

Blurring (0.2) 	 **1.0000**	 0.9514	 1.0000
Contrast (+50) 	 **1.0000**	 0.9883	 1.0000
Average	0.9858	0.9825	0.8984

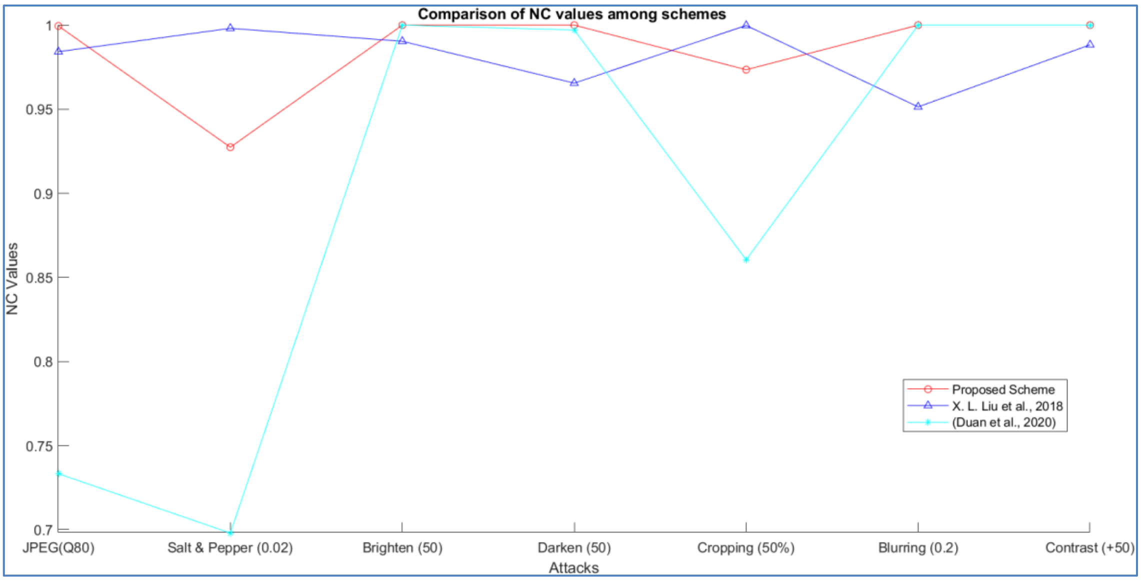
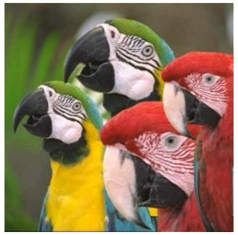
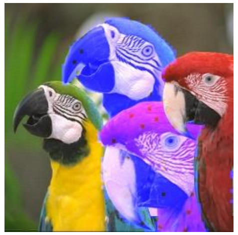


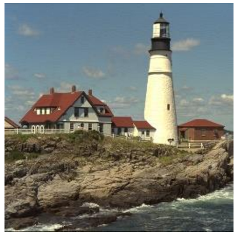
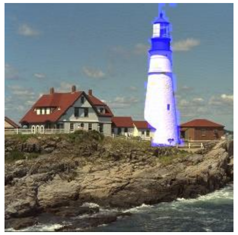
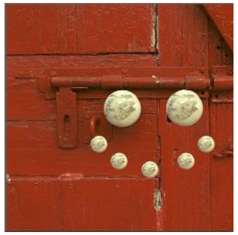
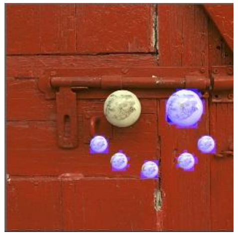
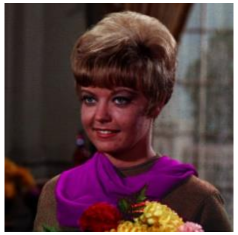
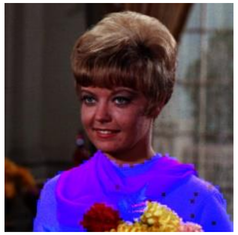
Figure 19: Graph of Comparison between 3 schemes

