DISCRETE WAVELET TRANSFORM (DWT) BASED DUAL WATERMARKING FOR AUTHENTICATION AND COPYRIGHT PROTECTION

LIM CHEN GEN

FACULTY OF COMPUTING
UNIVERSITI MALAYSIA PAHANG

UNIVERSITI MALAYSIA PAHANG

DECLARATION OF THESIS AND COPYRIGHT

Author's Full Name : Lim Chen Gen :

Date of Birth

Title : Discrete Wavelet Transform (DWT)
Based Dual Watermarking for
Authentication and Copyright Protection

Academic Session : SEMESTER II ACADEMIC SESSION 2022/2023

I declare that this thesis is classified as:

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

I acknowledge that Universiti Malaysia Pahang reserves the following rights:

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

Certified by:

____
(Supervisor's Signature)

____
(Student's Signature)

Profesor Madya
Ts. Dr. Ferda Ernawan
Date:

Universiti
Malaysia
PAHANG
Engineering • Technology • Creativity

SUPERVISOR'S DECLARATION

I hereby declare that I have checked this thesis and in my opinion, this thesis is adequate in terms of scope and quality for the award of the degree of Computer Science (Graphics & Multimedia Technology)

(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 :

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 : LIM CHEN GEN

ID Number : CD20136

Date : 7/6/2023

DISCRETE WAVELET TRANSFORM (DWT) BASED DUAL WATERMARKING FOR AUTHENTICATION AND COPYRIGHT PROTECTION

LIM CHEN GEN

Thesis submitted in fulfillment of the requirements
for the award of the degree of
Computer Science (Graphics & Multimedia Technology)

Faculty of Computing

UNIVERSITI MALAYSIA PAHANG

JUNE 2023

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to Dr. Ferda Ernawan, my research supervisor, for his invaluable guidance, support, and expertise throughout my thesis journey. His unwavering commitment to academic excellence and his passion for research have been a constant source of inspiration for me.

I am grateful to Dr. Ernawan for his patience, encouragement, and insightful feedback that significantly contributed to the development and refinement of my research work. His expertise in the field has been instrumental in shaping my research methodology and enhancing the quality of my findings.

I would also like to extend my appreciation to the faculty members and staff who have provided assistance, resources, and a conducive research environment during my academic pursuit. Their support and dedication have been instrumental in my growth as a researcher.

I am indebted to my family and friends for their unwavering support, understanding, and encouragement throughout this thesis journey. Their belief in my abilities and constant motivation have been the driving force behind my accomplishments.

Lastly, I would like to acknowledge all the researchers, scholars, and authors whose works and contributions have provided the foundation and inspiration for my research. Their insights and discoveries have paved the way for advancements in the field and have been instrumental in shaping my understanding.

ABSTRACT

Digital media faces significant challenges related to unauthorized access, manipulation, and copyright infringement, necessitating effective authentication and copyright protection mechanisms. This thesis proposes a novel dual watermarking scheme based on the Discrete Wavelet Transform (DWT) to address these concerns.

The primary objective of the proposed scheme is to provide robust copyright protection. A watermark, carrying ownership and copyright information, is embedded in the spatial domain using the DWT. This watermark acts as a digital signature, enabling the identification and tracing of the rightful owner of the content. The frequency domain embedding enhances the watermark's robustness against common attacks.

In addition to copyright protection, the scheme incorporates a fragile watermark for authentication purposes. The fragile watermark is embedded in the least significant bit which is highly sensitive to any modifications or tampering. By extracting and comparing the fragile watermark, the integrity and authenticity of the content can be verified.

Comprehensive experimental evaluations have been conducted to assess the performance of the proposed dual watermarking scheme. The results demonstrate its effectiveness in providing robust copyright protection and authentication capabilities. The scheme exhibits high imperceptibility, preserving the visual quality of the watermarked content, while ensuring a high level of sensitivity to unauthorized alterations.

TABLE OF CONTENT

DECLARATION

TITLE PAGE

ACKNOWLEDGEMEMTS **i**

ABSTRACT **ii**

TABLE OF CONTENT **iii**

LIST OF TABLES **vi**

LIST OF FIGURES **vii**

LIST OF ABBREVIATIONS **ix**

LIST OF APPENDICES **x**

CHAPTER 1 INTRODUCTION **1**

1.1 Background 1

1.2 Problem Statement 2

1.3 Research Objective 4

1.4 Research Scope 4

CHAPTER 2 LITERATURE REVIEW **5**

2.1 Introduction 5

2.2 Overview of Watermarking Technique 5

2.2.1 Dual Watermarking Scheme 6

2.2.2 Watermarking for Copyright Protection 6

2.2.3 Watermarking for Authentication 7

2.2.4 Embedding Sub-bands and Sub-block 8

2.2.5 Singular Value Decomposition (SVD) 8

2.2.6 Embedding Luminance Y Component from RGB Conversion 9

2.3 The Existing Dual Image Watermarking Scheme 10
2.4 Summary of The Existing Dual Image Watermarking Scheme 11
2.5 Relevance of Comparison 12
CHAPTER 3 METHODLOGY 13
3.1 Introduction 13
3.2 Research Framework 13
3.3 Research Requirement 15
3.4 Propose Design 16
3.4.1 Copyright Protection Watermarking Algorithm 19
3.4.2 Authentication Watermarking Algorithm 20
3.4.3 Tamper Localization Algorithm 21
3.4.4 Watermark Extraction Algorithm 22
3.5 Evaluation Plan 23
3.5.1 Imperceptibility Measurement 23
3.5.2 Robustness Measurement 24
3.5.3 Tamper Localization Measurement 25
3.6 Potential Use of Proposed Solution 26
3.7 Gantt Chart 26
CHAPTER 4 RESULT AND DISCUSSION 27
4.1 Introduction 27
4.2 Imperceptibility Experiment 28
4.3 Tamper Detection and Watermark Extraction under Regular Attack 32
4.4 Tamper Detection under Irregular Attack Experiment 39
4.5 Watermark extraction under Image Processing Attack 42
CHAPTER 5 CONCLUSION 48
5.1 Research Conclusion 48

5.2 Future Work 49

Reference 50

APPENDIX 53

LIST OF TABLES

Table 2.1	Summary of existing watermarking	10
Table 4.1	Comparison data PSNR and SSIM	29
Table 4.2	Comparison data of tamper detection performance under regular attacks	34
Table 4.3	Comparison data of extraction under regular attacks	37
Table 4.4	Data of tamper detection performance under irregular attacks	41
Table 4.5	Various image processing detail and its abbreviation	42
Table 4.6	NC BER result data and comparison	44

LIST OF FIGURES

Figure 2.1 Example Decomposition of DWT 7

Figure 3.1 Research Framework 14

Figure 3.2 Images and logo used for the experiment 15

Figure 3.3 The block diagram showing process of the proposed watermarking scheme 16

Figure 3.4 The block diagram showing process of the watermark extraction 17

Figure 3.5 The block diagram showing process of the tamper detection 18

Figure 4.1 Dual Watermarked Images Showing High Imperceptibility Embedding 28

Figure 4.2 Comparison PSNR values of the dual watermarked image between the schemes 29

Figure 4.3 Comparison SSIM values of the dual watermarked image between the schemes 30

Figure 4.4 Image with regular attack from 10% to 50% (a-e 1), detected tamper (a-e 2), correct detected tamper (a-e 3), and watermark extraction from the regular attact (a-e 4) 33

Figure 4.5 Precision Comparison of Tamper Detection from Different Tampering Rate 34

Figure 4.6 F1-Score Comparison of Tamper Detection from Different Tampering Rate 35

Figure 4.7 Accuracy Comparison of Tamper Detection from Different Tampering Rate 35

Figure 4.8 NC Comparison of Watermark Extraction from Different Tampering Rate 37

Figure 4.9 BER Comparison of Watermark Extraction from Different Tampering Rate 37

Figure 4.10 Watermarked images (a-f 1), irregular attacked images (a-f 2), red marked tamper detection images (a-f 3), correct detected area (a-f 4) 40

Figure 4.11 Images with image processing attack and its watermark extraction 43

Figure 4.12 NC Comparison of image processing attack (Lena) 46

Figure 4.13 BER Comparison of image processing attack (Lena) 46

LIST OF ABBREVIATIONS

DWT	Discrete Wavelet Transform
DCT	Discrete Cosine Transform
SVD	Singular Value Decomposition
PSNR	Peak Signal to Noise Ratio
SSIM	Structural Index Similarity
NC	Normalised Cross-Correlation
BER	Bit Error Rate
TPR	True Positive Rate
TNR	True Negative Rate
FPR	False Positive Rate
FNR	False Negative Rate
LSB	Least Significant Bit

LIST OF APPENDICES

Appendix A: Gant Chart 53

CHAPTER 1

INTRODUCTION

1.1 Background

Images are an important carrier of information on the web. According to psychologists, about 70% of all human perceptual information comes from vision. The increase of shooting devices and the convenience of shooting have made images widely used in military, medical, meteorological, e-government and personal affairs. Hence, people's awareness of image copyright protection is gradually increasing. However, the increase in hacking capability and the ease of image reproduction and distribution have posed new challenges to image watermarking technology. Therefore, data protection is an important aspect of ensuring that multimedia files are protected from unauthorized access and use. Image watermarking is an important technique to protect image copyright. (Laouamer & Tayan, 2018; S. P. Singh & Bhatnagar, 2018)

Multimedia data needs to be secured to prevent piracy, illegal copying, forgery and fraud. Data hiding through watermarking is a process that involves altering the contents of an image to conceal desired information. It must not affect the original quality of the finished watermarked image. (Mun et al., 2019) Digital watermarking is a solution for digital copyright authentication and protection that may be used to secure and protect the intellectual property of images. (Hsu & Hu, 2017)

A scheme by Ernawan (2016) presented embedding watermarks based on the psychovisual threshold. For the watermark to be invisible to the human visual system and generate only imperceptible distortion, watermark embedding under the psychovisual threshold limitation was adopted in his scheme. A scheme by Das, Panigrahi, Sharma, (2014) presented watermarking in DCT domain using inter-block coefficient correlation.

Their scheme used extremely robust to JPEG image compression and other typical picture processing techniques. A scheme by Dey, Samanta, Chakraborty, Das, Chaudhuri, Suri (2014) presented DWT, DCT, and SVD combined with the firefly algorithm (FA). They used this combination scheme to optimize the embedding multiple medical data within a biomedical image. A scheme by Lai (2011) presented an improved SVD-based watermarking scheme using human visual characteristics. This scheme used the characteristics of the human visual system to enhance the watermark imperceptibility and robustness. A scheme by Jagadeesh et al., (2016) presented watermarking based on fuzzy inference system and back propagation neural networks with DCT. Their scheme able to makes the watermark invisible and resistant to various type of watermarking attacks.

This research proposed watermarking scheme is DWT based watermarking for copyright protection and authentication. The watermarking scheme is implemented by a non-overlapping block of 8×8 pixels with DWT transform using 32 x 32 watermark on 512 x 512 host image. DWT can decompose the image matrix at diverse scales. Next, authentication provided by a self-embedding watermarking that generating authentication bit for tamper localization.

1.2 Problem Statement

With the increasing use of digital media, the need for robust and secure methods to protect the copyright of digital content has become more important. Traditional single watermarking methods are not sufficient to provide both authentication and protection. Therefore, a dual watermarking scheme is required to provide both authentication and protection for digital content. Dual image watermarking related work including scheme proposed by Bolourian Haghighi et al., (2018). Their scheme is based on lifting wavelet transform and halftoning technique (TRLH). Next, Nasir N. Hurrah et al., (2018) and Lusia Rakhmawati et al., (2020) proposed dual image watermarking schemes both are based on discrete cosine transform (DCT).

The research problem addressed in this study is the need for a secure and robust method for protecting the copyright of RGB images in the digital age. With the widespread use of digital images and the ease with which they can be copied and distributed, there is a growing concern about protecting the ownership and integrity of these images. Existing watermarking techniques have been developed to address this problem, but they often suffer from limitations such as low imperceptibility low accuracy and precision in tamper detection. Lusia Rakhmawati et al., (2020) scheme show a result of imperceptibility dual watermark image below 35.687db PSNR and only greyscale image supported in their scheme.

Therefore, there is a need to develop a more effective and reliable watermarking technique that can provide better protection for digital images. The research problem can be further refined to include the need for a DWT watermarking technique that can work effectively on RGB images, which are commonly used in various applications such as digital photography, video, and graphic design. RGB images contain three color channels, which can pose additional challenges for watermarking compared to grayscale images. Addressing these research problems will lead to the development of a more secure and reliable copyright protection mechanism for RGB images, which is essential for ensuring the ownership and integrity of digital content in various applications.

In shorts, the research problem is the optimisation of a DWT-based dual watermarking scheme for RGB images is potentially capable of further development.

1.3 Research Objective

The research objective is defined based on the research problem. The objectives of this research are listed as below:

- To study the existing dual image watermarking scheme for authentication and copyright protection.
- To propose DWT in dual watermarking scheme for authentication and copyright protection.
- To evaluate the proposed dual image watermarking scheme base on DWT in terms of imperceptibility, robustness, and tamper localization

1.4 Research Scope

The scope consists of:

1. This research focuses on the 512 x 512 pixels RGB host images.

2. Watermarking images in this research are using 32x32 pixels binary image

3. PSNR and SSIM are the measuring tools to evaluate the quality imperceptibility of the watermarked image.

4. The robustness of the watermark extraction was evaluated by normalised cross-correlation (NC) and bit error rate (BER) under various image attacks.

5. True Positive Rate (TPR), False Negative Rate (FNR), and False Positive Rate (FPR) are used to evaluate tamper localization.

6. MATLAB R2021b© with Dell workstation, Intel® Core™ i7-7700 CPU @ 3.60 GHz, memory 16GB. is the main tool conduct the research experiment. The program functions and measurement are all MATLAB functions.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

In this chapter, studies and analysis of existing image watermarking scheme is conducted. This is done to comprehend various image water marking techniques to analyse their advantages & disadvantages to understand how the proposed scheme can be further improved.

2.2 Overview of Watermarking Technique

Spatial domain techniques and transform domain techniques are the two primary categories of existing digital watermarking techniques in which the watermark is integrated. (Makbol et al., 2016) In the transform domain, the data are embedded by altering the amplitude of the transformed coefficients, meanwhile in the spatial domain, the watermark is directly embedded in the pixel values. Transform domain approaches are favoured because they enable more information to be incorporated and offer higher robustness against attacks, even though spatial domain approaches are having lower complexity and simple implementation. The most often used transforms in the field of digital watermarking are the discrete cosine transform (DCT) and discrete wavelet transform (DWT).

2.2.1 Dual Watermarking Scheme

In digital watermarking, spatial and transform domain are the main option to embedding a watermark. The research is aim to provide images copyright protection and authentication feature. Hence, dual watermarking technique using combination of both transform domains is used in the research. Dual watermarking able to embed different watermarks for multipurpose including copyright protection and authentication. For example, the focus of Jobin Abraham & Dr. Varghese Paul, (2017) was a dual watermarking scheme for copyright protection. According to their solution, the visible watermark picture is added to the host image based on the DWT and DCT suitability to distinct regions in the image. For RGB based pictures, Liu et al., (2018) proposed a blind dual watermarking mechanism for both authentication and copyright protection. From the analysis of these existing schemes, it is clearly they are emphasis on one or two functions per image, whereas the main objective of this research is aligned with their objective. The research is aimed to develop the scheme can simultaneously protect copyright, authenticate the tampered image, and extract watermarks from the protected image without knowing the original host or watermarks.

