

SECURE AND EFFECTIVE IMAGE
AUTHENTICATION AND COPYRIGHT
PROTECTION USING INTEGER
WAVELET TRANSFORM

NG CHING ONN

Bachelor Degree

UNIVERSITI MALAYSIA PAHANG

UNIVERSITI MALAYSIA PAHANG

DECLARATION OF THESIS AND COPYRIGHT

Author's Full Name : NG CHING ONN

Date of Birth :

Title : SECURE AND EFFECTIVE IMAGE AUTHENTICATION
AND COPYRIGHT PROTECTION USING INTEGER
WAVELET TRANSFORM

Academic Session : SEM 2 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)

New IC/Passport Number

Date: 6/6/2023

Associate Prof. Ts. Dr. Ferda Ernawan

Name of Supervisor

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 NG CHING ONN
Thesis Title: SECURE AND EFFECTIVE IMAGE AUTHENTICATION AND
COPYRIGHT PROTECTION USING INTEGER WAVELET
TRANSFORM

Reasons (i)

 (ii)

 (iii)

Thank you.

Yours faithfully,

(Supervisor's Signature)

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

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



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 : ASSOCIATE PROF. TS. DR. FERDA ERNAWAN

Position : Senior Lecturer

Date : 10/07/2023

(Co-supervisor's Signature)

Full Name :

Position :

Date :



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 : NG CHING ONN

ID Number : CD20139

Date : 6/6/2023

SECURE AND EFFECTIVE IMAGE AUTHENTICATION
AND COPYRIGHT PROTECTION USING
INTEGER WAVELET TRANSFORM

NG CHING ONN
CD20139

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

Faculty of Computing
UNIVERSITI MALAYSIA PAHANG

JUNE 2023

ACKNOWLEDGEMENTS

I am profoundly grateful to God for guiding me through my research and providing me the resources I needed to finish it. My sincere appreciation goes out to Dr. Ferda Ernawan, who served as my advisor, for his immense encouragement, tolerance, and valuable guidance throughout this study. Without his invaluable encouragement and guidance, I would not have been able to start this journey.

Furthermore, Jabatan Kemajuan Orang Asli's generous funding, which covered my study-related expenses and more, is what made this project possible. I appreciate my friends' encouragement, criticism, and moral support during late-night sessions. I also want to express my sincere gratitude to my family, especially to my grandmother and parents, for their unwavering belief in me. Throughout this endeavour, their inspiration and assistance kept me motivated and positive.

I also want to acknowledge the University's librarians and study participants for their influence and motivation. Finally, I would like to extend my gratitude to fellow researcher that contributed their study on similar topics.

ABSTRAK

Dengan penggunaan internet dan teknologi komunikasi digital yang meluas, data multimedia mungkin terdedah kepada cetak rompak kerana pengguna yang tidak berhemah boleh mengubah data multimedia seperti imej dengan mudah. Untuk meningkatkan keteguhan dan keselamatan imej, sistem tera air dwi diperkenalkan dengan menggabungkan berbilang tera air ke dalam satu kandungan. Penggunaan tera air dikatakan boleh meningkatkan keupayaan untuk mengesan dan mengenal pasti pemilik hak cipta sekiranya berlaku penggunaan yang tidak dibenarkan atau sebarang perubahan pada kandungan. Dalam kajian ini, IWT dan SVD berdasarkan ciri-ciri visual manusia dicadangkan, untuk membenamkan tera air dalam imej, menjadikannya lebih tahan terhadap serangan di samping tidak mengurangkan kualiti imej tersebut. Kaedah ini membantu memastikan imej digital skala kelabu dilindungi oleh hak cipta dan boleh disahkan jika terdapat gangguan. Pelbagai serangan geometri, mampatan, dan pemprosesan imej digunakan untuk menguji keberkesanan pendekatan yang dicadangkan. Oleh itu, keputusan ujian dinilai kepada sistem tera air dwi yang lain.

ABSTRACT

Widespread usage of the internet and digital communication technologies, multimedia data may be vulnerable to piracy as unauthorized users can easily alter multimedia data such as image. To increase the robustness and security of images, a dual watermarking system were introduced by combining multiple watermarks into a single content. The use of multiple watermarks enhances the ability to detect and identify the copyright owner in the case of unauthorized use or any altering on the content. In this study, IWT and SVD based on human visual characteristics are proposed, to embed the watermark in the image, making it more resistant to attacks while lower the distortion on image quality. The method helps to ensure that RGB supported digital images are protected by copyright and can be authenticated if there is any tampering. Various geometrical, compression, and image processing attacks are used to test the effectiveness of the proposed approach. Hence, the test results are compared to other dual watermarking systems.

TABLE OF CONTENT

DECLARATION	
TITLE PAGE	
ACKNOWLEDGEMENTS	ii
ABSTRAK	iii
ABSTRACT	iv
TABLE OF CONTENT	v
LIST OF TABLES	viii
LIST OF FIGURES	ix
LIST OF ABBREVIATIONS	xi
LIST OF ABBREVIATIONS (attacks)	xii
CHAPTER 1 INTRODUCTION	14
1.1 Introduction	14
1.2 Problem Statement	15
1.3 Objective	16
1.4 Scope	16
1.5 Thesis Organization	17
CHAPTER 2 LITERATURE REVIEW	18
2.1 Introduction	18
2.2 Overview of Existing Dual Watermarking Scheme	18
2.3 Embedding Components	19
2.3.1 Integer Wavelet Transform	19