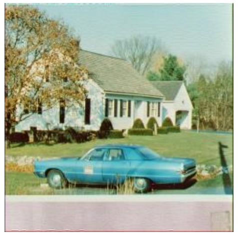
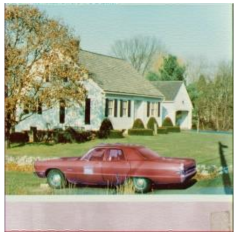
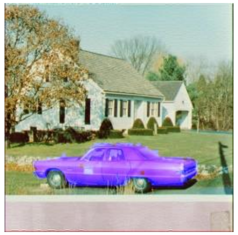
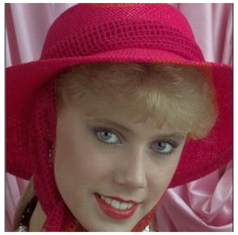
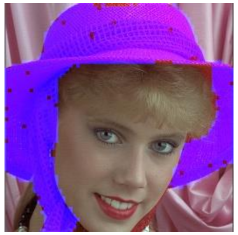
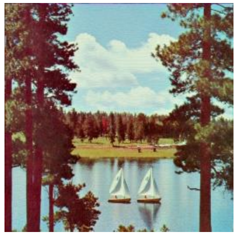
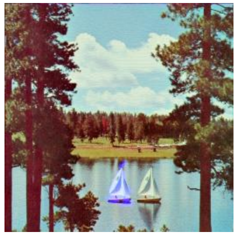
4.4 Tamper Localization

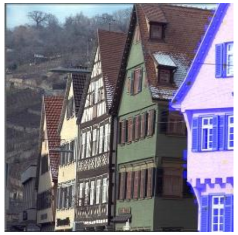
The performance of irregular tamper localization on a set of 8 images yielded an average true positive rate of 0.9658, a false negative rate of 0.0343, a false positive rate of 0.0163, and a true negative rate of 0.9837. The average precision and accuracy were found to be 0.9837 and 0.9836, respectively. Additionally, the f1-score was calculated to be 0.9745, indicating a high level of effectiveness in detecting tampering in the images.

Table 10: Irregular Tamper Localization Result

Original Image	Tampered Image / Tampering Rate (%)	Detected Tamper	TPR	FNR	FPR	TNR	Precision	Accuracy	F1-Score
	 35.0307%		0.9738	0.0262	0.0308	0.9692	0.9693	0.9707	0.9715

	 6.9118%		0.9567	0.0433	0.0092	0.9908	0.9904	0.9887	0.9733
	 5.3463%		0.9662	0.0338	0.0107	0.9893	0.9890	0.9883	0.9775
	 19.5568%		0.9798	0.0202	0.0162	0.9838	0.9837	0.9831	0.9818

	 9.3712%		0.9803	0.0197	0.0099	0.9901	0.9900	0.9893	0.9851
	 38.4888%		0.9791	0.0209	0.0438	0.9562	0.9572	0.9644	0.9680
	 1.3744%		0.9233	0.0767	0.0033	0.9967	0.9965	0.9959	0.9585

	 18.6367%		0.9668	0.0332	0.0065	0.9935	0.9933	0.9887	0.9799
Average			0.9658	0.0343	0.0163	0.9837	0.9837	0.9836	0.9745

CHAPTER 5

CONCLUSION

5.0 Introduction

A Dual Image Watermarking Based On Human Visual Characteristics For Authentication And Copyright Protection scheme is proposed in this research. The main objective of the proposed scheme is to dicover an enhanced dual image watermarking scheme that could achieve copyright protection and authentication purpose with the implementation of the principle of human visual system characteristics. From the discussion in previous section, it is proven that the proposed scheme could embed the watermarks without much distortion in the image and hence the watermark has high imperceptibility and hardly to be dicovered by human eyes. Besides that, the watermark can be extracted back after image processing attacks such as Guassian noise, salt and pepper noise etc. Moreover, the scheme could perform tamper localization to detect the modification made to the original image with high accuracy, precision and F1-score.

5.1 Research Constraints

During the writing of this thesis, a few constraints are identified. First, is the lacking of knowledge in digital watermarking. A lot of research and study need to be done in order to understand the image watermarking concepts including the inderlying principles, existing techniques and algorithms used for image watermarking for various purposes like copyright protection and authentication. Additionally, I am first exposed to MATLAB, a popular programming language and software environment that is widely used in image processing and digital signal processing applications, including image watermarking. Lack of experience with MATLAB has limited my ability to implement, test and evaluate my algorithm efficiently. Inevitably, during algorithm development, I have encountered errors, inconsistencies, or unexpected outcomes. Without prior experience in MATLAB, it is more challneging and time-consuming when I was troubleshooting and debugging issues within your code.