2.2.2 Watermarking for Copyright Protection

The ability to copy and modify digital works readily makes copyright protection in the digital age a significant concern. However, if the digital assets are watermarked, illegal copies may be tracked and the true owner can claim the copyright. In this research, the method applied for copyright protection watermarking is based on Discrete Wavelet Transform (DWT). DWT is a method for converting spatial signals into wavelets (Thakral & Manhas, 2019). DWT is used in the proposed copyright protection watermarking because of the theory from DWT multiresolution analysis that decomposes the image into recursive and band-limited component whereby the original image can be restored. The four frequency sub-bands of DWT are LL (low-low frequency), LH (low-high frequency), HL (high-low frequency), and HH (high-high frequency) (Bhinder et al., 2019). The DWT is capable of offering flawless image reconstruction. The formula of DWT is defined as (Donald et al., 2009)

$$b(j,k) = m^{\frac{j}{2}} \int_{-\infty}^{\infty} f(t) \psi_{1,0}(m^{j} - k) dt \qquad 2.1$$

where $j, k \in \mathbb{Z},\ \ m \geq 2,\ \ m \in \mathbb{Z}^{+}$. Typically, m is set at two,1 in which case the mother wavelet is stretched or compressed by powers of two. Wavelets with m 3 are referred to as higher multiplicity wavelets. There are many types of wavelets such as 'Haar', 'Daubechies', 'Coiflet' and etc. Haar Wavelet is considered as the easiest wavelet and chosen in this research scheme. It has the ability to run the filter bank method to separate various frequency components from the other wavelets. With the aid of the Haar Wavelet, we can divide the total number of pixel values in the selected image or frame to find the components with lower frequency.

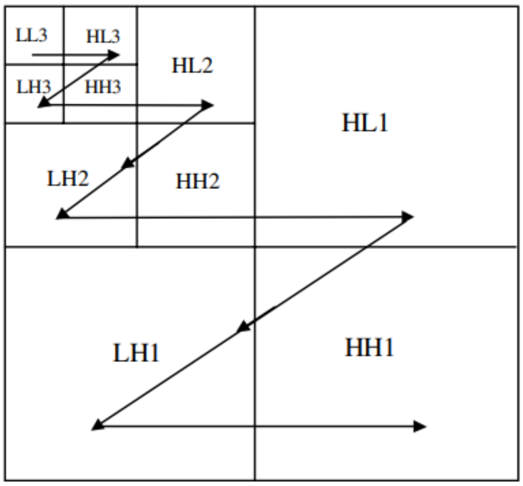


Figure 2.1 Example Decomposition of DWT

Source: (Daren et al., 2001)

2.2.3 Watermarking for Authentication

Watermark embedding, insertion technique, tamper localisation are the components of a fragile watermarking provide image an authentication feature. Self-embedding fragile watermarking techniques are used for the existing systems that employ a portion of the cover picture as the watermark image (Aminuddin & Ernawan, 2022; Huang et al., 2019). A collection of embedding bits that includes the authentication bits can also be used to generate a watermark. (Huang et al., 2019; D. Singh & Singh, 2019) By changing the host image's bits, the embedding watermark in fragile watermarking can be carried out. The Least Significant Bit (LSB) was used to incorporate watermark bits, rendering them undetectable to the human eye (Molina-Garcia et al., 2020). An inverse process comparing the LSB in sub-block and the current image LSB bit allow the image perform tamper localization.

2.2.4 Embedding Sub-bands and Sub-block

In DWT, high frequency parts stand for complete information of image's edge, texture and contour etc. Embedding watermarking in these having high imperceptibility. But if any tamper attack conducted will cause a low security result. Meanwhile, the lower frequency band consist of detail of the image so that watermarking information embedded in low frequency coefficients has better robustness. (Dimple Bansal & Manish Mathuria, 2017) Hence, LL coefficient of DWT is selected to perform the copyright logo information embedding in the research to test the ability of the logo extraction result after some image attack. 8x8 block division is used to perform DWT because it is widely used in the existing scheme to obtain 4x4 LL coefficient where it got 16 of bit can be embedded with copyright information (Nasir N. Hurrah et al., 2018). In the fragile embedding for authentication, block division 6x6 and sub-block 3x3 is used because the calculation will involve embedding 9 authentication bit that fit into 9 pixel from the 3x3 sub-block.

2.2.5 Singular Value Decomposition (SVD)

SVD is a widely used technique in image processing and has been extensively used in image watermarking. The SVD technique is used in image watermarking to transform the image data into a domain that is suitable for watermark embedding while preserving the visual quality of the original image. The SVD transform allows the image to be decomposed into a set of singular values and corresponding singular vectors. The singular values and vectors can be used to modify the image data in a way that is robust to various image processing attacks while maintaining the perceptual quality of the original image. In the context of image watermarking, SVD is used to hide the watermark by modifying the singular values or vectors in a way that the watermark is imperceptible and difficult to remove. The modified singular values or vectors can be used to extract the watermark at a later stage. SVD is an effective technique to embed a watermark in an image since it provides high robustness against common image processing attacks and preserves the visual quality of the original image.

2.2.6 Embedding Luminance Y Component from RGB Conversion

YCbCr and RGB color spaces is that the Y component in YCbCr represents the luminance information, which is the most important information for human perception of images. By embedding the watermark in the Y component, the imperceptibility of the watermarked image can be maintained at a high level while ensuring robustness against attacks. Additionally, converting between YCbCr and RGB can help to spread the watermark across different color channels, increasing its robustness. Finally, by using the inverse transformation to convert the watermarked image back to RGB, the original color information can be preserved, ensuring that the watermarked image appears the same as the original to the human eye. The formula below able to obtain YCbCr image from RGB value.

$$\begin{aligned} Y &= 0.299 \times R + 0.587 \times G + 0.114 \times B \\ Cb &= 0.596 \times R - 0.275 \times G - 0.321 \times B \\ Cr &= 0.212 \times R - 0.523 \times G - 0.311 \times B \end{aligned} \tag{2.2}$$

The embedding randomness can be enhanced since all RGB value involve in process obtaining Y. Therefore, an inverse process with new Y will obtain new RGB value to form a watermarked image having high imperceptibility. The inverse converting YCbCr to RGB can be performed using the formula below. (Hussein & Sulaimani, 2012)

$$\begin{aligned} R' &= Y' + 0.956 \times Cb + 0.620 \times Cr \\ G' &= Y' - 0.272 \times Cb - 0.\ 647 \times Cr \\ B' &= Y' - 1.108 \times Cb + 1.705 \times Cr \end{aligned} \tag{2.3}$$

2.3 The Existing Dual Image Watermarking Scheme

The table below shows comparison analysis of the reviewed watermarking schemes:

Table 2.1 Summary of existing watermarking scheme

	Lusia Rakhmawati et al., (2020)	Duan et al., (2020)	Nasir N. Hurrah et al., (2018)	Deepa B. Maheshwari (2018)	Jobin Abraham & Dr. Varghese Paul (2017)	(Ahmadi et al., 2021)
Copyright embedding method	DCT	DWT	DWT-DCT	DWT	DWT-DCT	DWT
Embedding sub-bands	8 x 8 blocks	LL	4 x 4 blocks	LL	LL, HL, LH	LL, HH
Host image size	512 x 512	512 x 512	512 x 512	512 x 512	512 X 512	512 x 512
Watermark size	32 x 32	32 x 32	64 x 64	64 x 64 & 128 x 128	32 x 32	32 x 32 & 64 x 64
Watermark image type	Grey and RGB	RGB	Grey and RGB	Grey	Grey	RGB
Copyright protection	Yes	Yes	Yes	Yes	Yes	Yes
Authentication	Yes	Yes	Yes	No	No	Yes

2.4 Summary of The Existing Dual Image Watermarking Scheme

The watermarking scheme proposed by Nasir N. Hurrah et al., (2018) using combination of DWT-DCT for both copyright protection and spatial technique for authentication. Their scheme able to resist one until three attacks with Normalized Correlation (NCC) 0.95 in average, tamper localization of average 45% of bit error rate (BER), imperceptibility with value greater than 41 dB. Their scheme shows high watermarking robustness, imperceptibility, and ability tamper localization comparing single watermarking scheme. However, there is an issue only able detect a tampered region in their image authentication solution.

Dual watermarking scheme proposed by Lusia Rakhmawati et al., (2020) using spatial and DCT method is superior compared to other existing scheme in terms of watermarking robustness, imperceptibility and tamper localization. The solution they proposed is to provide image ability in both copyright protection, and content authentication. The dual watermark is evaluated one by one separately with the PSNR value. The robust watermark produce PSNR 41.83dB, fragile watermark produce 37.27dB, and dual watermark produce 35.69dB. The scheme not having significant disadvantages proved by various measurement data compared to other schemes. Hence, it is suitable for secure image since it produces great ability in copyright protection and authentication.

Scheme proposed by Jobin Abraham & Dr. Varghese Paul (2017) is aimed to perform higher imperceptibility in robustness watermarking combining method DWT and DCT. Their objective is to perform high imperceptibility with implementation of multiple transform domain operation. As result, each transform domain operation able to overcome the disadvantage of each other. The watermarked image imperceptibility is tested using the PSNR measurement. The scheme can perform high imperceptibility robust watermarking but fail to clearly extract watermark in some types of attack.

Next, scheme proposed by Deepa B. Maheshwari (2018) perform dual image watermark separately with primary and secondary watermark with DWT and singular value decomposition (SVD) respectively. The primary watermark in their scheme able to be extracted under many types of image attack but the secondary watermark extraction is not easily be recognized after most of the image attack type.

(Ahmadi et al., 2021) proposed scheme using method embedding watermark into LL sub-band in blue channel and fragile model in HH-sub band of all channels. The proposed scheme offers a feasible approach to safeguard valuable and authentic color images. The experimental and comparative analysis demonstrate that the proposed scheme outperforms the existing methods in terms of high robustness, imperceptibility, and capacity, while maintaining a good accuracy rate in identifying the tampered regions of an image.

2.5 Relevance of Comparison

Through the study of existing schemes, each has its own different characteristics, strengths, and weaknesses in terms of copyright protection and authentication. The reviewed watermarking scheme especially DWT based dual image watermarking schemes that able to provide image both copyright protection and authentication are mostly embedding the watermark into the RGB channel with different process and calculation. Therefore, the analysis giving motivation and inspiration that the DWT-based dual watermarking scheme for RGB images is potentially having capacity of further development in a different method.

CHAPTER 3

METHODLOGY

3.1 Introduction

This chapter discuss about the proppposed methodology of the research. The methodology define the process of the research. The detail explaination of the flow and process of the technique image watermaking technique used in this research will be included in this chapter.

3.2 Research Framework

The research consists of 7 phases. The consists will begin with the phase literature review to analyse the existing schemes in terms of features, advantages, and disadvantages. Their experimental results also will be collected to be benchmark comparing each other along with the proposed scheme. The second phase is conduct experimental design consist of the defining research requirement setup and block diagrams describing the watermarking schemes workflow. The evaluation measurements also will be defined in this phase. The third phase is developing the watermarking scheme. In the 4th phase, if the watermarking scheme is failed to produce watermarked image with copyright protection along with the authentication, the phase will go back to the third, fix and modify the watermarking scheme again. Else, the research go into 5th phase. The value of the validation measurement will use as benchmark compared to other existing scheme. At the end, a documentation recording the result comparing each other scheme will be prepared.

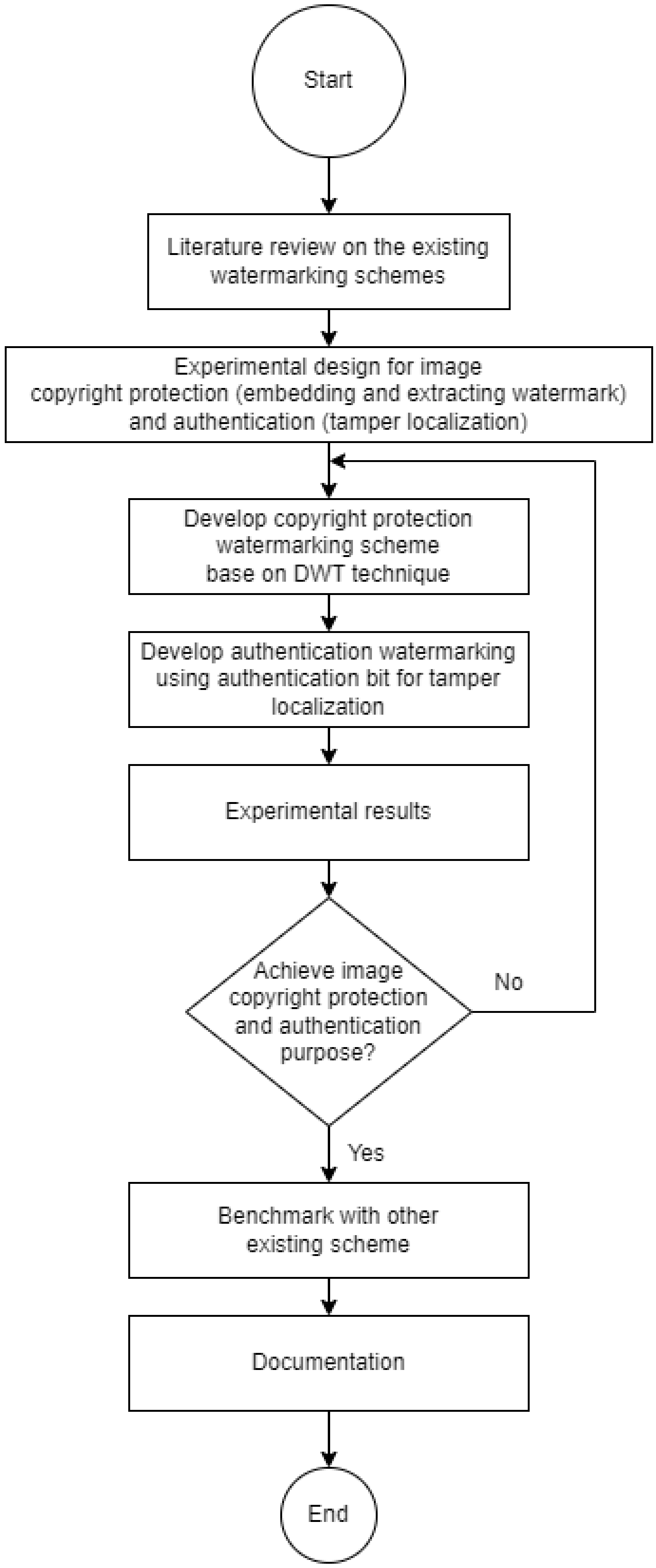

Start
Literature review on the existing watermarking schemes
Experimental design for image copyright protection (embedding and extracting watermark) and authentication (tamper localization)
Develop copyright protection watermarking scheme base on DWT technique
Develop authentication watermarking using authentication bit for tamper localization
Experimental results
Achieve image copyright protection and authentication purpose?
No
Yes
Benchmark with other existing scheme
Documentation
End

Figure 3.1 Research Framework

3.3 Research Requirement

The research is mainly using MATLAB to conduct the image processing works. The research is required to use the RGB host image with size 512 x 512 to conduct the watermarking scheme evaluation. Besides that, a black and white watermark with size 32 x 32 will be used for the copyright protection watermarking in the research.