2.3.2	Human Visual Characteristic	19
2.3.3	Singular Value Decomposition	20
2.4	Analysis/Comparison of Existing Scheme	21
2.5	Summary	24
CHAPTER 3 METHODOLOGY		25
3.1	Introduction	25
3.2	Research Requirements	26
3.3	Research Methodology	27
3.3.1	Literature Review	27
3.3.2	Identification of Research Problems	27
3.3.3	Development of Potential Solution	27
3.3.4	Analysis of Empirical Result	28
3.3.5	Documentation	28
3.4	Proposed Dual Watermarking Approach	29
3.4.1	Algorithm of Robust Watermark Embedding Process	30
3.4.2	Algorithm of Robust Watermark Embedding Process	31
3.4.3	Algorithm of Robust Watermark Extracting Process	32
3.4.4	Algorithm of Fragile Tamper Localization Process	33
3.5	Evaluation of the Watermarked Image	35
3.5.1	Imperceptibility, Robustness, Computational Time Measurements	35
3.5.2	Abbreviation of Attacks	36
3.5.3	Tamper Localization	36
3.5.4	F1-score	37
3.6	Summary	38
3.7	Gantt Chart	39

CHAPTER 4 RESULTS AND DISCUSSION	40
4.1 Introduction	40
4.2 Imperceptibility Performance for Different Watermark Images	41
4.2.1 Imperceptibility Comparison	45
4.3 Robustness Performance after Dual Watermarking using Proposed Scheme	46
4.3.1 NC and BER Values for Proposed Scheme	47
4.3.2 Robustness Comparison of NC and BER Values for Proposed Scheme	50
4.3.3 Extracted Watermark of Proposed Scheme after Irregular Attack Combined with Image Processing Attacks	54
4.3.4 NC and BER Values for Proposed Scheme	58
4.4 Tamper Localization	60
4.4.1 Tamper Localization Result	61
4.4.2 Tamper Localization Comparison	64
CHAPTER 5 CONCLUSION	66
5.1 Introduction	66
5.2 Research Constraint	67
5.3 Future work	68
REFERENCES	70
APPENDIX A	72

LIST OF TABLES

<i>Table 1: Analysis breakdown on existing scheme.</i>	21
<i>Table 2: List of research requirements.</i>	26
<i>Table 3: PSNR, SSIM, ARE value after Watermark logo embedding.</i>	41
<i>Table 4: PSNR, SSIM, ARE value after watermark logo and authentication bit embedding.</i>	41
<i>Table 5: Imperceptibility comparison between Lusia's, Kamili's and proposed scheme.</i>	45
<i>Table 6: Visualization of host image under various attacks, including NC and BER values.</i>	47
<i>Table 7: NC and BER values comparison between Duan's scheme and proposed scheme under various attacks.</i>	50
<i>Table 8: Visualization of host image and watermark logo after irregular tamper attack combined various image processing attacks, including NC and BER values.</i>	54
<i>Table 9: NC and BER values of watermarked images after irregular attack combined with image processing attacks.</i>	58
<i>Table 10: Tamper localization result for 8 host images.</i>	61
<i>Table 11: Tamper localization parameters comparison of proposed scheme and (Duan et al., 2020)'s scheme.</i>	64

LIST OF FIGURES

<i>Figure 1: Block diagram of dual watermark embedding using IWT.</i>	29
<i>Figure 2: Block diagram of watermark logo embedding (first round embedding).</i>	30
<i>Figure 3: Block diagram of watermark logo embedding (second round embedding).</i>	31
<i>Figure 4: Block diagram of watermark extraction.</i>	32
<i>Figure 5: Block diagram of tamper localization extraction.</i>	33
<i>Figure 6: Timeline of PSM research.</i>	39
<i>Figure 7: Lena</i>	41
<i>Figure 8: Avion</i>	41
<i>Figure 9: Sailboat</i>	41
<i>Figure 10: Parrots</i>	41
<i>Figure 11: House</i>	41
<i>Figure 12: Lighthouse</i>	41
<i>Figure 13: Statue</i>	41
<i>Figure 14: Rafting</i>	41
<i>Figure 15: Bar graph visualization of PSNR values comparison after each embedding phase.</i>	42
<i>Figure 16: Bar graph visualization of SSIM values comparison after each embedding phase.</i>	43
<i>Figure 17: Bar graph visualization of ARE values comparison after each embedding phase.</i>	44
<i>Figure 18: Line graph of NC values for Duan's scheme and proposed scheme</i>	51
<i>Figure 19: Lena</i>	60
<i>Figure 20: Lena tampered</i>	60
<i>Figure 21: Avion</i>	60
<i>Figure 22: Avion tampered</i>	60
<i>Figure 23: Sailboat</i>	60
<i>Figure 24: Sailbaot tampered</i>	60
<i>Figure 25: Parrots</i>	60
<i>Figure 26: Parrots tampered</i>	60
<i>Figure 27: House</i>	60
<i>Figure 28: House tampered</i>	60
<i>Figure 29: Lighthouse</i>	60
<i>Figure 30: Lighthouse tampered</i>	60
<i>Figure 31: Statue</i>	60

<i>Figure 32: Statue tampered</i>	60
<i>Figure 33: Rafting</i>	60
<i>Figure 34: Rafting tampered</i>	60
<i>Figure 35: Host Image (Avion)</i>	64
<i>Figure 36: Tampered Image</i>	64
<i>Figure 37: Actual Tampered Region</i>	64
<i>Figure 38: Tamper Detected (Proposed)</i>	64
<i>Figure 39: Detected Region (Proposed)</i>	64
<i>Figure 40: False Positive Region (Proposed)</i>	64
<i>Figure 41: Tamper Detected (Duan et al., 2020)</i>	64
<i>Figure 42: Detected Region (Duan et al., 2020)</i>	64
<i>Figure 43: False Positive Region (Duan et al., 2020)</i>	64