5.2 Research Conclusions

An enhanced dual image watermarking scheme based on human visual system characteristics for copyright protection and authentication is proposed. The purpose of this proposed scheme is to develop an algorithm that could embed two watermarks in an image where the watermarks could not be easily detected by human eyes (high imperceptibility) and could be extracted back as perfect as possible after any kind of image processing attack (high robustness), additionally, could detect any modification that has been made on the image (tamper localization). The extraction of the watermark from the image could be used for copyright protection to prove the owner of the image and tamper localization could ensure the authenticity of the image.

The experiment results show that the scheme has achieve the objective of the proposed scheme, where it commonly shows better results in imperceptibility, robustness and tamper localization rate compared to other existing scheme after the same attacks.

5.3 Future Work

1. Arnold Scrambling: Arnold scrambling is an image encryption scheme. It can be implemented into the scheme by scrambling the watermark before embedding it into an image. This could enhance the security of the watermark. Unauthorised users will find it more challenging to find, eliminate, or alter the watermark as there is an added layer of complexity on the watermark image.

2. Blind watermarking: Blind watermarking is a technique in which the original, unwatermarked image is not required for watermark extraction. In other words, the watermark can be extracted directly from the watermarked image without needing any knowledge of the original image or the watermarking process. This could be researched and implement in the proposed scheme to eliminate the need for maintaining a separate copy of the original image, which can be challenging or impractical in certain scenarios.

3. Mobile and real-time watermarking: Adapt the watermarking scheme for mobile devices or other real-time applications. Developing a lightweight watermarking techniques that can be efficiently implemented on mobile devices and support real-time watermark embedding and extraction could be an extended milestone for this scheme. This could improve the usability and accessibility of the algorithm.

REFERENCES

Al-Gindy, A., Tawfik, A., Al-Ahmad, H., & Qahwaji, R. (n.d.). *A New Blind Image Watermarking Technique for Dual Watermarks Using Low-Frequency Band DCT Coefficients*.

Al-Haj, A. (2007). Combined DWT-DCT Digital Image Watermarking. *Journal of Computer Science, 3*(9), 740–746. https://doi.org/10.3844/jcssp.2007.740.746

Al-Otum, H. M., & Ellubani, A. A. A. (2022). Secure and effective color image tampering detection and self restoration using a dual watermarking approach☆. *Optik*, *262*. https://doi.org/10.1016/j.ijleo.2022.169280

Bhinder, P., Jindal, N., & Singh, K. (2020). An improved robust image-adaptive watermarking with two watermarks using statistical decoder. *Multimedia Tools and Applications*, *79*(1–2), 183–217. https://doi.org/10.1007/s11042-019-07941-2

Deepa B. Maheshwari. (2018). *An Analysis of Wavelet Based Dual Digital Image Watermarking Using SVD*. IEEE.

Duan, S., Wang, H., Liu, Y., Huang, L., & Zhou, X. (2020). A Novel Comprehensive Watermarking Scheme for Color Images. *Security and Communication Networks, 2020*. https://doi.org/10.1155/2020/8840779

Han, Q., Han, L., Wang, E., & Yang, J. (2013). Dual watermarking for image tamper detection and self-recovery. *Proceedings - 2013 9th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIH-MSP 2013*, 33–36. https://doi.org/10.1109/IIH-MSP.2013.17

Han, Y., Shang, Y., & He, W. (2013). DWT-domain dual watermarking algorithm of color image based on visual cryptography. *Proceedings - 2013 9th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIH-MSP 2013*, 373–378. https://doi.org/10.1109/IIH-MSP.2013.100

Kiatpapan, S., & Kondo, T. (2015, August 17). An image tamper detection and recovery method based on self-embedding dual watermarking. *ECTI-CON 2015 - 2015 12th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology*. https://doi.org/10.1109/ECTICon.2015.7206973

Li, Z., Zhang, H., Liu, X., Wang, C., & Wang, X. (2021). Blind and safety-enhanced dual watermarking algorithm with chaotic system encryption based on RHFM and DWT-DCT. *Digital Signal Processing: A Review Journal*, *115*. https://doi.org/10.1016/j.dsp.2021.103062

Liao, Y., & Liu, Q. (2010). Applying dual digital watermarking technology in digital rights management. *Proceedings - 3rd International Conference on Information Sciences and Interaction Sciences, ICIS 2010*, 616–619. https://doi.org/10.1109/ICICIS.2010.5534674