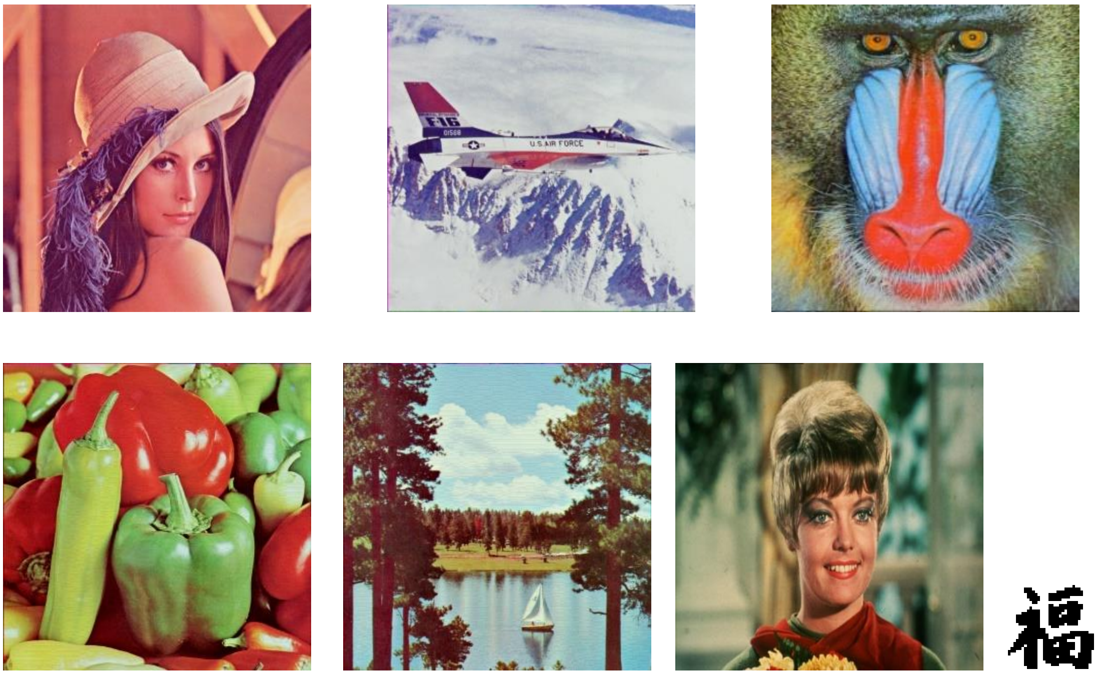
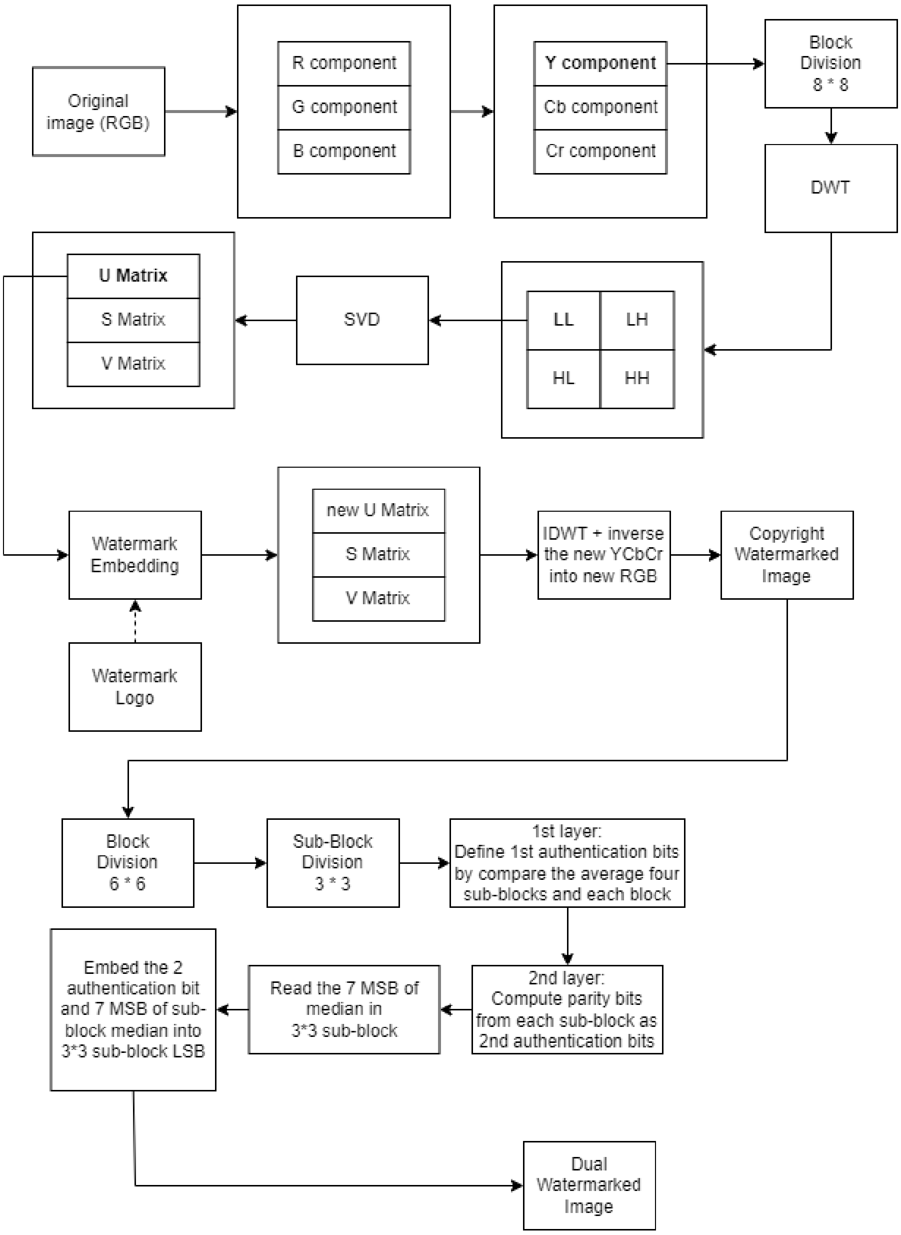


Figure 3.2 Images and logo used for the experiment

3.4 Propose Design

The research is going to implement Discrete Wavelet Transform (DWT) technique to perform a copyright watermarking marking process to an image. This robust watermarking purpose is to provide image copyright protection by embed information from a watermark image into an input image. Next, the authentication watermarking with fragile watermarking technique modify LSB with authentication bits is performed to provide image authentication feature. The block diagram below shows the general process of the proposed scheme:



Original image (RGB)
R component
G component
B component
Y component
Cb component
Cr component
Block Division 8 * 8
DWT
LL
LH
HL
HH
SVD
U Matrix
S Matrix
V Matrix
Watermark Embedding
Watermark Logo
new U Matrix
S Matrix
V Matrix
IDWT + inverse the new YCbCr into new RGB
Copyright Watermarked Image
Block Division 6 * 6
Sub-Block Division 3 * 3
1st layer: Define 1st authentication bits by compare the average four sub-blocks and each block
2nd layer: Compute parity bits from each sub-block as 2nd authentication bits
Read the 7 MSB of median in 3*3 sub-block
Embed the 2 authentication bit and 7 MSB of sub-block median into 3*3 sub-block LSB
Dual Watermarked Image

Figure 3.3 The block diagram showing process of the proposed watermarking scheme

There are two blocks selected and performed watermark embedding based on the black and white watermark. The two selected blocks value after embedding is related to the black and white bit of watermark in the embedding calculation. Hence, a same process conducts DWT on the watermarked image, then deduct the two selected embedding block in the LL coefficient able to obtain back the black and white bit of watermark to complete the watermark extraction.

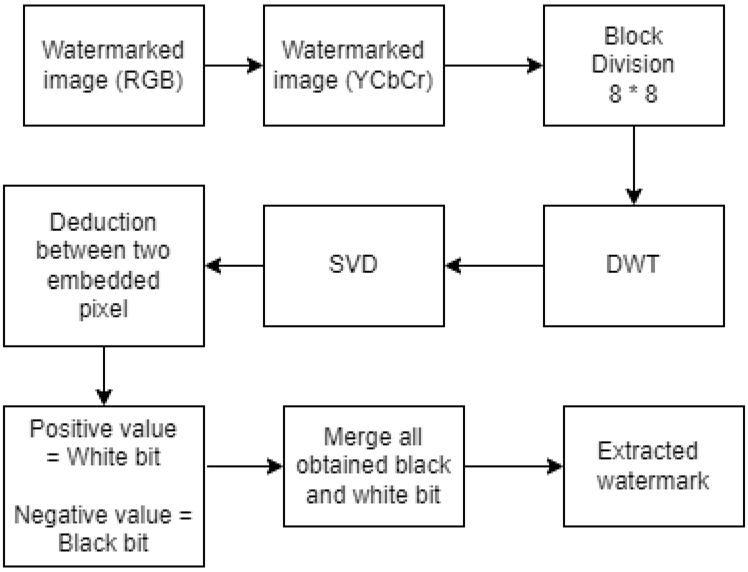

Watermarked image (RGB)
Watermarked image (YCbCr)
Block Division 8 * 8
DWT
SVD
Deduction between two embedded pixel
Positive value = White bit
Negative value = Black bit
Merge all obtained black and white bit
Extracted watermark

Figure 3.4 The block diagram showing process of the watermark extraction

To perform tamper detection, a tampered image will perform again the authentication bit obtaining process. Next, compare the new obtained authentication bit with the LSB that embedded in correspond sub-block during authentication watermarking process. When the authentication bit shows not equal means tamper detected.

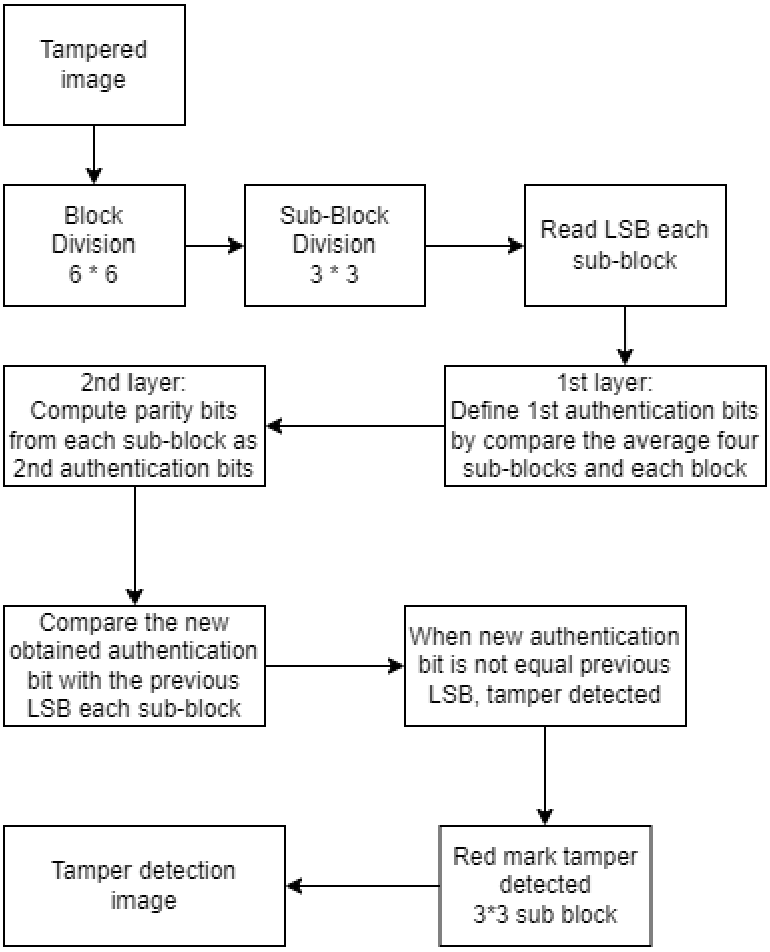

Tampered image
Block Division 6 * 6
Sub-Block Division 3 * 3
Read LSB each sub-block
1st layer: Define 1st authentication bits by compare the average four sub-blocks and each block
2nd layer: Compute parity bits from each sub-block as 2nd authentication bits
Compare the new obtained authentication bit with the previous LSB each sub-block
When new authentication bit is not equal previous LSB, tamper detected
Red mark tamper detected 3*3 sub block
Tamper detection image

Figure 3.5 The block diagram showing process of the tamper detection

3.4.1 Copyright Protection Watermarking Algorithm

As the block diagram described in the previous section, the first process of the proposed scheme is robust watermarking using DWT. Below is the detail process and algorithm regarding the DWT watermarking. An alfa value variable indicates the threshold embedding the watermark is set to 0.027 because it is an optimal threshold based on a trade-off between robustness and imperceptibility. (Ernawan & Ariatmanto, 2019)

Input RGB image m * n pixel, i_o
Black & White Watermark, i_w

Step 1 Convert RGB channels of image i_o into luminance channels, YCbCr.

Step 2 Divide i_o into 8 * 8 block, (m/8)*(n/8)

Step 3 Block selection f_n (x,y) where are the n-th block pixel values of the image i_o

Step 4 Perform DWT on Y channel of i_o using 'Haar' wavelet to obtain image value of approximation (LL), horizontal (HL), vertical (LH) and diagonal (HH) coefficients

Step 5 Select approximation coefficient, LL to perform embedding watermark

Step 6 Perform Singular Value Decomposition (SVD) to the LL image value matrix, to obtain left singular value (Uimg), singular value (Simg), right singular value (Vimp)

Step 7 Select Uimg to define the alpha value by the algorithm below:

```
if(Uimg(a,1)<0)
  x1 = -1; alfa=-1*T;
  elseif(Uimg(a,1)>0)
  x1 = 1; alfa=T;
  end

  if(Uimg(b,1)<0)
  y1 = -1; alfa=-1*T;
  elseif(Uimg(b,1)>0)
  y1 = 1; alfa=T;
  end
```

Step 8 Read black and white bit from i_w perform the embedding. Value of the embedding determine by algorithm:

```
  m=(abs(double(Uimg(a,1)))+abs(double(Uimg(b,1))))/2;
  if(message(u)==1)
        Uimg(a,1)=(x1*m)+alfa/2;
        Uimg(b,1)=(y1*m)-alfa/2;
  elseif(message(u)==0)
        Uimg(a,1)=(x1*m)-alfa/2;
        Uimg(b,1)=(y1*m)+alfa/2;
  end
```

Step 9 Inverse SVD values by Uimg*Simg*Vimg to obtain new LL coefficient value

Step 10 Inverse DWT (IDWT) with new LL coefficient value, original LH, HL, HH coefficient value

Step 11 Inverse the conversion from luminance channels to RGB channels. New value of luminance channel Y is used for the calculation obtain a new RGB channels value.

Step 12 Repeat the steps again until all blocks f_n (x,y) are finished embedding

Output Copyright watermarked image i_c

3.4.2 Authentication Watermarking Algorithm

Authentication watermark is performed in a self-embedding way that modify LSB to provide image an authentication feature. Below is the algorithm of the authentication watermarking.