LIST OF ABBREVIATIONS

ARE	Absolute Error Rate
BER	Bit Error Rate
DCT	Discrete Cosine Transform
DWT	Discrete Wavelet Transform
FN	False Negative
FNR	False Negative Rate
FP	False Positive
FPR	False Positive Rate
GBT	Wavelet Packet Transform
IWT	Integer Wavelet Transform
NC	Normalised Cross-correlation
PSNR	Peak Signal-to-Noise Ratio
RDWT	Redundant Discrete Wavelet Transform
RHFMs	Radial Harmonic Fourier Moments
SSIM	Structural Similarity Index
SVD	Singular Value Decomposition
SWT	Stationary Wavelet Transform
TN	True Negative
TNR	True Negative Rate
TP	True Positive
TPR	True Positive Rate
WPT	Wavelet Packet Transform

LIST OF ABBREVIATIONS (ATTACKS)

GLF3	Gaussian lowpass filter 3,1
GLF5	Gaussian lowpass filter 5,1
GLF7	Gaussian lowpass filter 7,1.4
GN0.015	Gaussian noise 0, 0.015
GN0.01	Gaussian noise 0, 0.01
GN0.005	Gaussian noise 0,0.005
SN0.05	Speckle noise 0.05
SN0.25	Speckle noise 0.25
SN0.5	Speckle noise 0.5
SP0.004	Salt & pepper 0.004
SP0.04	Salt & pepper 0.04
SP0.06	Salt & pepper 0.06
SP0.012	Salt & pepper 0.012
SP0.3	Salt & pepper 0.3
SC1.6	Scaling 1.6
SC0.5	Scaling 0.5
SC0.33	Scaling 0.33
SC0.8	Scaling 0.8
MD2x2	Median 2 x 2
MD3x3	Median 3 x 3
MD4x4	Median 4 x 4
SH	Sharpening
PS	Poisson
HG	Histogram
CC25B	Centred Cropping off 25% (128x128) by black
CC50B	Centred Cropping off 50% (256x256) by black
CC25W	Centred Cropping off 25% (128x128) by white
CC50W	Centred Cropping off 50% (256x256) by white
CR50B	Cropping row off 50% by black
CR12.5B	Cropping row off 12.5% by black
CR50W	Cropping row off 50% by white
CR12.5W	Cropping row off 12.5% by white
CC50CB	Cropping column off 50% by black

CC50CW	Cropping column off 50% by white
JPG80	Jpeg compression 80
JPG70	Jpeg compression 70
JPG60	Jpeg compression 60
JPG50	Jpeg compression 50
JPG40	Jpeg compression 40
JPG30	Jpeg compression 30

CHAPTER 1

INTRODUCTION

1.1 Introduction

With the widespread use of the internet and digital communication technologies, multimedia data of various form such as text document, image, audio, and video can be shared or obtained easily on public networks; multimedia data floating on the internet may be vulnerable to piracy as unauthorised users can easily alter multimedia data such as image. Hence, image watermarking is crucial ways to protect copyright and authenticity of these multimedia data (Su et al., 2012a).

Dual image watermarking allows the embedding of digital ownership or signature within graphical data as method of copyright (Lee et al., 2009). Besides, Ahmadi et al. (2021) mentioned that reacquiring imperceptible watermark from watermarked image allow us to identify authenticity of images, where tampered images can be located by specific algorithms.

The associated works show how important dual watermarks are to multimedia security. Hybrid techniques can be used to improve this watermarking model, and scrambled watermarks can add an extra layer of security. This paper suggests a reliable, dual watermarking technique by directly map the pixel value to an integer without rounding errors within the space domain to preserve the copyright protection of watermarked RGB image. Additionally, the integrity of the watermarked RGB image will also be authenticated or verified using image authentication techniques in this paper.

1.2 Problem Statement

Watermarking method acts as an important component to protect copyright of an image or remain the integrity of an image. However, wide range of watermarking technique might cause huge effects on image quality distortion. Thus, suitable watermarking should be implemented and practiced avoiding distortion of image quality.

There are many watermarking mechanics used for copyright protection, however, only few able to provide better security and robustness such as multiple watermarking scheme (Ernawan et al., 2018). A hybrid technique is proposed within the paper using DCT-SVD multiple watermarking technique. Similar techniques can be testified using IWT to replace DCT method, hence performing dual watermarking to examine the effectiveness on RGB image authentication and copyright protection. To sum up, new proposed technique shall act as better option compared DCT-SVD multiple watermarking method.

Although many mechanics are being proposed, much progress on authentication on image are required. Bhargava et al. (2012) introduced an authentication check for integrity. The tampers were found, but the location's accuracy was compromised. An efficient SV-based semi-fragile watermarking scheme for image content authentication with tamper localization is presented, but it is unable to recover the areas that have been altered. In order to obtain a possibly better authentication method, IWT is introduced.

Conclusion, new implementation of dual watermarking method shall aim to obtain better watermarked image with higher resolution, lower rate of image quality distortion, and achieve faster computational time on finding out the tampered region.

1.3 Objective

The objective of this project are:

- To study the methods of existing dual image watermarking methods.
- To propose new watermarking embedding methods that can achieve high imperceptibility, robustness, and tamper localization on RGB image.
- To evaluate the imperceptibility, robustness, tamper localization and computational time for authentication and copyright protection using the proposed watermarking method, in comparison to benchmark of other existing watermarking method.

1.4 Scope

- i. 10 host images of medium scale images (512 x 512 pixels) used in this study.
- ii. Two binary images with a resolution of 32 x 32 pixels are used in this study.
- iii. PSNR, SSIM, and ARE were used to assess the quality of the watermarked image.
- iv. The proposed scheme's robustness was assessed by normalized cross- correlation (NC) and bit error rate (BER) under various image attacks.
- v. The proposed scheme's tamper localization will be examined using True Positive Rate (TPR), False Negative Rate (FNR), False Positive Rate (FPR), True Negative Rate (TNR), Precision, Accuracy and F1-scaore.
- vi. The experiments were conducted using MATLAB R2022a with hpworkstation, Intel® Core™ i5-8250U CPU @ 1.60 GHz, 12GB RAM memory.