Lim, S. J., Moon, H. M., Chae, S. H., Pan, S. B., Chung, Y., & Chang, M. H. (2008). Dual Watermarking Method for integrity of medical images. *Proceedings of the 2008 2nd International Conference on Future Generation Communication and Networking, FGCN 2008*, *2*, 70–73. https://doi.org/10.1109/FGCN.2008.213

Liu, F., & Liu, Y. (2008). A watermarking algorithm for digital image based on DCT and SVD. *Proceedings - 1st International Congress on Image and Signal Processing, CISP 2008*, *1*, 380–383. https://doi.org/10.1109/CISP.2008.412

Liu, X. L., Lin, C. C., & Yuan, S. M. (2018). Blind Dual Watermarking for Color Images' Authentication and Copyright Protection. *IEEE Transactions on Circuits and Systems for Video Technology*, *28*(5), 1047–1055. https://doi.org/10.1109/TCSVT.2016.2633878

LUSIA RAKHMAWATI, WIRAWAN, SUWADI, CLAUDE DELPHA, & PIERRE DUHAMEL. (2017). *Dual Watermarking Schemes for Image Authentication and Copyright Protection with Recovery Capability*. https://doi.org/10.1109/ACCESS.2017.Doi

Mishra, A., Agarwal, C., Sharma, A., & Bedi, P. (2014). Optimized gray-scale image watermarking using DWT-SVD and Firefly Algorithm. *Expert Systems with Applications*, *41*(17), 7858–7867. https://doi.org/10.1016/j.eswa.2014.06.011

SINGH, H., KAUR, L., & SINGH, K. (2014). Fractional M-band dual tree complex wavelet transform for digital watermarking. *Sadhana*, *39*(2), 345–361. https://doi.org/10.1007/s12046-013-0217-2

Singh, S. K., & Kumar, S. (2011). Novel adaptive color space transform and application to image compression. *Signal Processing: Image Communication*, *26*(10), 662–672. https://doi.org/https://doi.org/10.1016/j.image.2011.08.001

SIPI Image Database - Misc. (n.d.). Retrieved July 2, 2023, from https://sipi.usc.edu/database/database.php?volume=misc

APPENDIX A
NC AND BER UNDER VARIOUS IMAGE PROCESSING ATTACKS

			Parrot		**Light House**		**Ball**		**Houses**		**Lady**		**Kid**		**Sailboat**		**Car**	
			NC	**BER**	**NC**	**BER**	**NC**	**BER**	**NC**	**BER**	**NC**	**BER**	**NC**	**BER**	**NC**	**BER**	**NC**	**BER**
Centre 12.5%	Gaussian Lowpass Filter	size=3×3, σ=1	0.9783	0.0215	0.9912	0.0088	0.9212	0.0830	0.8908	0.1172	0.9240	0.0742	0.8401	0.1631	0.9290	0.0693	0.9755	0.0244
	Gaussian Lowpass Filter	size=5×5, σ=1	0.9491	0.0518	0.9788	0.0215	0.9024	0.1035	0.8719	0.1416	0.8987	0.1006	0.8220	0.1836	0.9148	0.0840	0.9692	0.0313
	Gaussian Lowpass Filter	size=7×7, σ=1.4	0.9438	0.0576	0.9619	0.0391	0.8578	0.1572	0.8301	0.1943	0.8699	0.1309	0.7713	0.2432	0.8836	0.1191	0.9364	0.0674
	Salt & Pepper	density= 0.01	0.8648	0.1338	0.8566	0.1416	0.8171	0.1855	0.8480	0.1465	0.8138	0.1777	0.7676	0.2236	0.8667	0.1289	0.9261	0.0732
	Salt & Pepper	density= 0.001	0.9643	0.0352	0.9823	0.0176	0.9431	0.0576	0.9346	0.0635	0.9275	0.0703	0.8958	0.1025	0.9366	0.0615	0.9683	0.0313
Centre 50%	Gaussian Lowpass Filter	size=3×3, σ=1	0.9102	0.0859	0.9250	0.0723	0.8674	0.1270	0.8145	0.1787	0.7795	0.1973	0.7767	0.2139	0.7764	0.1992	0.9684	0.0313
	Gaussian Lowpass Filter	size=5×5, σ=1	0.8817	0.1143	0.9121	0.0850	0.8480	0.1465	0.7941	0.2021	0.7437	0.2305	0.7710	0.2236	0.7629	0.2109	0.9620	0.0381
	Gaussian Lowpass Filter	size=7×7, σ=1.4	0.8752	0.1211	0.8946	0.1025	0.8102	0.1885	0.7539	0.2480	0.7162	0.2568	0.7161	0.2842	0.7366	0.2363	0.9327	0.0703
	Salt & Pepper	density= 0.01	0.7875	0.1982	0.8191	0.1729	0.7888	0.2031	0.7647	0.2139	0.7054	0.2627	0.7103	0.2734	0.7221	0.2471	0.9073	0.0898
	Salt & Pepper	density= 0.001	0.8995	0.0957	0.9114	0.0850	0.8740	0.1191	0.8522	0.1367	0.7896	0.1885	0.8265	0.1631	0.7823	0.1943	0.9602	0.0391
Row 50%	Gaussian Lowpass Filter	size=3×3, σ=1	0.6637	0.2793	0.1655	0.4854	0.8670	0.1318	0.7224	0.2451	0.7823	0.1943	0.6006	0.3311	0.5173	0.3662	0.6370	0.2969
	Gaussian Lowpass Filter	size=5×5, σ=1	0.6623	0.2803	0.1655	0.4854	0.8513	0.1484	0.7168	0.2510	0.7707	0.2041	0.5925	0.3389	0.5122	0.3691	0.6289	0.3027