Input Copyright watermarked **i**mage resized to 516 * 516 pixel, i_c

Step 1 Divide i_c into 6 * 6 block, (m/6) * (n/6)

Step 2 Divide again all 6 * 6 block into 3 * 3 sub-block

Step 3 Remove least significant bit (LSB) from the value of image

Step 4 Compare the average of sum image value between 6 * 6 each blocks i_c and 3 * 3 sub-blocks in it. If sub-block having bigger average value, set the 1st authentication bit v = 1, else v = 0

Step 5 Check the parity of the average of sum image value in each 3 * 3 sub-blocks, even number set the 2nd authentication bit p = 1, else p = 0

Step 6 Read the 7 MSB from the value of the sub-block median

Step 7 Embed the sub-block LSB with the sequence v, p, sub-block median 7 MSB

Output Dual watermarked image i_d

3.4.3 Tamper Localization Algorithm

The tampered image able to localize the tampered area by compare the new computed authentication bit with the authentication bit that was embedded in LSB each sub-block LSB during the authentication watermarking process. Below is the algorithm of tamper localization.

Input Tampered image, i_t

Step 1 Divide i_t into 6 * 6 block, (m/6) * (n/6)

Step 2 Divide again all 6 * 6 block into 3 * 3 sub-block

Step 3 Read least significant bit (LSB) from subblock (1,1) and (1,2)

Step 4 Remove LSB from the value of image

Step 5 Compare the average of sum image value between 6 * 6 each blocks i_t and 3 * 3 sub-blocks in it. If sub-block having bigger average value, set the 1st authentication bit v = 1, else v = 0

Step 6 Check the parity of the average of sum image value in each 3 * 3 sub-blocks, even number set the 2nd authentication bit p = 1, else p = 0

Step 7 Read the 7 MSB from the value of the sub-block median

Step 8 Compare the v and p authentication bit along with 7 MSB with the LSB subblock, if both match mean not tampered, else proceed step 9

Step 9 White mark sub-block that detected tamper

Output Tamper detected image i_{td}

3.4.4 Watermark Extraction Algorithm

Below is the watermark extraction algorithm. It shares the same initial process as watermarking algorithm. At the step comparing the approximation coefficient (LL) value in singular value decomposition able to obtain back the watermark black and white bit.

```
Input     Watermarked Image m * n pixel, $i_d$
          Watermark size, $S_{i_w}$
Step 1  Convert RGB channels of image $i_d$ into luminance channels, YCbCr.
Step 2  Divide $i_d$ into 8 * 8 block, (m/8)*(n/8)
Step 3  Block selection $f_n$ (x,y) where are the n-th block pixel values of the image $i_d$
Step 4  Perform DWT on Y channel of $i_d$ using 'Haar' wavelet to obtain image value of
        approximation (LL),   horizontal (HL), vertical (LH) and diagonal (HH)
        coefficients
Step 5  Select approximation coefficient, LL to perform embedding watermark
Step 6  Perform Singular Value Decomposition (SVD) to the LL image value matrix, to
        obtain left singular value (Uimg), singular value (Simg), right singular value
         (Vimp)
Step 7  Select Uimg to compare the Uimg value of (a,1) and (b,1) value by the
        algorithm below:
        if(abs(UWimg(a,1))-abs(UWimg(b,1))>0)

            Watermark(u)=1; %white bit

        else

            Watermark(u)=0; %black bit

         End

        Step 8  Loop algorithm above until size of watermark $S_{i_w}$ reached

        Step 9  Arrange each bit to form the original watermark.

Output    Extracted watermarked $i_e$
```

3.5 Evaluation Plan

The proposed solution will be validated in three aspects. These aspects include imperceptibility, robustness and the ability in tamper localization. The detailed formulations and value implications of these measurements are discussed in the following sections.

3.5.1 Imperceptibility Measurement

Imperceptibility can be evaluated by Structure Similarity Index Method (SSIM), Absolute Reconstruction Error (ARE), Mean Square Error (MSE), and Peak Signal to Noise Ratio (PSNR) value. The similarity between the watermarked image and the host image was calculated using the SSIM. The SSIM index is defined by:

$$SSIM(x,y) = [l(x,y)]^{\alpha} \cdot [c(x,y)]^{\beta} \cdot [s(x,y)]^{\gamma} \qquad 3.1$$

where α>0, β>0, γ>0, are parameters to define the relative importance of the three components l, c and s. The ARE was used to measure the distortion of the watermarked image. The ARE is defined by:

$$MSE = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(f(k,1) - g(k,1))^2 \qquad 3.2$$

The effectiveness of picture reconstruction was evaluated using the PSNR. Higher PSNR indicates closer alignment with the original host image.

$$PSNR = 10\log \frac{(255)^2}{MSE} xxxxxxxxx \qquad 3.3$$

3.5.2 Robustness Measurement

The normalised cross-correlation (NC) are used to assess how robust the watermarked image is. The range of the NC value between 0 and 1 is used to gauge how resilient the retrieved watermark is. The recovery of the watermark is closest to the original watermark if the NC values are higher. Below is the formula of NC:

$$NC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} W(i,j) \cdot W*(i,j)}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N} W(i,j)^2 \sum_{i=1}\sum_{j=1} W*(i,j)^2}} \qquad 3.4$$

where, W *(i, j) is the watermark recovery and W (i, j) is the original watermark. M and N denote the row and column sizes of the watermark image.

Bit Error Rate (BER) is a metric used to quantify the errors occurring in a digital communication system. It represents the percentage of bits that are transmitted incorrectly over a communication channel. The lower the BER, the better the quality of the communication channel.

$$BER = \frac{n_{error}}{n_{bit}} \qquad 3.5$$

Where n_{error} mean number of received bits in error, while n_{bit} mean the total number of transmitted bits.

3.5.3 Tamper Localization Measurement

For the authentication part, True Positive Rate (TPR), False Negative Rate (FNR), False Positive Rate (FPR), and True Negative Rate (FNR) are used to measure the ratio between detected area against the real tampered. The higher TPR value means the tamper detect zone is more correctly be detected. In opposite, FNR means the ratio between the undetected area compared to the real tampered area. TPR and FNR are define as::

$$TPR = \frac{TP}{TP - FN} = 1 - FNR \tag{3.6}$$

$$FNR = \frac{FN}{TP + FN} = 1 - TPR \tag{3.7}$$

The FPR represents the ratio between the false detected area against the untampered area. The range of FPR values is between 0 to 1 indicate the lower to higher detection of the untampered area as tampered area. In opposite, TNR is a ratio of non-detected to untampered region. FPR and TNR are define as:

$$FPR = \frac{FP}{FP + TN} \tag{3.8}$$

$$TNR = \frac{TN}{FP + TN} \tag{3.9}$$

The precision shows how precisely the image was tampered with. The proposed scheme was able to provide high true positive values and low false positive values, as indicated by the greater and lower precision value. To evaluate the effectiveness of the suggested approach, the tampering detection accuracy is evaluated with F1 Score.

$$Precision = \frac{TPR}{TPR + FPR} \tag{3.10}$$

$$Recall = \frac{TPR}{TPR + FNR} \tag{3.11}$$

$$F1\,Score = 2 * \frac{Precision * Recall}{Precision + Recall} \tag{3.12}$$

3.6 Potential Use of Proposed Solution

Digital watermarking is a technology that can safely and delicately hide information in digital media content. The technology able to help identify the origin of unauthorized copies and trace them back to the previous legitimate recipient or legitimate content holder. Digital watermarking with high imperceptibility prevents the quality and the value of the content itself from being diminished. Robustness watermarking ensures that the watermark retains its readability after any modification, processing, or media conversion.

The greatest potential of digital watermarking lies in dealing with digital content pirates. With the growing amount of pay-per-view (PPV) content nowadays, pirates can benefit from illegal access to digital content through recording and downloading, etc. The proposed DWT image watermarking technique creates watermarks that are completely invisible under normal viewing conditions, and watermarking technology provides a way to encapsulate information in digital content. As a result, digital watermarks can generate detailed information including precise date, time and location information in the watermarks depending on the situation. This makes it possible to accurately identify the piracy in tracking and reducing such infringement. In addition, authentication watermarking gives digital content the ability to identify the possibility of being modified. This allows digital content creators to protect their works from low-quality secondary creations and allow them to obtain legal accountability.

From the above examples, the proposed scheme can be used as a way to track illegal copies and alterations of digital content, helping to improve copyright liability issues. It also shows a potential in DWT based dual image watermarking scheme that provide both copyright protection and authentication fields which are lack of investigate currently.

3.7 Gantt Chart

Gantt chart shows the progress of every milestone in the research with its starting and ending date. The Gantt chart describe the estimate milestone progress of this research is attached to the Appendix.

CHAPTER 4

RESULT AND DISCUSSION

4.1 Introduction

Chapter 4 present the results and discussion of the proposed image watermarking technique compared to other existed schemes. The proposed technique aims to embed watermarks providing image copyright protection and authentication for tamper detection while maintaining imperceptibility, robustness. In this chapter, the results of the experiments and analysis on the imperceptibility, robustness, and tamper detection ability of the proposed technique are represented.

The first section of this chapter discusses the results of imperceptibility analysis. The proposed scheme is tested with a set of material images to evaluate the watermark can be embedded into the host image without being visually perceptible.

The second section of this chapter will discuss the robustness of the proposed technique. Experiments to test the ability of the watermarking technique to withstand various attacks, such as noise addition, compression, and cropping.

The third section of this chapter will focus on the tamper detection ability of the proposed technique. The accuracy, precision and F1-Score are used to measure the tamper detection ability.

4.2 Imperceptibility Experiment

Two widely used metrics for evaluating image quality are Peak Signal to Noise Ratio (PSNR) and Structural Similarity Index (SSIM). In this section, the experiment use PSNR and SSIM to measure the performance of our proposed watermarking scheme on five host images. Result of two existing dual watermarking schemes are used for comparison to determine the superiority of the proposed schemes. Figure 4.1 shows the host image before and after the dual watermark embedding. Table 4.1 shows the result along with their average value. Visualized data with line graph comparison of PSNR and SSIM are shown in Figure 4.2 and Figure 4.3.

Figure 4.1 Dual Watermarked Images Showing High Imperceptibility Embedding

Table 4.1 Comparison data PSNR and SSIM

	X.L. Liu et al (2018)		Lusia et al (2020)		Proposed Scheme	
Cover image	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
Lena	34.8722	0.9684	36.1430	0.895	**46.1588**	**0.9988**
Airplane	34.6581	**0.9612**	36.1600	0.901	**43.5675**	0.9504
Baboon	33.8956	0.9710	35.5450	0.970	**44.5454**	**0.9961**
Peppers	34.9268	0.9605	35.3470	0.900	**46.8007**	**0.9989**
Sailboat	34.8855	0.9748	35.2490	0.917	**44.2202**	**0.9890**
Average	34.6476	0.9672	35.6870	0.916	**45.0585**	**0.9866**

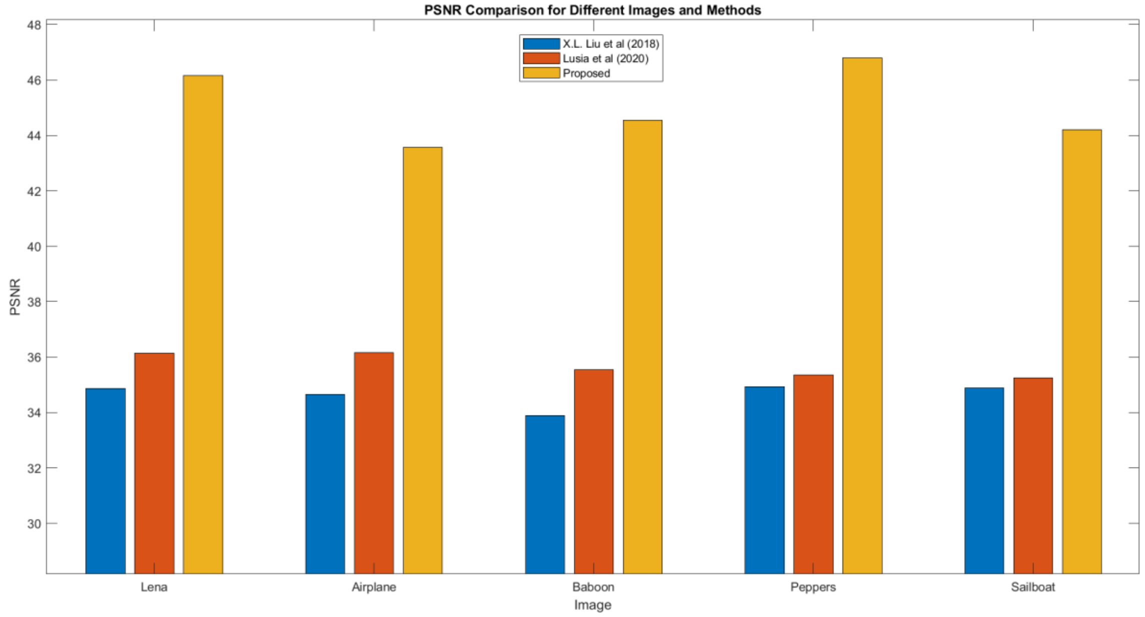


Figure 4.2 Comparison PSNR values of the dual watermarked image between the schemes

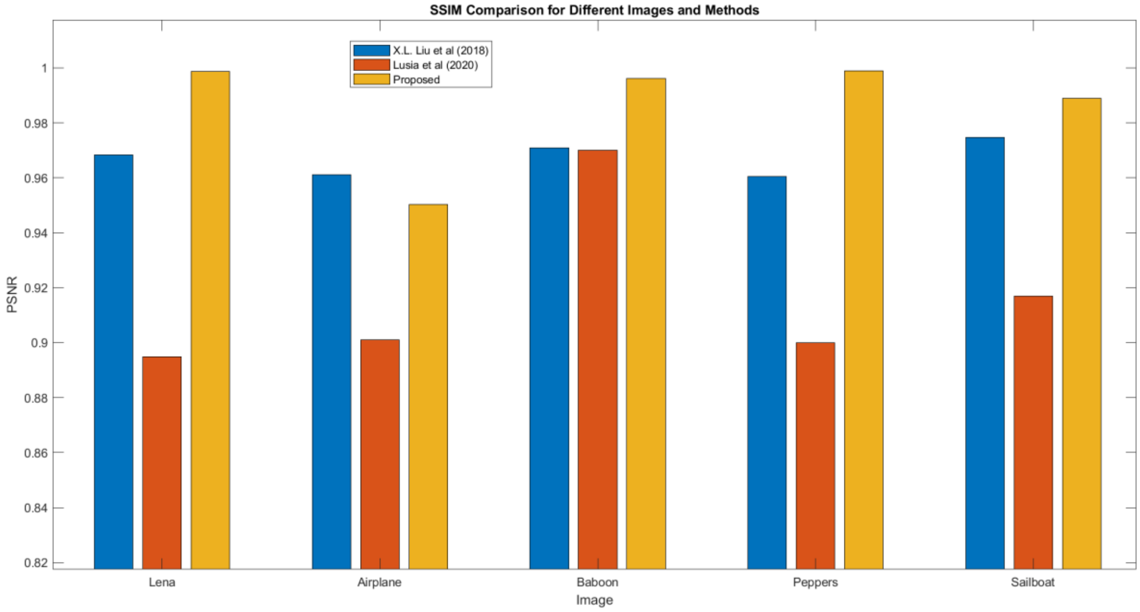


Figure 4.3 Comparison SSIM values of the dual watermarked image between the schemes

Table 4.1 presents the performance of different image watermarking schemes, including X.L. Liu et al (2018), Lusia Rakhmawati et al (2020), and the proposed scheme in the evaluation metrics of Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM) for various cover images.