1.5 Thesis Organization

This thesis consists of five chapters.

Chapter 1 shall be discussing about the introduction of the whole research.

Chapter 2 contains the relevant study on research in general. This chapter describes the existing methods to resolve the past existing issue. Besides that, this chapter will also elaborate the techniques, method and interconnected technologies that are suitable to be compared within this research.

Chapter 3 review the overall approach and framework of the research. It explains the methodology applied when this research is executed.

Chapter 4 Discuss the results of finding on the proposed method of the experiment with detailed explanations.

Chapter 5 Contains the overall conclusion of the research findings, including future work of this research.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter contains information about the studies of existing methods and current methods of dual image watermarking. This is to grasp other method of dual image watermarking, meanwhile, making analysis on the existing methods of dual image watermarking. As dual image watermarking is known as one of the main technique for authentication and copyright protection (Manikandan & Masilamani, 2018), this chapter describes the contribution and limitation of existing watermarking methods on the imperceptibility and robustness. A literature review elaborates on few aspects.

2.2 Overview of Existing Dual Watermarking Scheme

In dual watermarking, there are two common approaches that are normally being practiced by fellow researchers, which consists of robust watermarking approach and fragile watermarking approach. Robust watermarking shall focus on tackling the durable robustness and visibility of the watermark, which serve as an important trait for copyright protection on any image. Meanwhile, fragile watermarking serves to tackles the authenticity of any image, in most case, focus on detecting tampered region of image and recovery of the original image for enhanced version. Based on different purpose of fellow researchers and different methods, robust and fragile watermarking approach are often combined to produce effective dual watermark scheme. Multiple existing works selected are performing research regarding dual watermarking method that mainly focus on images. The existing works selected consist of IWT method, DWT method, DCT method and other MATLAB function methods that are experimented to obtained best possible results in terms of imperceptibility, robustness, tamper localization and computational time.

2.3 Embedding Components

The embedding process involves strategically placing the embedding components within the content using specialized algorithms or techniques. The goal is to ensure that the embedded watermarks are robust, imperceptible to human senses, and resistant to various attacks or modifications.

2.3.1 Integer Wavelet Transform

Integer wavelet transform can map the pixel value directly to an integer without any rounding errors, allowing the watermarking algorithm to be completed quickly due to pixel values of image are integers, despite the image contains a large amount of information (Su et al., 2012b). Compared to traditional DWT, IWT has some favorable circumstances such as a simpler structure, lower operation costs, and a small storage space.

2.3.2 Human Visual Characteristic

Human Visual System (HVS) has been investigated for the intention of concealing sensitive information within images (Ahmadi et al., 2021). It locates a suitable region to embed the watermark that cause lesser distortion on the original image. Because each pixel has a different noise tolerance and effect on its adjacent pixels, the proposed approach utilized HVS characteristics to obtain higher imperceptibility and robustness by embedding on selective pixel block regions based on visual entropy and edge entropy. Visual entropy is applied to determine the spatial correlation and calculate the amount of pixels content in an image (Ernawan & Kabir, 2020a). The equation of visual entropy is:

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

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

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

2.3.3 Singular Value Decomposition

The SVD mathematical matrix decomposition is a refined method for extracting algebraic features from images. The relationship between the entries in the first column vector is one of the features. By using the Single Value Decomposition, the U component's entries could be preserved, whereas the entries for other sub-matrices component were changed when general image processing was performed (Lai, 2011).

We used this characteristic here, inserting the watermark using the singular values of the cover image's wavelet decomposition. The following is the proposed watermark embedding procedure.

The relationship between these coefficients can be used to determine whether the watermark bit is 0 or 1. SVD of A is described as follows (Ernawan & Kabir, 2020b; Lai, 2011)

$$A = USV^T$$

$$A = \sum_{i=1}^r u_i \lambda_i v_i^T$$

2.4 Analysis/Comparison of Existing Scheme

Table 1: Analysis breakdown on existing scheme.

Description	(Hurrah et al., 2019)	(Li et al., 2021)	(Han et al., 2022)	(Tiwari & Srivastava, 2022)
Type of transforms	DWT-DCT	RHFMs, DWT-DCT	GBT-SWT	IWT-Schur, SVD
Embedding sub-bands	Some blocks of LL	LL1	sub-bands L	HH
Optimization algorithm	-	-	-	-
Watermark action before embedding	AT + novel encryption	-	Fibonacci + CTBCS	3-Level IWT
Host image size	512 x 512	512 x 512	512 x 512	512 x 512
Watermark size	64 x 64	32 x 32	32 x 32	512 x 512
Watermark image type	Binary	Binary	RGB supported	Grayscale
Advantages	With double layer of security, the embedded watermark is extremely secure.	Robustness is performing well against different types of attacks and is also demonstrating strong invisibility.	Hold back arbitrary angle rotation attacks, typical image processing attacks, and to a particular extent non-rotation geometry attacks.	Integrity is provided by Arnold cat map encryption and IWT-Schur-SVD.
Disadvantages	Unable to perform image recovery after tamper is detected.	Direction corrections are too time consuming and authentication method are not proposed.	Inability to apply the watermarking method on video.	-
Description	(Hadjer & Ismail, 2022)	(Mokashi et al., 2021)	(Anand & Singh, 2020)	(Ahmadi et al., 2021)
Type of transforms	WPT, Chaotic encryption	RDWT-SVD	RDWT-SVD, Firefly	DWT-HVS-SVD
Embedding sub-bands	Some blocks of HH	All sub-bands	LL sub-bands	LL sub-bands
Optimization algorithm	-	-	-	PSO
Watermark action before embedding	-	-	ASCII, Turbo	-
Host image size	512 x 512	512 x 512	512 x 512	512 x 512
Watermark size	32 x 32	Various	256 x 256	32 x 32, 64 x 64
Watermark image type	Binary	Grayscale	Grayscale	Binary
Advantages	Encrypted with chaotic encryption, shows great effectiveness against various imperceptibility and robustness attacks	Works well at resisting attacks but also at enhancing the performance respect to noise.	Presented better results compared to a similar existing approach and had good defence against attacks.	Integrate the specialised PSO for better standards on strong watermark.
Disadvantages	Lack of appropriate transform domain technique for security.	Does not support the embedding of audio, video, 3D images, or other biometric features like the voice, iris, palm, etc.	-	Strictly limited to JPEG compression, which has poor quality and a lot of salt and pepper noise addition. needs to be improved in terms of accuracy rate.