	Gaussian Lowpass Filter	size=7×7, σ=1.4	0.6624	0.2803	0.1599	0.4863	0.8121	0.1934	0.6921	0.2744	0.7497	0.2227	0.5573	0.3711	0.4954	0.3799	0.6136	0.3135
	Salt & Pepper	density= 0.01	0.5901	0.3359	0.2486	0.4932	0.7902	0.2041	0.6848	0.2734	0.7055	0.2598	0.6139	0.3301	0.5068	0.3838	0.6141	0.3203
	Salt & Pepper	density= 0.001	0.6594	0.2822	0.1648	0.4873	0.8928	0.1035	0.7601	0.2109	0.7906	0.1875	0.6603	0.2852	0.5366	0.3555	0.6414	0.2939
Row 25%	Gaussian Lowpass Filter	size=3×3, σ=1	0.7650	0.2070	0.4987	0.3750	0.9004	0.1025	0.8073	0.1836	0.8915	0.1035	0.7149	0.2578	0.7734	0.2012	0.6509	0.2881
	Gaussian Lowpass Filter	size=5×5, σ=1	0.7638	0.2080	0.4968	0.3760	0.8833	0.1211	0.7995	0.1924	0.8709	0.1240	0.6985	0.2734	0.7587	0.2139	0.6418	0.2949
	Gaussian Lowpass Filter	size=7×7, σ=1.4	0.7576	0.2129	0.4893	0.3799	0.8406	0.1719	0.7701	0.2236	0.8451	0.1504	0.6584	0.3164	0.7152	0.2549	0.6270	0.3057
	Salt & Pepper	density= 0.01	0.6857	0.2705	0.4481	0.4121	0.8059	0.1934	0.7752	0.2070	0.8035	0.1855	0.6862	0.2793	0.7456	0.2256	0.6186	0.3154
	Salt & Pepper	density= 0.001	0.7549	0.2148	0.4994	0.3750	0.9330	0.0664	0.8636	0.1270	0.8975	0.0977	0.7638	0.2129	0.7767	0.1982	0.6499	0.2891
Row 12.5%	Gaussian Lowpass Filter	size=3×3, σ=1	0.8737	0.1182	0.7283	0.2344	0.9124	0.0918	0.8685	0.1328	0.9132	0.0840	0.7520	0.2334	0.8854	0.1084	0.7893	0.1885
	Gaussian Lowpass Filter	size=5×5, σ=1	0.8704	0.1211	0.7270	0.2354	0.8944	0.1113	0.8595	0.1436	0.8930	0.1045	0.7374	0.2480	0.8692	0.1240	0.7814	0.1953
	Gaussian Lowpass Filter	size=7×7, σ=1.4	0.8585	0.1318	0.7139	0.2451	0.8456	0.1709	0.8170	0.1934	0.8657	0.1328	0.6972	0.2939	0.8224	0.1729	0.7510	0.2227
	Salt & Pepper	density= 0.01	0.7621	0.2178	0.6502	0.3008	0.8259	0.1777	0.8150	0.1758	0.8264	0.1680	0.6994	0.2793	0.8497	0.1406	0.7383	0.2314
	Salt & Pepper	density= 0.001	0.8557	0.1338	0.7310	0.2324	0.9385	0.0615	0.9219	0.0752	0.9192	0.0781	0.8126	0.1748	0.8991	0.0957	0.7856	0.1914
Column 50%	Gaussian Lowpass Filter	size=3×3, σ=1	0.6882	0.2627	0.7481	0.2197	0.5398	0.3574	0.6906	0.2686	0.5409	0.3535	0.3477	0.4434	0.7498	0.2188	0.7829	0.1934
	Gaussian Lowpass Filter	size=5×5, σ=1	0.6665	0.2783	0.7329	0.2314	0.5276	0.3662	0.6843	0.2754	0.5358	0.3564	0.3394	0.4482	0.7328	0.2324	0.7793	0.1963