For the Lena image, the proposed scheme achieved the highest PSNR value of 46.1588, indicating superior image quality preservation compared to X.L. Liu et al (2018) and Lusia et al (2020). The SSIM value for the proposed scheme was also the highest at 0.9988, indicating a high level of structural similarity between the watermarked and original images. The other two schemes, X.L. Liu et al (2018) and Lusia et al (2020), exhibited lower PSNR and SSIM values for the Lena image.

Similar trends can be observed for the Airplane, Baboon, Peppers, and Sailboat images. The proposed scheme consistently outperformed the other two schemes in terms of both PSNR and SSIM values. The average PSNR value for the proposed scheme was 45.0585, higher than that of X.L. Liu et al (2018) and Lusia et al (2020). Similarly, the average SSIM value for the proposed scheme was 0.9866, indicating better structural similarity compared to the other schemes.

Overall, the comparative analysis demonstrates that the proposed scheme excels in preserving image quality and maintaining structural similarity across various cover images. It achieves higher PSNR and SSIM values compared to the existing schemes, indicating its effectiveness in watermarking images while minimizing distortion. The results highlight the superiority of the proposed scheme in terms of image fidelity and quality preservation, making it a promising approach for image watermarking applications.

Based on results, it can be concluded that the proposed scheme for DWT and fragile watermarking on RGB images for copyright protection and authentication has provided superior performance compared to the existing schemes by Liu et al., (2018) and Lusia Rakhmawati et al., (2020) The proposed scheme has achieved an average PSNR of 45.0585 and SSIM of 0.9866, which is significantly higher than the existing schemes.

The higher PSNR value indicates that the proposed scheme has lesser distortion between the original and watermarked image, which means that the watermark is more imperceptible. Similarly, the higher SSIM value indicates that the proposed scheme has better structural similarity with the original image, which means that the watermark is well-preserved and has less impact on the image quality. Therefore, it can be inferred that the proposed scheme for DWT and fragile watermarking on RGB images has a higher potential for copyright protection and authentication compared to the existing schemes.

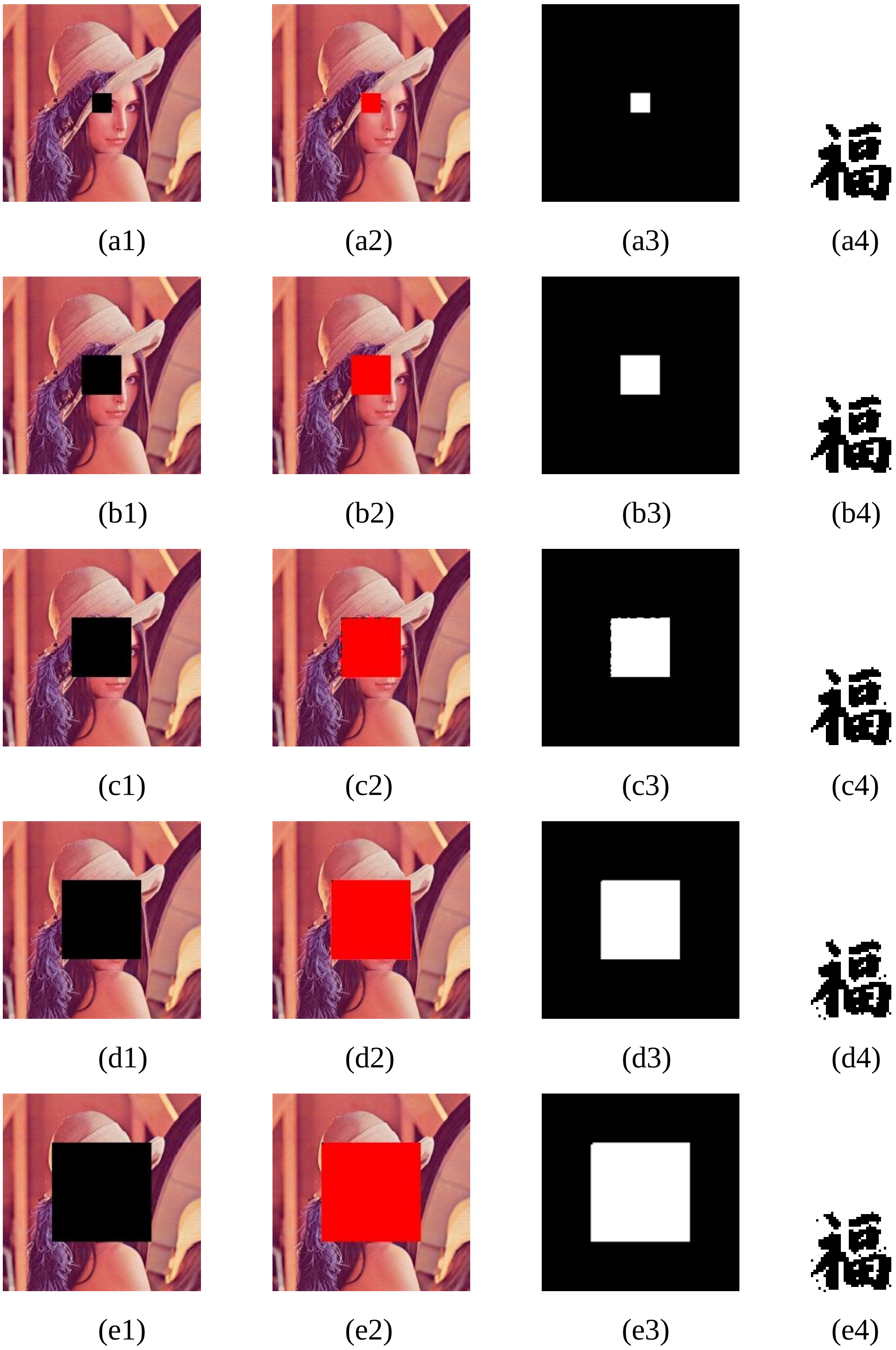
4.3 Tamper Detection and Watermark Extraction under Regular Attack

In this experiment, the tamper detection performance of the proposed watermarking scheme under regular and irregular attacks is evaluated. The true positive (TP), false negative (FN), false positive (FP), and true negative (TN) detection areas were calculated by performing a bit-wise OR logic operation between the watermarked image, the tampered image, and the red marked detected tampered image. The TP area represents the correctly detected tampered area, while the FN area represents the missed tampered area. The FP area indicates the incorrectly detected tampered area, and the TN area shows the correctly detected non-tampered area.

The rates of TP, FN, FP, and TN areas were then used to calculate the f1-score, precision, and accuracy of the tamper detection and watermark extraction. The f1-score is a measure of the trade-off between precision and recall, while precision is the fraction of true positives among the total number of detections, and accuracy is the fraction of true detections among the total number of pixels.

Figure 4.4 shows the watermarked image, red mark tamper detection image, true positive detection area image, and output of extraction watermark from regular attack. Table 4.2 shows the result and comparison of the regular attack tamper detection performance. Figure 4.5 shows visualized data comparison of all aspect of the measurements in terms of tamper detection and watermark extraction.

The results showed that the proposed scheme achieved high accuracy, precision and f1-score in tamper detection They were mostly higher than existing schemes by Duan et al., (2020). Besides that, the NC value is higher and BER is lower than Duan et al., (2020) scheme. Hence, the result indicating the superiority of the proposed method in protecting digital images from tampering while preserving the embedded watermark.



(a1) (a2) (a3) (a4)

(b1) (b2) (b3) (b4)

(c1) (c2) (c3) (c4)

(d1) (d2) (d3) (d4)

(e1) (e2) (e3) (e4)

Figure 4.4 Image with regular attack from 10% to 50% (a-e 1), detected tamper (a-e 2), correct detected tamper (a-e 3), and watermark extraction from the regular attact (a-e 4)

Table 4.2 Comparison data of tamper detection performance under regular attacks

Tampering rate	Scheme	TPR	FNR	FPR	TNR	Precision	F-1 Score	Accuracy
50%	Duan et al., (2020)	1.0000	0.0000	0.0405	0.9595	0.9611	0.9802	0.9697
	Proposed	1.0000	0.0000	**0.0026**	**0.9974**	**0.9974**	**0.9987**	**0.9980**
40%	Duan et al., (2020)	**1.0000**	**0.0000**	0.0370	0.9630	0.9643	0.9818	0.9689
	Proposed	0.9998	0.0002	**0.0093**	**0.9907**	**0.9908**	**0.9953**	**0.9922**
30%	Duan et al., (2020)	**1.0000**	**0.0000**	0.0079	0.9921	0.9922	**0.9961**	**0.9928**
	Proposed	0.9840	0.0160	**0.0072**	**0.9928**	**0.9927**	0.9883	0.9920
20%	Duan et al., (2020)	1.0000	0.0000	0.0238	0.9762	0.9768	0.9883	0.9772
	Proposed	1.0000	0.0000	**0.0000**	**1.0000**	**1.0000**	**1.0000**	**1.0000**
10%	Duan et al., (2020)	1.0000	0.0000	0.0058	0.9942	0.9943	0.9971	0.9943
	Proposed	1.0000	0.0000	**0.0012**	**0.9988**	**0.9988**	**0.9994**	**0.9988**

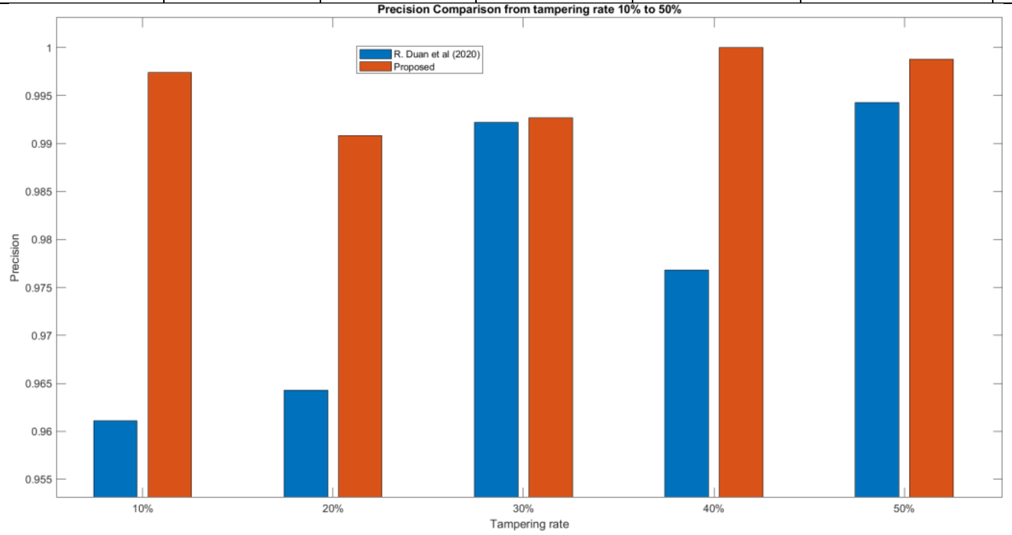


Figure 4.5 Precision Comparison of Tamper Detection from Different Tampering Rate

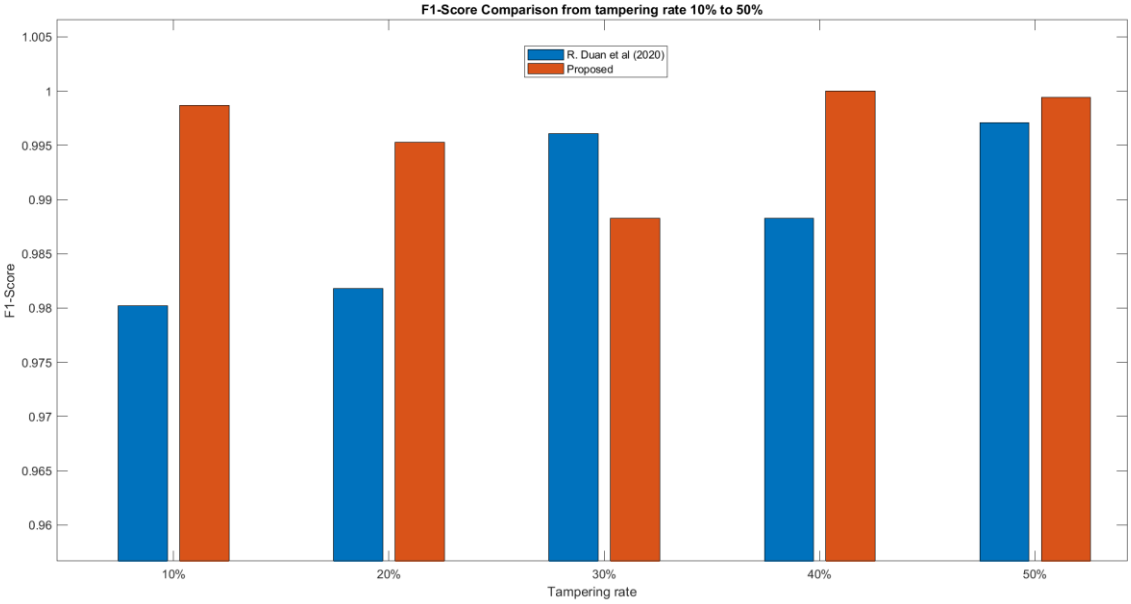


Figure 4.6 F1-Score Comparison of Tamper Detection from Different Tampering Rate

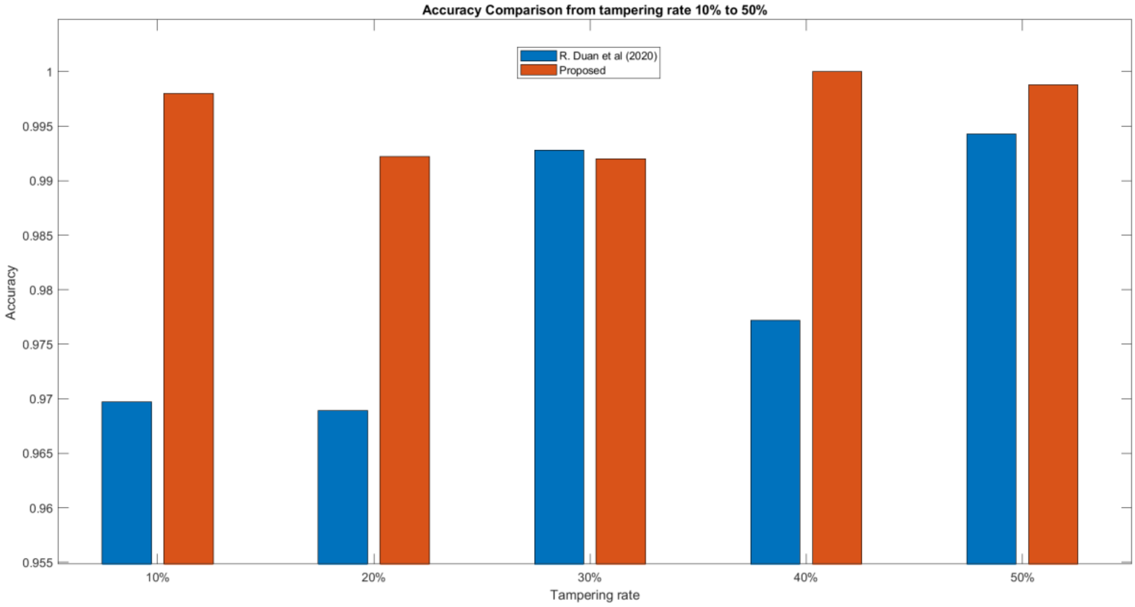


Figure 4.7 Accuracy Comparison of Tamper Detection from Different Tampering Rate

Table 4.3 the tamper detection performance under regular attacks, specifically varying tampering rates from 10% to 50%. The analysis compares the performance of Duan et al. (2020) and the proposed scheme based on several evaluation metrics, including True Positive Rate (TPR), False Negative Rate (FNR), False Positive Rate (FPR), True Negative Rate (TNR), Precision, F-1 Score, and Accuracy.