Hurrah et al. (2019) proposed a dual watermarking system using a combination of Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT). By embedding the watermark in some blocks of the Low-Low (LL) sub-band, they achieved a double layer of security. However, their approach lacked the ability to perform image recovery after tampering was detected, which could be a drawback in certain scenarios.

Li et al. (2021) utilized Radial Harmonic Fourier Moments (RHFMs) and DWT-DCT transforms, embedding the watermark in the first level of the Low-Low (LL1) sub-band. Their technique demonstrated robustness against various types of attacks and maintained strong invisibility. However, the direction correction process was time-consuming, and an authentication method was not proposed, potentially limiting the practicality of their approach.

Han et al. (2022) employed Graph-Based Transform (GBT) and Stationary Wavelet Transform (SWT) to combat attacks, such as arbitrary angle rotation and typical image processing attacks. By embedding the watermark in the Low-pass (L) sub-bands, their method showcased resilience to these attacks. However, they did not specify the watermark action before embedding and noted the inability to apply their watermarking technique on videos, restricting its versatility.

Tiwari & Srivastava (2022) adopted an approach combining Integer Wavelet Transform (IWT) with Schur decomposition and Singular Value Decomposition (SVD). They applied 3-Level IWT before embedding the watermark in the High-High (HH) sub-band. Their method ensured integrity through Arnold cat map encryption and IWT-Schur-SVD. However, further details regarding their optimization algorithm were not provided.

Hadjer & Ismail (2022) proposed a technique that embeds the watermark in some blocks of the High-High (HH) sub-band. Their approach encrypts the watermark using chaotic encryption, demonstrating high effectiveness against imperceptibility and robustness attacks. By ensuring secure embedding and improved resistance to various attacks, their technique provides a strong level of security for watermarking.

Mokashi et al. (2021) presented a technique that utilizes a combination of Redundant Discrete Wavelet Transform (RDWT) and Singular Value Decomposition (SVD) in all sub-bands. Their approach showcases resistance against attacks while enhancing performance in the presence of noise. However, a limitation of their technique is its inability to support the embedding of audio, video, or other biometric features, limiting its application solely to image watermarking.

Anand & Singh (2020) focused on embedding the watermark using Redundant Discrete Wavelet Transform (RDWT) and Singular Value Decomposition (SVD) in the Low-Low (LL) sub-bands. They utilized ASCII and Turbo techniques for watermark action before embedding. Their approach demonstrated superior results compared to a similar existing approach, providing strong defense against attacks. Additionally, the method is suitable for watermarking large-sized images, making it practical for various applications.

Ahmadi et al. (2021) concentrated on the watermarking is embedded into the blue channel of RGB color space based on DWT, HVS and SVD. They integrated a specialized Particle Swarm Optimization (PSO) algorithm to enhance the standards and strength of the watermark. By leveraging the capabilities of PSO, their approach achieved better performance and defense against attacks, ensuring a robust and reliable watermarking solution. Fragile watermark in RGB channels authenticates suspected image without original watermark and host images. However, a drawback of their technique is its strict limitation to JPEG compression, which may result in poor image quality and the addition of salt and pepper noise. The accuracy rate of the technique also requires improvement.

Overall, these comparative analyses highlight the advantages and disadvantages of each technique. The approaches presented offer varying levels of security, robustness, invisibility, and resistance against different attacks. Considerations such as image recovery capabilities, processing time, versatility across media types, and details about the optimization algorithms used should be taken into account when selecting a suitable watermarking technique for specific applications.

2.5 Summary

In this chapter, an extended review of the existing dual watermarking approaches on copyright protection and authentication was given. The researchers were motivated to mainly design methods to perform dual watermarking copyright protection, while some researchers include methods for image authentication. The advantages and disadvantages of existing schemes are analyzed to have better understanding on what had been achieved and what has not been achieved by existing methods of dual watermarking authentication and copyright protection. To obtain a new method of copyright protection and authentication technique of dual image watermarking, IWT formula is proposed.