	Gaussian Lowpass Filter	size=7×7, σ=1.4	0.6584	0.2842	0.7216	0.2402	0.5014	0.3867	0.6668	0.2910	0.5269	0.3613	0.3233	0.4570	0.6988	0.2627	0.7440	0.2266
	Salt & Pepper	density= 0.01	0.6079	0.3281	0.6513	0.2979	0.5183	0.3818	0.6550	0.2920	0.5110	0.3867	0.3924	0.4424	0.7192	0.2451	0.7257	0.2432
	Salt & Pepper	density= 0.001	0.6755	0.2715	0.7353	0.2295	0.5551	0.3477	0.7299	0.2334	0.5533	0.3467	0.3849	0.4268	0.7663	0.2061	0.7830	0.1934
Column 25%	Gaussian Lowpass Filter	size=3×3, σ=1	0.7403	0.2256	0.8936	0.1006	0.6899	0.2695	0.7773	0.2090	0.8221	0.1621	0.5575	0.3564	0.9563	0.0430	0.9302	0.0674
	Gaussian Lowpass Filter	size=5×5, σ=1	0.7090	0.2500	0.8799	0.1133	0.6778	0.2803	0.7652	0.2236	0.8155	0.1680	0.5459	0.3662	0.9392	0.0605	0.9263	0.0713
	Gaussian Lowpass Filter	size=7×7, σ=1.4	0.7030	0.2549	0.8665	0.1260	0.6402	0.3184	0.7399	0.2500	0.8020	0.1797	0.5225	0.3867	0.8971	0.1074	0.8869	0.1123
	Salt & Pepper	density= 0.01	0.6646	0.2871	0.7924	0.1943	0.6237	0.3271	0.7508	0.2246	0.7606	0.2178	0.5582	0.3662	0.9026	0.0947	0.8801	0.1152
	Salt & Pepper	density= 0.001	0.7379	0.2275	0.8860	0.1074	0.7117	0.2490	0.8233	0.1611	0.8186	0.1650	0.6067	0.3213	0.9642	0.0352	0.9208	0.0762
Column 12.5%	Gaussian Lowpass Filter	size=3×3, σ=1	0.8452	0.1426	0.9560	0.0430	0.8118	0.1777	0.8283	0.1689	0.8815	0.1123	0.7429	0.2383	0.9585	0.0410	0.9674	0.0322
	Gaussian Lowpass Filter	size=5×5, σ=1	0.8191	0.1660	0.9411	0.0576	0.7922	0.1973	0.8156	0.1846	0.8699	0.1240	0.7242	0.2578	0.9405	0.0596	0.9618	0.0381
	Gaussian Lowpass Filter	size=7×7, σ=1.4	0.8094	0.1748	0.9267	0.0723	0.7469	0.2490	0.7849	0.2197	0.8548	0.1387	0.6833	0.3018	0.8978	0.1074	0.9249	0.0781
	Salt & Pepper	density= 0.01	0.7364	0.2383	0.8573	0.1367	0.7370	0.2490	0.7783	0.2051	0.8050	0.1836	0.6787	0.2910	0.9065	0.0918	0.9136	0.0850
	Salt & Pepper	density= 0.001	0.8362	0.1504	0.9488	0.0498	0.8326	0.1563	0.8761	0.1162	0.8774	0.1162	0.8095	0.1758	0.9702	0.0293	0.9652	0.0342
Average			0.7784	0.1938	0.7164	0.2142	0.7882	0.1934	0.7899	0.1969	0.7917	0.1840	0.6590	0.2895	0.7994	0.1744	0.8192	0.1577
Average NC			0.7678															
Average BER			0.2005															