For the tampering rate of 50%, both Duan et al. (2020) and the proposed scheme achieved perfect TPR values of 1.0000, indicating successful detection of tampering. However, the proposed scheme exhibited a significantly lower FPR of 0.0026 compared to Duan et al. (2020), which had an FPR of 0.0405. This demonstrates the improved capability of the proposed scheme in correctly identifying non-tampered regions while minimizing false alarms.

Similar trends can be observed for the tampering rates of 40%, 30%, and 20%. The proposed scheme consistently outperformed Duan et al. (2020) in terms of FPR, achieving lower values and indicating a higher ability to distinguish tampered and non-tampered regions accurately. For the tampering rate of 10%, both schemes achieved excellent performance with perfect TPR values and low FPR values. However, the proposed scheme demonstrated a slightly lower FPR of 0.0012 compared to Duan et al. (2020), which had an FPR of 0.0058.

Furthermore, the proposed scheme consistently exhibited high Precision, F-1 Score, and Accuracy values across all tampering rates, indicating its effectiveness in correctly identifying tampered regions and minimizing false positives. The visualized results in Figure 4.5, Figure 4.6, and Figure 4.7 demonstrate the superior tamper detection capabilities of the proposed scheme compared to Duan et al. (2020), especially in terms of minimizing false positives and achieving high accuracy.

Overall, the comparative analysis highlights the advantages of the proposed scheme in tamper detection under regular attacks. It consistently outperforms Duan et al. (2020) in terms of FPR, Precision, F-1 Score, and Accuracy, indicating its robustness and reliability in detecting tampering accurately. The proposed scheme presents a promising solution for tamper detection applications, offering improved performance and greater potential for practical implementation.

Table 4.3 Comparison data of extraction under regular attacks

Tampering rate	Scheme	NC	BER
10%	Duan et al., (2020)	0.9872	0.0127
	Proposed	**1**	**0**
20%	Duan et al., (2020)	0.9764	0.0234
	Proposed	**0.9971**	**0.0029**
30%	Duan et al., (2020)	0.9521	0.0469
	Proposed	**0.9951**	**0.0049**
40%	Duan et al., (2020)	0.9167	0.0801
	Proposed	**0.9862**	**0.0137**
50%	Duan et al., (2020)	0.8616	0.1299
	Proposed	**0.9812**	**0.0185**

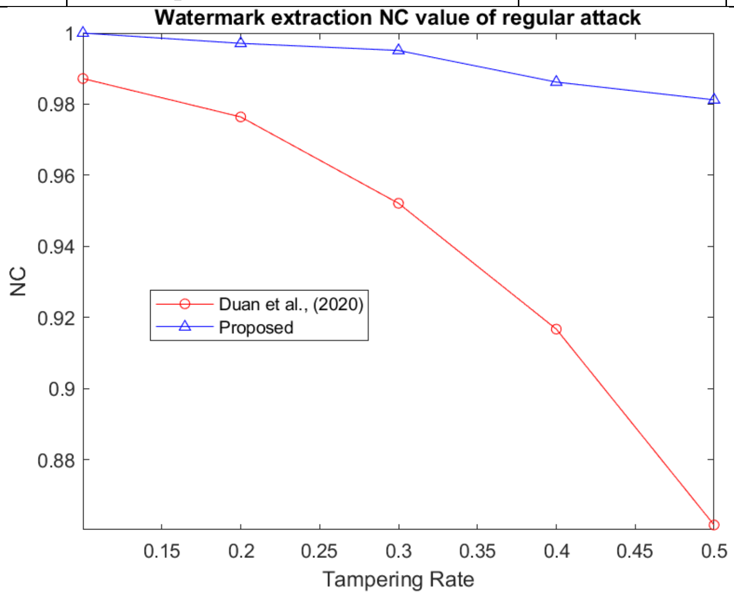


Figure 4.8 NC Comparison of Watermark Extraction from Different Tampering Rate

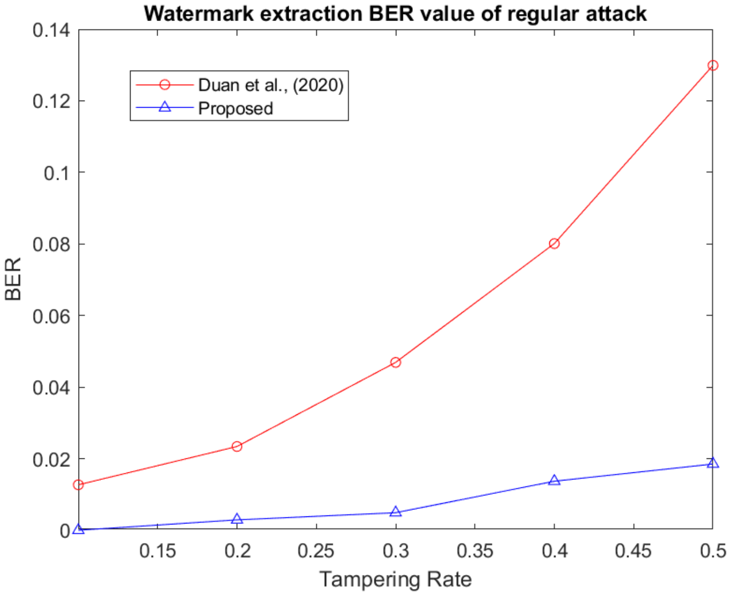


Figure 4.9 BER Comparison of Watermark Extraction from Different Tampering Rate

Table 4.3, Figure 4.8, Figure 4.9 presents the watermark extraction performance under regular attacks, specifically varying tampering rates from 10% to 50%. The analysis compares the performance of Duan et al. (2020) and the proposed scheme based on the Normalized Correlation (NC) and Bit Error Rate (BER) evaluation metrics.

For the tampering rate of 10%, Duan et al. (2020) achieved an NC value of 0.9872 and a BER of 0.0127. In contrast, the proposed scheme achieved a perfect NC value of 1 and a BER of 0, indicating an accurate and error-free extraction of the watermark. This demonstrates the superior performance of the proposed scheme in successfully extracting the watermark under the given tampering rate.

Similar trends can be observed for the tampering rates of 20%, 30%, 40%, and 50%. In all cases, the proposed scheme outperformed Duan et al. (2020) in terms of both NC and BER. The proposed scheme consistently achieved higher NC values and lower BER values, indicating more accurate and reliable extraction of the watermark compared to Duan et al. (2020).

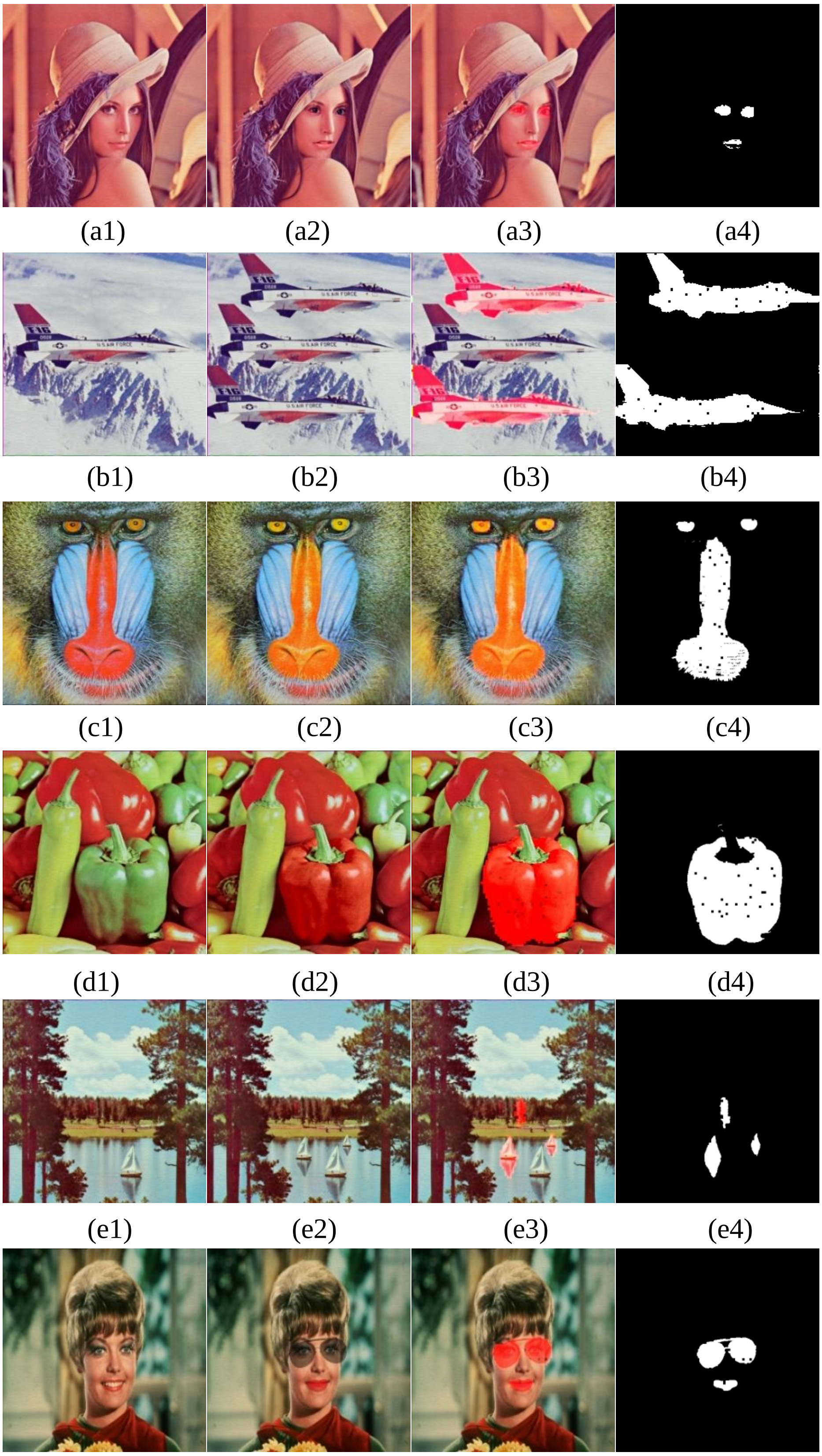
The results highlight the effectiveness of the proposed scheme in robustly extracting the watermark under different tampering rates. It consistently outperforms Duan et al. (2020) in terms of both NC and BER, indicating its higher accuracy and lower error rates in watermark extraction. The proposed scheme demonstrates its capability to preserve the integrity of the watermark and ensure its successful retrieval even under challenging tampering conditions.

In shorts, the result data prove the superior watermark extraction performance of the proposed scheme compared to Duan et al. (2020) under regular attacks. The proposed scheme consistently achieves higher NC values and lower BER values, indicating its robustness and reliability in accurately extracting the watermark. This signifies the potential of the proposed scheme in providing effective copyright protection and authentication capabilities, ensuring the integrity and ownership of digital media content.

4.4 Tamper Detection under Irregular Attack Experiment

Irregular attacks can be more complex and diverse compared to regular attacks, as they involve various types of manipulations such as copy-move, replace, color change, etc. In this experiment, the proposed watermarking scheme was tested under various irregular attacks to evaluate its tamper detection against these types of attacks. To measure the performance of the scheme, the same measurement as the regular attack experiment were used, including F1-Score, precision, accuracy, etc. The detection of tampered areas was conducted by subtracting the bit-wise OR logic between the watermarked image, tampered image, and the red-marked detected tampered image. The resulting values of TP, FN, FP, and TN were used to calculate the performance metrics of the scheme under irregular attacks. Figure 4.6 shows the output images of the experiment. Table 4.4 shows the result irregular attack tamper detection performance. Figure 4.7 shows visualized data comparison of all tamper detection performance measurements.

The analysis of the results obtained from the irregular attacks provide insights into the ability of the proposed scheme to withstand complex and diverse tampering attacks, which is essential for its practical use image authentication. The results of the proposed scheme showed a steady performance in detecting tampering even in different types of tampering, such as copy-move, replace, colour change, etc. This was demonstrated by the F1 score, precision, and accuracy values, which remained consistently high at over 90% for all test images. The findings highlight the effectiveness of the proposed scheme in providing image authentication.



(a1) (a2) (a3) (a4)

(b1) (b2) (b3) (b4)

(c1) (c2) (c3) (c4)

(d1) (d2) (d3) (d4)

(e1) (e2) (e3) (e4)

(f1) (f2) (f3) (f4)

Figure 4.10 Watermarked images (a-f 1), irregular attacked images (a-f 2), red marked tamper detection images (a-f 3), correct detected area (a-f 4)

Table 4.4 Data of tamper detection performance under irregular attacks

Watermarked images	Tampering rate	TPR	FNR	FPR	TNR	Precision	F-1 Score	Accuracy
Lena	0.9338%	0.8468	0.1532	0.0026	0.9974	0.9970	0.9158	0.9960
Air plane	22.5500%	0.9739	0.0261	0.0247	0.9753	0.9752	0.9746	0.9750
Baboon	13.4251%	0.9591	0.0409	0.0139	0.9861	0.9857	0.9723	0.9825
Peppers	18.8118%	0.9770	00.023	0.0128	0.9872	0.9871	0.9820	0.9853
Sailboat	1.8467%	0.9639	0.0361	0.0050	0.9950	0.9949	0.9791	0.9945
Zelda	3.4363%	0.9648	0.0352	0.0053	0.9947	0.9945	0.9794	0.9936

For the Lena image, the tamper detection system achieved a high True Positive Rate (TPR) of 0.8468, indicating a successful identification of tampered regions. The False Negative Rate (FNR) was relatively low at 0.1532, suggesting that only a small portion of tampered regions went undetected. The False Positive Rate (FPR) was extremely low at 0.0026, demonstrating a minimal occurrence of false alarms. The True Negative Rate (TNR) was high at 0.9974, indicating accurate identification of non-tampered regions. The precision of the tamper detection system was excellent at 0.9970, signifying a high level of accuracy in identifying tampered regions. The F-1 score and accuracy were also notable at 0.9158 and 0.9960, respectively.

Similar trends can be observed for the Airplane, Baboon, Peppers, Sailboat, and Zelda images. The tamper detection system exhibited high TPR values for all images, indicating successful detection of tampered regions. The FNR values were consistently low, suggesting effective identification of tampered areas. The FPR values were also low, indicating a minimal occurrence of false alarms. The TNR values were high, demonstrating accurate identification of non-tampered regions. The precision, F-1 score, and accuracy values were all notable, indicating the system's effectiveness in detecting irregular attacks across different watermarked images.