CHAPTER 3

METHODOLOGY

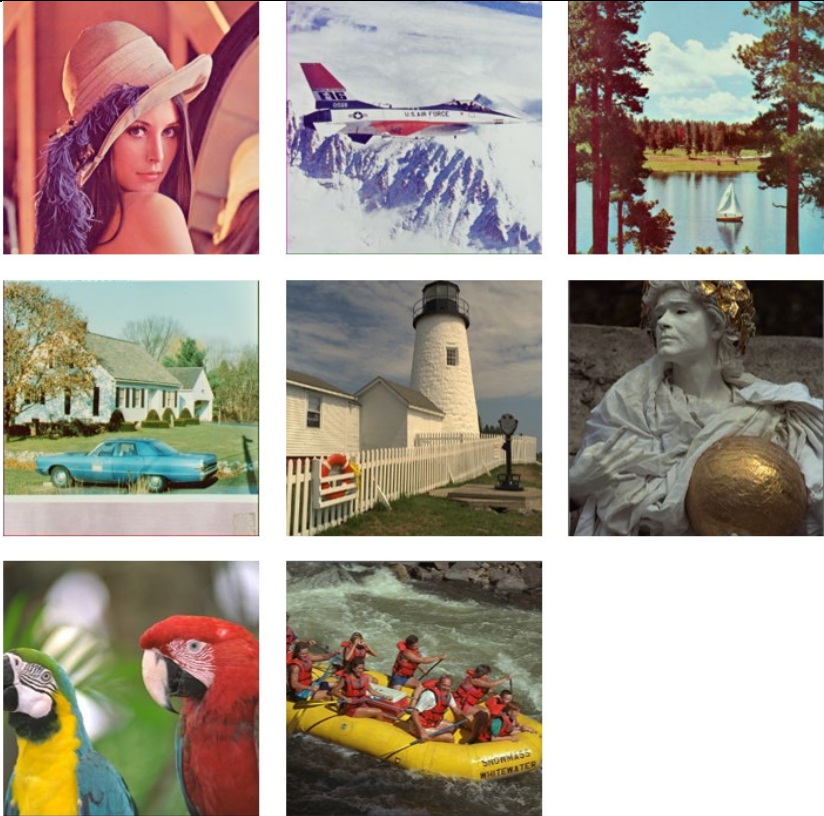

3.1 Introduction

This chapter discusses the overall approach or framework of an Undergraduate Project. It should cover method/technique or approach to be used whereas a student should discuss the methodology in detail to accomplish the project/research. The content for this chapter can contains: Introduction, ProjectManagement Framework, Project/User Requirement, Propose Design, Data Design, Proof of Initial Concept, Testing Plan and Potential use of proposed solution. The previous chapter discussed the literature review on the existing watermarking techniques. This chapter is structured as follows: the research requirements is presented in Section 3.2. Section 3.3 discussed the general research design. The experimental designs for embedding and extracting watermark are presented in Section 3.4, while Section 3.5 presented the evaluations of the watermarked image. Moreover, summary of this chapter are discussed in Section 3.6. Finally, Section 3.7 execution plans for the experimental research of this paper.

3.2 Research Requirements

The proposed approach are carried out with the setup shown as below:

Table 2: List of research requirements.

Software Requirement	Description
MATLAB R2022a	To develop the proposed system, simulate and analyses the test of algorithm.
Hardware Requirement	Description
Laptop <ul style="list-style-type: none"> • HP 15-cs0033TX • Intel® Core™ i5-8250U CPU @ 1.60 GHz • 12GB RAM memory • 480GB WD Green M.2 2280 3DSSD 	Used to conduct testing of research, obtains results and documentation of research.
Cover Image Materials	512 x 512 pixels
	
Watermark Image Materials	32 x 32 pixels
	

3.3 Research Methodology

The research methodology was constructed to develop and enhance the imperceptibility, robustness, computational time measurements, and tamper localization of existing dual watermarking approach. The methodology is divided into 5 major objectives:

1. Literature review
2. Identification of Research Problems
3. Development of Potential Solution
4. Analysis of Empirical Result
5. Documentation

3.3.1 Literature Review

The proposed plan of a secure and effective image authentication and copyright dual watermarking method were outlined in Chapter 2. In section 2.3, a summary of the comparison has been tabulated. Within section 2.4, the fundamental ideas of the dual watermarking with IWT method were thoroughly covered. Later in this study, a number of related techniques are to be used after compared with other existing studies regarding to dual watermarking.

3.3.2 Identification of Research Problems

From the literature review, research gaps in the field of dual image watermarking on copyright protection and authentication are identified. The aim to obtain better watermarked image with higher resolution, lower rate of image quality distortion, and achieve faster computational time on finding out the tampered region.

3.3.3 Development of Potential Solution

To solve the research gaps, a secure and effective image authentication and copyright protection using IWT dual watermarking approach algorithm is proposed. The development utilized IWT method to construct a robust dual watermarking algorithm and deploy a fragile watermarking for a detection of tamper region using tamper localization algorithm. The detailed proposed algorithm is presented in section 3.4.

3.3.4 Analysis of Empirical Result

The experimental result that are outputted by proposed approach are observed and presented **Chapter 4**. Detailed analysis of proposed approach are described and the results are compared with some of the approach introduced by existing papers. The upside and downside proposed approach would be recorded.

3.3.5 Documentation

The identification of problem, literature review, development of proposed algorithm, experimental results, summary and appreciation are documented for the purpose of future enhance on proposed approach.

3.4 Proposed Dual Watermarking Approach

The IWT dual watermark approach is proposed with aims to improve robustness, imperceptibility, computational time. Besides, spiral block mapping approach is included to embed the image content itself into the cover image and enhance the tamper localization of the modified image. Below are detailed algorithms for the proposed approach on image authentication and copyright protection using IWT dual watermarking approach:

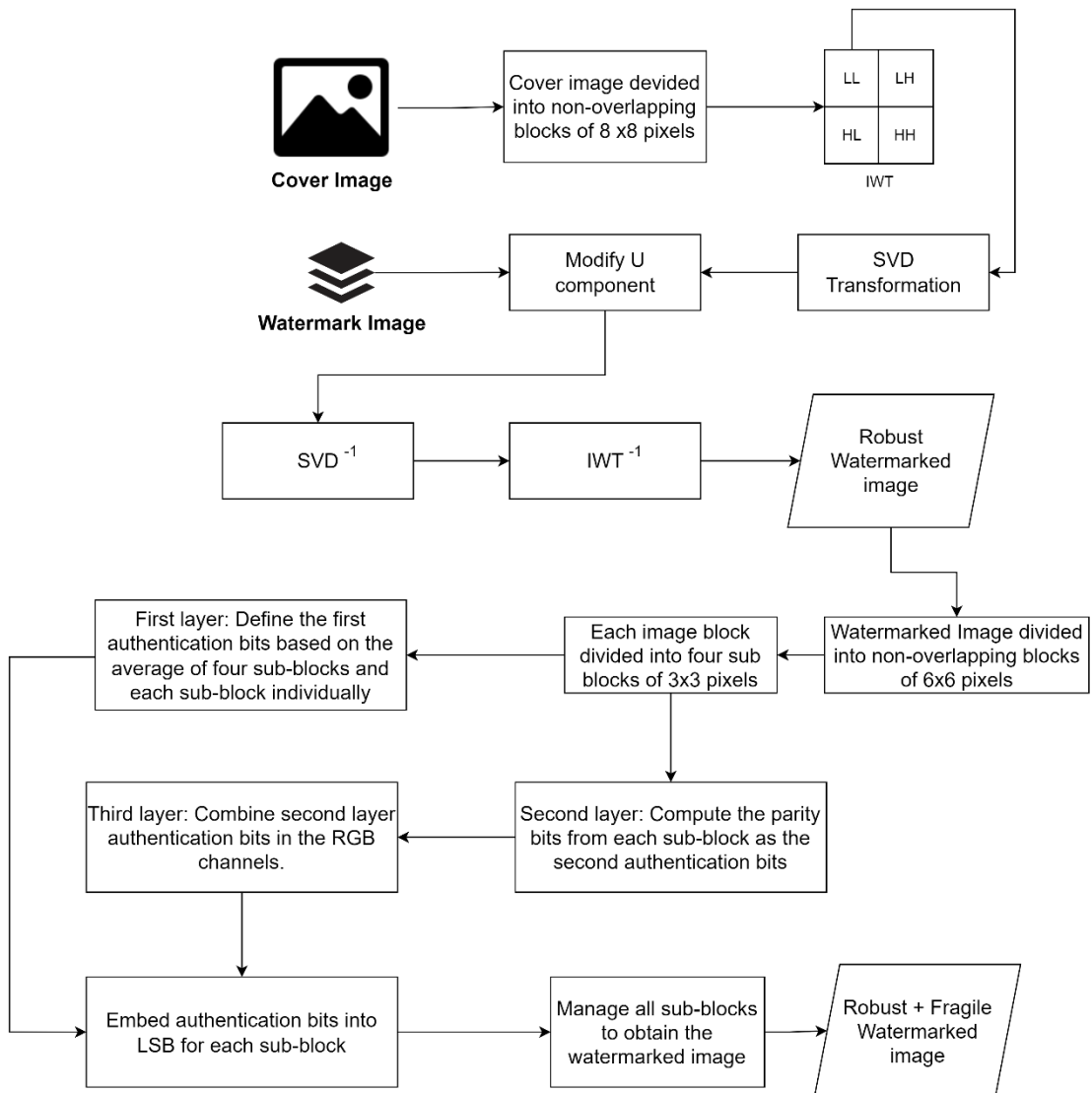


Figure 1: Block diagram of dual watermark embedding using IWT.

3.4.1 Algorithm of Robust Watermark Embedding Process

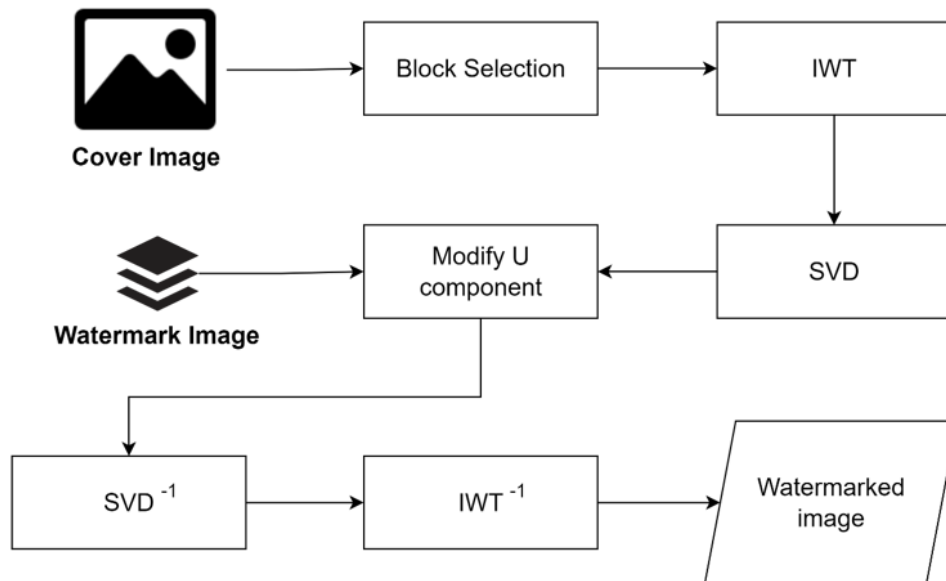


Figure 2: Block diagram of watermark logo embedding (first round embedding).

Input: Cover image, watermark image

Pre-processing:

Step 1: Divide the cover image into distinct blocks of 8 x 8 pixels.

Step 2: Using the HVS characteristics, select each non-overlapping blocks for watermark embedding.

Watermark embedding:

Step 3: Use IWT technique for each chosen blocks. To obtain U,S and V matrices,transform the first level LL sub-band matrix with SVD.

Step 4: Apply SVD to all IWT transformed blocks.

Step 5: For each chosen block, examine the relationship between the entries in the first column of the U matrix.

Post-processing:

Step 6: Perform inverse SVD and IWT on each selected block.

Step 7: Transform LL sub-band matrix with SVD all IWT transformed blocks.