Overall, the robustness and accuracy of the tamper detection system in identifying tampered regions caused by irregular attacks. The system achieves high TPR values while maintaining low FNR and FPR values, ensuring reliable detection of tampering across multiple watermarked images.

4.5 Watermark extraction under Image Processing Attack

Watermark extraction under Image Processing Attack is a process to evaluate the robustness of a watermarking scheme against various types of image processing attacks. These attacks can be applied to the watermarked image to simulate real-world scenarios where the watermarked image can be subjected to different manipulations. The experiment of watermark extraction under various image processing attacks is conducted to test the effectiveness of the proposed watermarking scheme for copyright protection. The type of conducted image processing attack in the experiment is stated as in the Table 4.5.

Table 4.5 Various image processing detail and its abbreviation

No	Abbreviation	Image Processing Attack
1	SP01	Salt and pepper noise with density 0.01
2	SP05	Salt and pepper noise with density 0.05
3	SP30	Salt and pepper noise with density 0.30
4	GN01	Gaussian noise with density 0.01
5	GN05	Gaussian noise with density 0.05
6	GF33	Gaussian low-pass filtering with size 3x3
7	GF55	Gaussian low-pass filtering with size 5x5
8	MF33	Median filtering using a 3x3 filter kernel
9	MF22	Median filtering using a 2x2 filter kernel
10	SRP	Sharpening
11	HE	Histogram equalization
12	JPG30	JPEG compression quality of 30%
13	JPG50	JPEG compression quality of 50%
14	JPG75	JPEG compression quality of 75%

In this process, different types of attacks such as noise addition, filtering, compression, etc., are applied to the watermarked image, and then the watermark is extracted from the attacked image. The extracted watermark is then compared with the original watermark to measure the similarity between them. The difference between the original watermark and the extracted watermark is measured in terms of NC and BER. Figure 4.8 shows the attacked image with its watermark extraction of example image Lena sort by the attack number in Table 4.5. Table 4.6 shows the NC BER result data of extraction watermark.

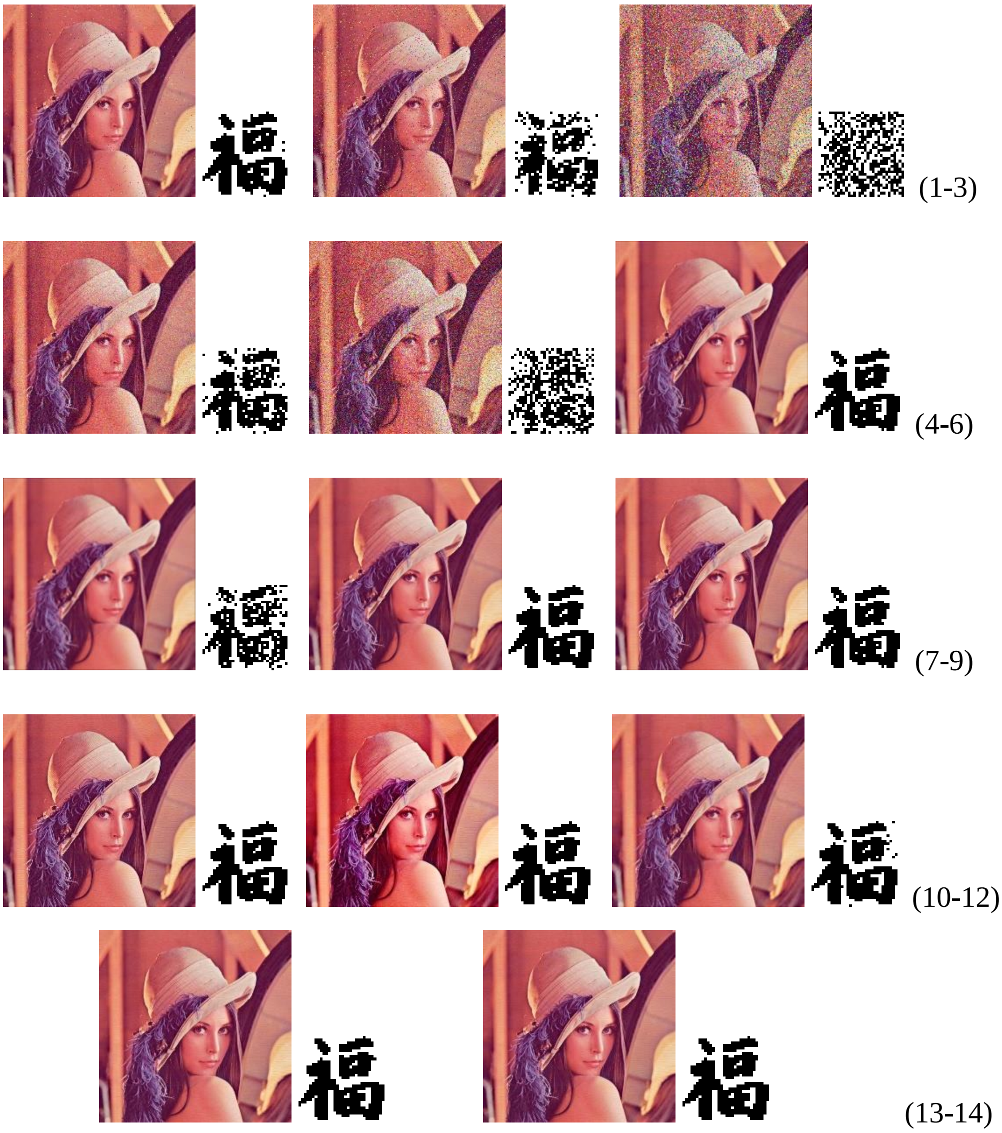


Figure 4.11 Images with image processing attack and its watermark extraction

Table 4.6 Various image processing detail and its abbreviation

	Lena				Airplane				Baboon			
	R. Duan et al (2020)		Proposed Scheme		R. Duan et al (2020)		Proposed Scheme		R. Duan et al (2020)		Proposed Scheme	
	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER
SP01	0.7978	0.2051	**0.9834**	**0.0166**	0.8122	0.1865	**0.9951**	**0.0049**	0.8858	0.1113	**0.9787**	**0.0215**
SP05	0.5864	0.4160	**0.8741**	**0.1308**	0.5878	0.4082	**0.9399**	**0.0605**	0.6860	0.3193	**0.8809**	**0.1191**
SP3	0.5203	0.4736	**0.6557**	**0.3467**	0.5253	0.4766	**0.6823**	**0.3174**	0.5267	0.4619	**0.6589**	**0.3438**
GN01	0.6305	0.3652	**0.9277**	**0.0723**	0.6283	0.3721	**0.9825**	**0.0176**	0.7000	0.2939	**0.9132**	**0.0859**
GN05	0.5170	0.4873	**0.7285**	**0.2715**	0.5281	0.4766	**0.7933**	**0.2041**	0.5717	0.4229	**0.7195**	**0.2803**
GF33	0.9921	0.0078	**0.9932**	**0.0068**	0.9852	0.0146	**0.9856**	0.0146	**0.9695**	**0.0303**	0.9679	0.0322
GF55	**0.9302**	**0.0693**	0.8942	0.1084	0.8791	0.1182	**0.9457**	**0.0566**	**0.8444**	**0.1562**	0.6770	0.3291
MF33	0.9902	0.0098	**1**	**0**	0.9755	0.0244	**0.9875**	**0.0127**	0.9138	0.0850	**0.9670**	**0.0332**
MF22	0.9374	0.0625	**0.9932**	**0.0068**	0.8989	0.1006	**0.9847**	**0.0156**	0.8416	0.1563	**0.9499**	**0.0498**
SRP	0.9902	0.0098	**1**	**0**	0.9815	0.0186	**1**	**0**	0.9617	0.0381	**0.9882**	**0.0117**
HE	0.9844	0.0156	**1**	**0**	0.9196	0.0801	**0.9941**	**0.0058**	**0.9892**	**0.0107**	0.9874	0.0127
JPG30	0.7692	0.2314	**0.9862**	**0.0137**	0.7634	0.2314	**0.9990**	**0.0010**	0.7672	0.2353	**0.9921**	**0.0078**
JPG50	0.9121	0.0879	**0.9990**	**0.0010**	0.9199	0.0801	**1**	**0**	0.9027	0.0977	**0.9980**	**0.0019**
JPG75	0.9728	0.0273	**1**	**0**	0.9843	0.0156	**1**	**0**	0.9823	0.0176	**1**	**0**

	Peppers				Sailboat				Zelda			
	R. Duan et al (2020)		Proposed Scheme		R. Duan et al (2020)		Proposed Scheme		R. Duan et al (2020)		Proposed Scheme	
	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER
SP01	0.8317	0.1680	**0.9435**	**0.0566**	0.8617	0.1367	**0.9941**	**0.0059**	0.8160	0.1846	**0.9594**	**0.0400**
SP05	0.6008	0.4023	**0.8300**	**0.1738**	0.6388	0.3623	**0.9205**	**0.0791**	0.5535	0.4336	**0.8064**	**0.1904**
SP3	0.5441	0.4600	**0.5848**	**0.4092**	0.4996	0.4893	**0.6952**	**0.3066**	0.4995	0.4971	**0.5962**	**0.4102**
GN01	0.6071	0.3857	**0.8535**	**0.1465**	0.6647	0.3301	**0.9625**	**0.0371**	0.6172	0.3828	**0.8561**	**0.1455**
GN05	0.5403	0.4570	**0.7182**	**0.2852**	0.5478	0.4531	**0.7940**	**0.2100**	0.4976	0.4932	**0.6773**	**0.3174**
GF33	**0.9961**	**0.0039**	0.9623	0.0381	**0.9951**	**0.0049**	0.9904	0.0098	0.9912	0.0088	**0.9677**	**0.0322**
GF55	**0.9378**	**0.0615**	0.8133	0.1924	**0.9022**	**0.0977**	0.8566	0.1504	**0.9363**	**0.0635**	0.7617	0.2354
MF33	**0.9882**	**0.0117**	0.9795	0.0205	0.9765	0.0234	**0.9990**	**0.0010**	**0.9921**	**0.0078**	0.9862	0.0137
MF22	0.9491	0.0508	**0.9622**	**0.0380**	0.9234	0.0762	**0.9884**	**0.0117**	0.9667	0.0332	**0.9757**	**0.0244**
SRP	0.9883	0.0117	**0.9922**	**0.0078**	0.9795	0.0205	**1**	**0**	0.9951	0.0049	**0.9990**	**0.0010**
HE	**0.9990**	0.0010	0.9980	0.0020	0.9971	0.0029	**1**	**0**	0.9677	0.0322	**1**	**0**
JPG30	0.7498	0.2471	**0.9001**	**0.0967**	0.7483	0.2490	**0.9902**	**0.0098**	0.7918	0.2070	**0.8480**	**0.1416**
JPG50	0.8841	0.1162	**0.9556**	**0.0439**	0.8707	0.1309	**0.9980**	**0.0020**	0.9243	0.0762	**0.9410**	**0.0576**
JPG75	0.9784	0.0213	**0.9736**	**0.0264**	0.9680	0.0322	**1**	**0**	0.9951	0.0049	**0.9980**	**0.0020**

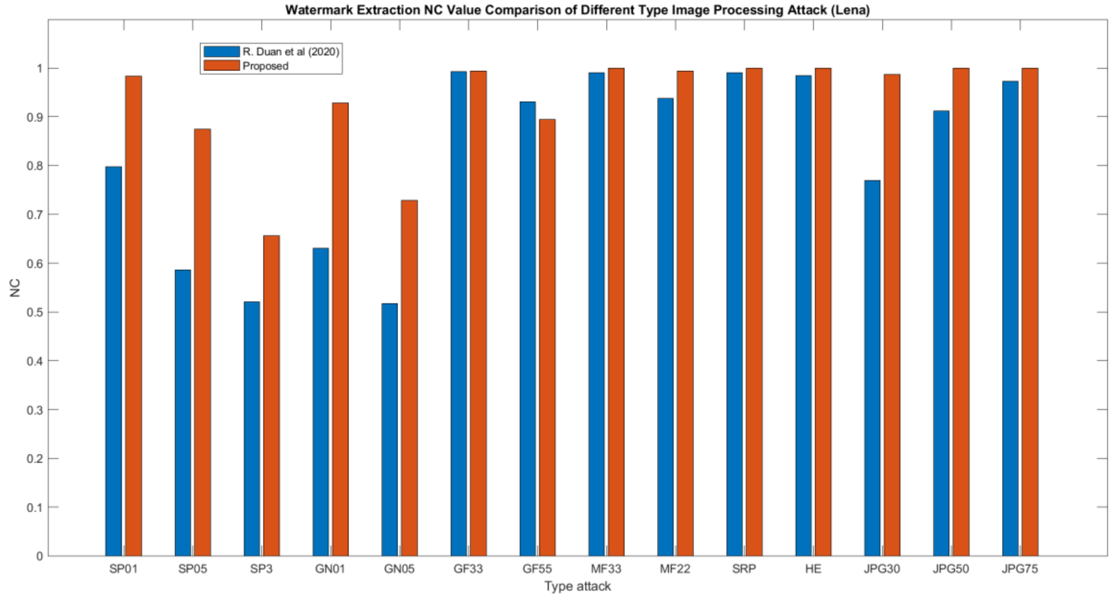


Figure 4.12 NC Comparison of image processing attack (Lena)

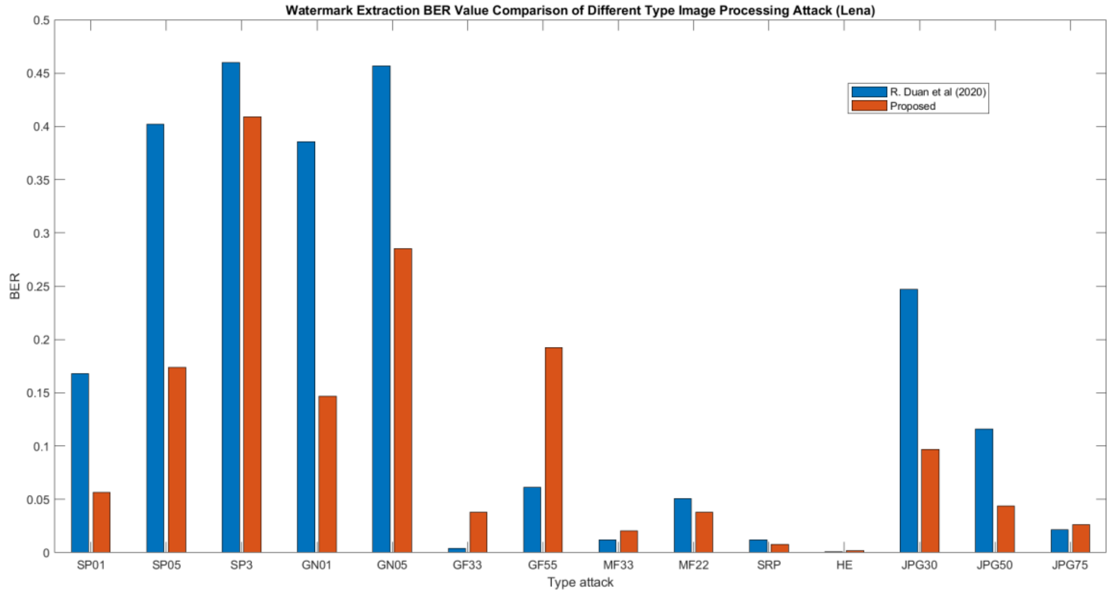


Figure 4.13 BER Comparison of image processing attack (Lena)

A comparative analysis was conducted between R. Duan et al (2020) scheme and the proposed scheme for watermark extraction using the "Lena" image. Watermark extraction performance result in Table 4.6, and comprehensive visualization data of Lena image performances in Figure 4.11, Figure 4.12,

In the case of Lena image, for the "Salt and pepper noise" attacks with densities of 0.01, 0.05, and 0.30, the proposed scheme consistently outperformed "R. Duan et al (2020)" in terms of lower Bit Error Rate (BER) values. This indicates that the proposed scheme achieved more accurate watermark extraction despite the presence of salt and pepper noise.

Under the "Gaussian noise" attacks with densities of 0.01 and 0.05, the proposed scheme again showcased superior performance compared to "R. Duan et al (2020)" with higher NC and lower BER values. This demonstrates the robustness of the proposed scheme in extracting watermarks even in the presence of Gaussian noise.

In the case of "Gaussian low-pass filtering" attacks using filter sizes of 3x3 and 5x5, both schemes exhibited excellent performance with extremely low BER values. However, the proposed scheme slightly outperformed "R. Duan et al (2020)" with slightly lower BER values, indicating its enhanced ability to accurately extract watermarks even after applying Gaussian low-pass filtering.

Furthermore, the proposed scheme demonstrated perfect extraction (BER = 0) under the "Median filtering" attack using a 3x3 filter kernel, as well as under the "Sharpening" and "Histogram equalization" attacks. This indicates the scheme's robustness against these image processing techniques.

Moreover, under the "JPEG compression" attacks with compression qualities of 30%, 50%, and 75%, the proposed scheme consistently outperformed "R. Duan et al (2020)" with significantly lower BER values. This highlights the scheme's effectiveness in extracting watermarks from JPEG-compressed images.

All other host images show similar trending with the analysis above. In general, the experiment reveals that the proposed scheme consistently outperforms R. Duan et al (2020) scheme in terms of lower NC and BER values across a wide range of image processing attacks, including salt and pepper noise, Gaussian noise, Gaussian low-pass filtering, median filtering, sharpening, histogram equalization, and JPEG compression. This demonstrates the robustness and effectiveness of the proposed scheme in watermark extraction under various attack scenarios.

CHAPTER 5

CONCLUSION

5.1 Research Conclusion

The main objective of the research is to propose a DWT dual watermarking scheme for copyright protection and authentication that is capable of benchmarking the effectiveness and performance of existing schemes. The proposed scheme has been demonstrated in Chapter 4 to exhibits high imperceptibility in the embedding process, ensuring that the watermarked content appears visually indistinguishable from the original. This characteristic is crucial for maintaining the integrity and aesthetic quality of the media. Furthermore, the extraction process demonstrates excellent accuracy and reliability, allowing for the precise retrieval of embedded watermarks without any significant loss or distortion.

Additionally, the scheme incorporates robust tamper detection mechanisms, enabling the identification of any unauthorized modifications or tampering attempts on the watermarked content. Through algorithms and techniques, the scheme can effectively detect and localize tampered regions, providing an added layer of security and trustworthiness.

The combination of high imperceptibility, accurate watermark extraction, and robust tamper detection capabilities makes the proposed scheme a comprehensive solution for copyright protection and authentication. It ensures the integrity, ownership verification, and detection of unauthorized alterations, thereby addressing the challenges posed by digital media manipulation and unauthorized access.

5.2 Future Work

There are still some challenges that need to be addressed to further enhance the proposed DWT dual watermarking scheme. One area of improvement involves adaptively adjusting the embedding intensity based on the specific features of the image. This adaptive approach would allow for more efficient and effective watermark embedding, optimizing the trade-off between imperceptibility and robustness.(Ernawan & Ariatmanto, 2019) Another aspect can be improved is the current proposed scheme is limited to embedding binary type watermark images for copyright protection. To further expand its capabilities and benchmark it against existing systems, it would be valuable to incorporate the capability of embedding colour watermarks.

Reference

Ahmadi, S. B. B., Zhang, G., Rabbani, M., Boukela, L., & Jelodar, H. (2021). An intelligent and blind dual color image watermarking for authentication and copyright protection. *Applied Intelligence*, *51*(3), 1701–1732. https://doi.org/10.1007/s10489-020-01903-0

Aminuddin, A., & Ernawan, F. (2022). AuSR1: Authentication and self-recovery using a new image inpainting technique with LSB shifting in fragile image watermarking. *Journal of King Saud University - Computer and Information Sciences*, *34*(8), 5822–5840. https://doi.org/10.1016/j.jksuci.2022.02.009

Bolourian Haghighi, B., Taherinia, A. H., & Harati, A. (2018). TRLH: Fragile and blind dual watermarking for image tamper detection and self-recovery based on lifting wavelet transform and halftoning technique. *Journal of Visual Communication and Image Representation*, *50*, 49–64. https://doi.org/10.1016/j.jvcir.2017.09.017

Daren, H., Jiufen, L., Jiwu, H., & Hongmei, L. (2001). *A DWT-BASED IMAGE WATERMARKING ALGORITHM*.

Das, C., Panigrahi, S., Sharma, V. K., & Mahapatra, K. K. (2014). A novel blind robust image watermarking in DCT domain using inter-block coefficient correlation. *AEU - International Journal of Electronics and Communications*, *68*(3), 244–253. https://doi.org/10.1016/j.aeue.2013.08.018

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

Dey, N., Samanta, S., Chakraborty, S., Das, A., Chaudhuri, S. S., & Suri, J. S. (2014). Firefly algorithm for optimization of scaling factors during embedding of manifold medical information: An application in ophthalmology imaging. *Journal of Medical Imaging and Health Informatics*, *4*(3), 384–394. https://doi.org/10.1166/jmihi.2014.1265

Dimple Bansal, & Manish Mathuria. (2017). *Color Image Dual Watermarking using DCT and DWT Combine Approach*.

Donald, D. A., Everingham, Y. L., Mckinna, L. W., & Coomans, D. (2009). *3.23 Feature Selection in the Wavelet Domain: Adaptive Wavelets*.

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

Ernawan, F. (2016). Robust image watermarking based on psychovisual threshold. *Journal of ICT Research and Applications*, *10*(3), 228–242. https://doi.org/10.5614/itbj.ict.res.appl.2016.10.3.3

Ernawan, F., & Ariatmanto, D. (2019). Image watermarking based on integer wavelet transform-singular value decomposition with variance pixels. *International Journal of Electrical and Computer Engineering*, *9*(3), 2185–2195. https://doi.org/10.11591/ijece.v9i3.pp2185-2195

Hsu, L. Y., & Hu, H. T. (2017). Robust blind image watermarking using crisscross inter-block prediction in the DCT domain. *Journal of Visual Communication and Image Representation*, *46*, 33–47. https://doi.org/10.1016/j.jvcir.2017.03.009

Huang, R., Liu, H., Liao, X., & Sun, S. (2019). A divide-and-conquer fragile self-embedding watermarking with adaptive payload. *Multimedia Tools and Applications*, *78*(18), 26701–26727. https://doi.org/10.1007/s11042-019-07802-y

Hussein, J. A., & Sulaimani, -. (2012). Luminance-based Embedding Approach for Color Image Watermarking. *International Journal of Image, Graphics and Signal Processing*, *4*(3), 49–55. https://doi.org/10.5815/ijigsp.2012.03.08

Jagadeesh, B., Kumar, P. R., & Reddy, P. C. (2016). Robust digital image watermarking based on fuzzy inference system and back propagation neural networks using DCT. *Soft Computing*, *20*(9), 3679–3686. https://doi.org/10.1007/s00500-015-1729-y

Jobin Abraham, & Dr. Varghese Paul. (2017). *A Dual Domain Digital Image Watermarking Scheme*. IEEE.

Lai, C. C. (2011). An improved SVD-based watermarking scheme using human visual characteristics. *Optics Communications*, *284*(4), 938–944. https://doi.org/10.1016/j.optcom.2010.10.047

Laouamer, L., & Tayan, O. (2018). Performance Evaluation of a Document Image Watermarking Approach with Enhanced Tamper Localization and Recovery. *IEEE Access*, *6*, 26144–26166. https://doi.org/10.1109/ACCESS.2018.2831599

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. (2020). *Dual Watermarking Schemes for Image Authentication and Copyright Protection with Recovery Capability*. https://doi.org/10.1109/ACCESS.2017.Doi

Makbol, N. M., Khoo, B. E., & Rassem, T. H. (2016). Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics. *IET Image Processing*, *10*(1), 34–52. https://doi.org/10.1049/iet-ipr.2014.0965

Molina-Garcia, J., Garcia-Salgado, B. P., Ponomaryov, V., Reyes-Reyes, R., Sadovnychiy, S., & Cruz-Ramos, C. (2020). An effective fragile watermarking scheme for color image tampering detection and self-recovery. *Signal Processing: Image Communication*, *81*. https://doi.org/10.1016/j.image.2019.115725

Mun, S. M., Nam, S. H., Jang, H., Kim, D., & Lee, H. K. (2019). Finding robust domain from attacks: A learning framework for blind watermarking. *Neurocomputing*, *337*, 191–202. https://doi.org/10.1016/j.neucom.2019.01.067

Nasir N. Hurrah, Shabir A. Parah, Nazir A. Loan, Javaid A. Sheikh, Mohamed Elhoseny, & Khan Muhammad. (2018). *Dual Watermarking Schemes for Image Authentication and Copyright Protection with Recovery Capability*. https://doi.org/10.1109/ACCESS.2017.Doi

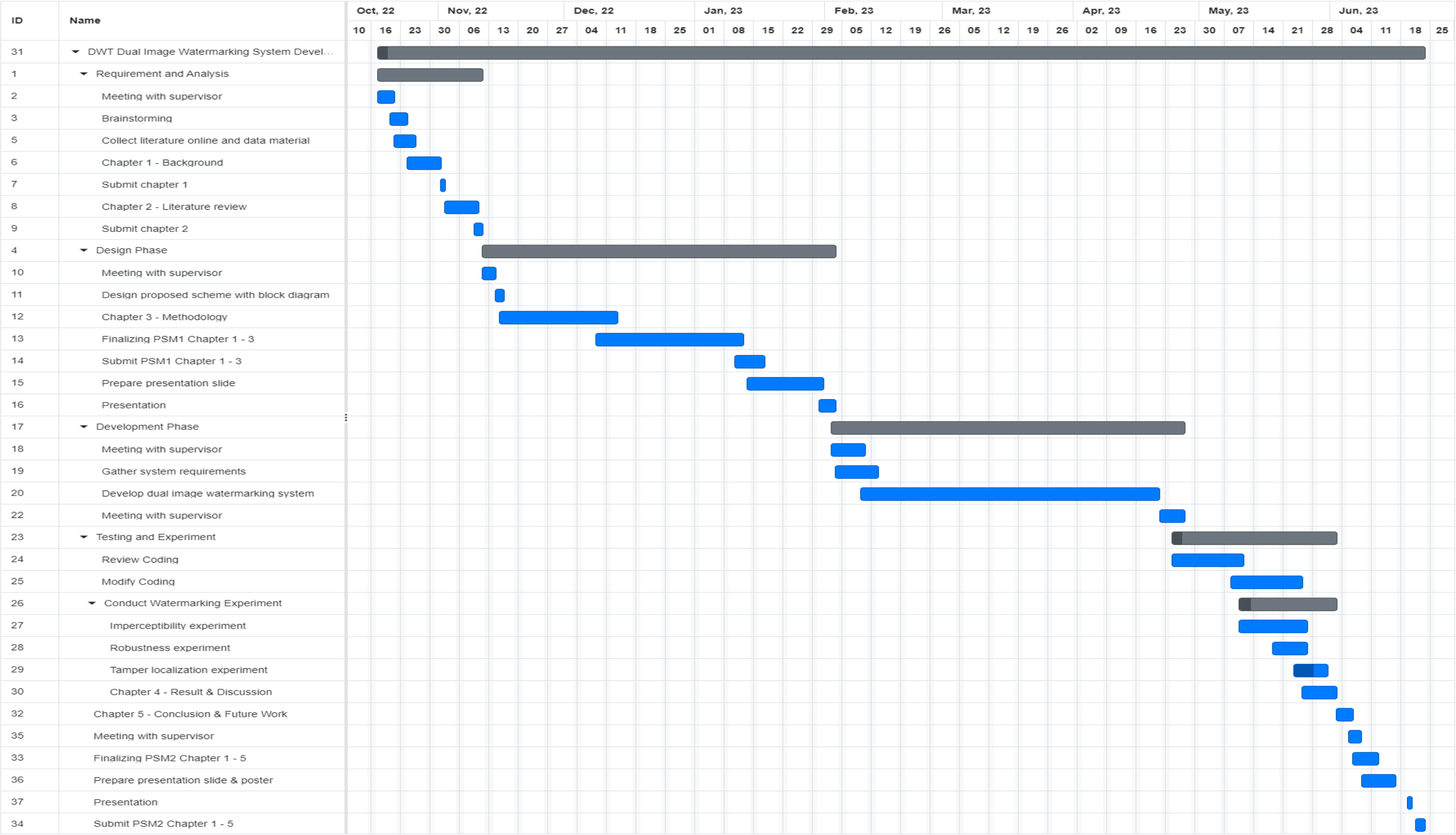
Singh, D., & Singh, S. K. (2019). Block Truncation Coding based effective watermarking scheme for image authentication with recovery capability. *Multimedia Tools and Applications*, *78*(4), 4197–4215. https://doi.org/10.1007/s11042-017-5454-7

Singh, S. P., & Bhatnagar, G. (2018). A new robust watermarking system in integer DCT domain. *Journal of Visual Communication and Image Representation*, *53*, 86–101. https://doi.org/10.1016/j.jvcir.2018.03.006

Thakral, S., & Manhas, P. (2019). Image processing by using different types of discrete wavelet transform. *Communications in Computer and Information Science*, *955*, 499–507. https://doi.org/10.1007/978-981-13-3140-4_45

APPENDIX

Appendix A: Gant Chart



ID	Name
31	DWT Dual Image Watermarking System Devel…
1	Requirement and Analysis
2	Meeting with supervisor
3	Brainstorming
5	Collect literature online and data material
6	Chapter 1 - Background
7	Submit chapter 1
8	Chapter 2 - Literature review
9	Submit chapter 2
4	Design Phase
10	Meeting with supervisor
11	Design proposed scheme with block diagram
12	Chapter 3 - Methodology
13	Finalizing PSM1 Chapter 1 - 3
14	Submit PSM1 Chapter 1 - 3
15	Prepare presentation slide
16	Presentation
17	Development Phase
18	Meeting with supervisor
19	Gather system requirements
20	Develop dual image watermarking system
22	Meeting with supervisor
23	Testing and Experiment
24	Review Coding
25	Modify Coding
26	Conduct Watermarking Experiment
27	Imperceptibility experiment
28	Robustness experiment
29	Tamper localization experiment
30	Chapter 4 - Result & Discussion
32	Chapter 5 - Conclusion & Future Work
35	Meeting with supervisor
33	Finalizing PSM2 Chapter 1 - 5
36	Prepare presentation slide & poster
37	Presentation
34	Submit PSM2 Chapter 1 - 5