Output: Watermark embedded image

3.4.2 Algorithm of Robust Watermark Embedding Process

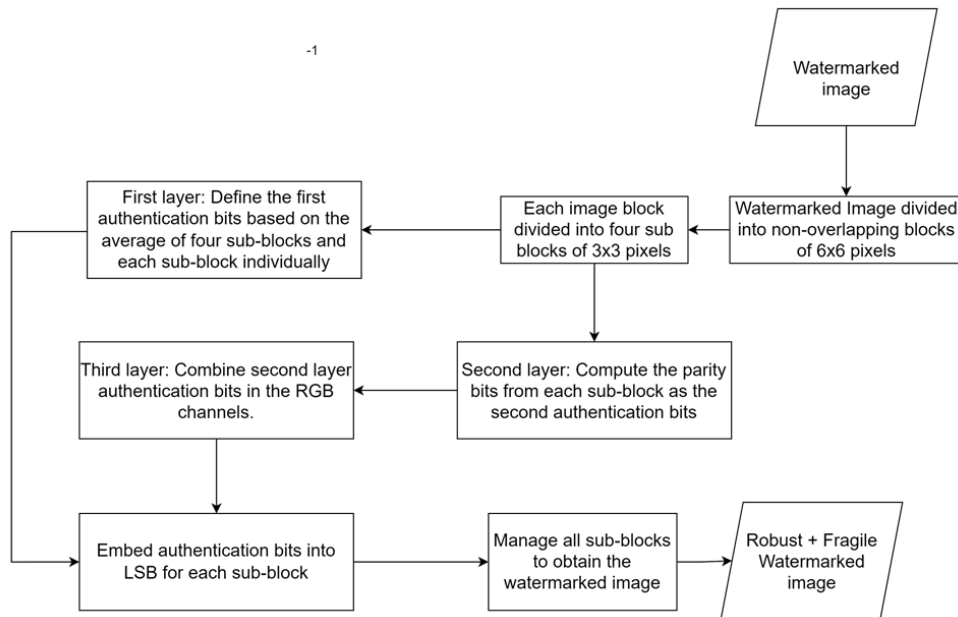


Figure 3: Block diagram of watermark logo embedding (second round embedding).

Input: First round watermark embedded image

Pre-processing:

Step 1: Divide the watermark embedded image into distinct blocks of 6 x 6 pixels. Then, each block is divided into four distinct sub-blocks of 3 x 3 pixels.

Step 2: Calculate and determine the average pixel value of each block, AvgB and average sub-blocks, AvgSB.

Watermark embedding:

Step 3: By comparing the average image block size of 6 x 6 pixels (AvgB) and each of its sub-block sizes of 3 x 3 pixels (AvgSB), the initial authentication bits were calculated. The authentication bit designated as v is 1 if the average AvgB is greater than the average AvgSB, and vice versa.

Step 4: The parity bits of each sub-block were used to create the second authentication bits. When the parity number is an odd number, the authentication bit, represented by the letter p , is 1, and when it is an even number, it is 0.

Step 5: The first and second authentication bits are embedded in each LSB of each sub-block.

Post-processing:

Step 6: In order to produce the dual watermarked image, the self-embedding watermark is repeated for each sub-block.

Output: Dual watermarked image

3.4.3 Algorithm of Robust Watermark Extracting Process

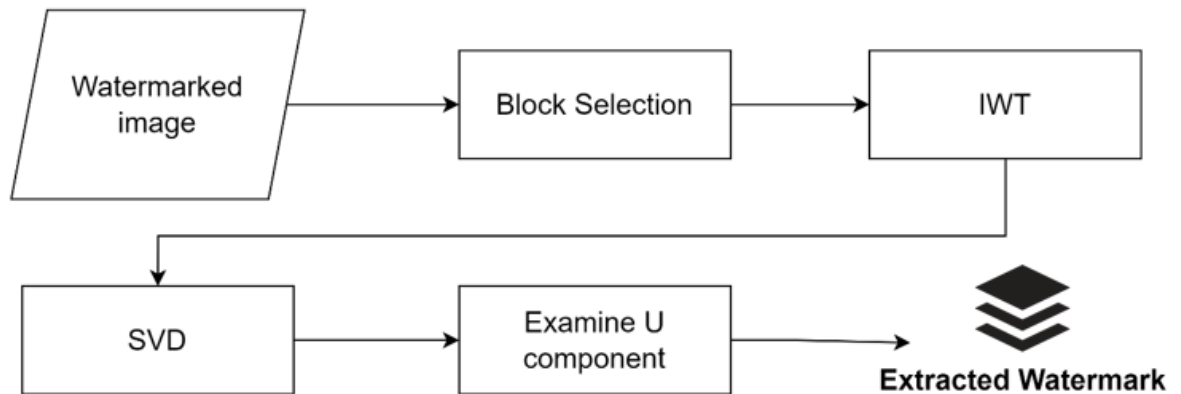


Figure 4: Block diagram of watermark extraction.

Input: Watermarked image

Pre-processing:

Step 1: Divide the cover image into distinct blocks of 8 x 8 pixels.

Step 2: The location of watermark embedded is determined by calculating each block using visual entropy and edge entropy.

Watermark extracting:

Step 3: Use IWT technique for each chosen blocks to acquires IWT domainfrequency bands.

Step 4: Apply SVD to all IWT transformed blocks.

Post-processing:

Step 5: Obtain the examined first column of U matrix, after comparing the third and fourth entries. Positive difference would result the extracted watermark bit to be 1, meanwhile, negative difference would result the extracted watermark bit to be 0. The extracted watermark bit would be used to retrieve the extracted watermark image.

Output: Extracted watermark image

3.4.4 Algorithm of Fragile Tamper Localization Process

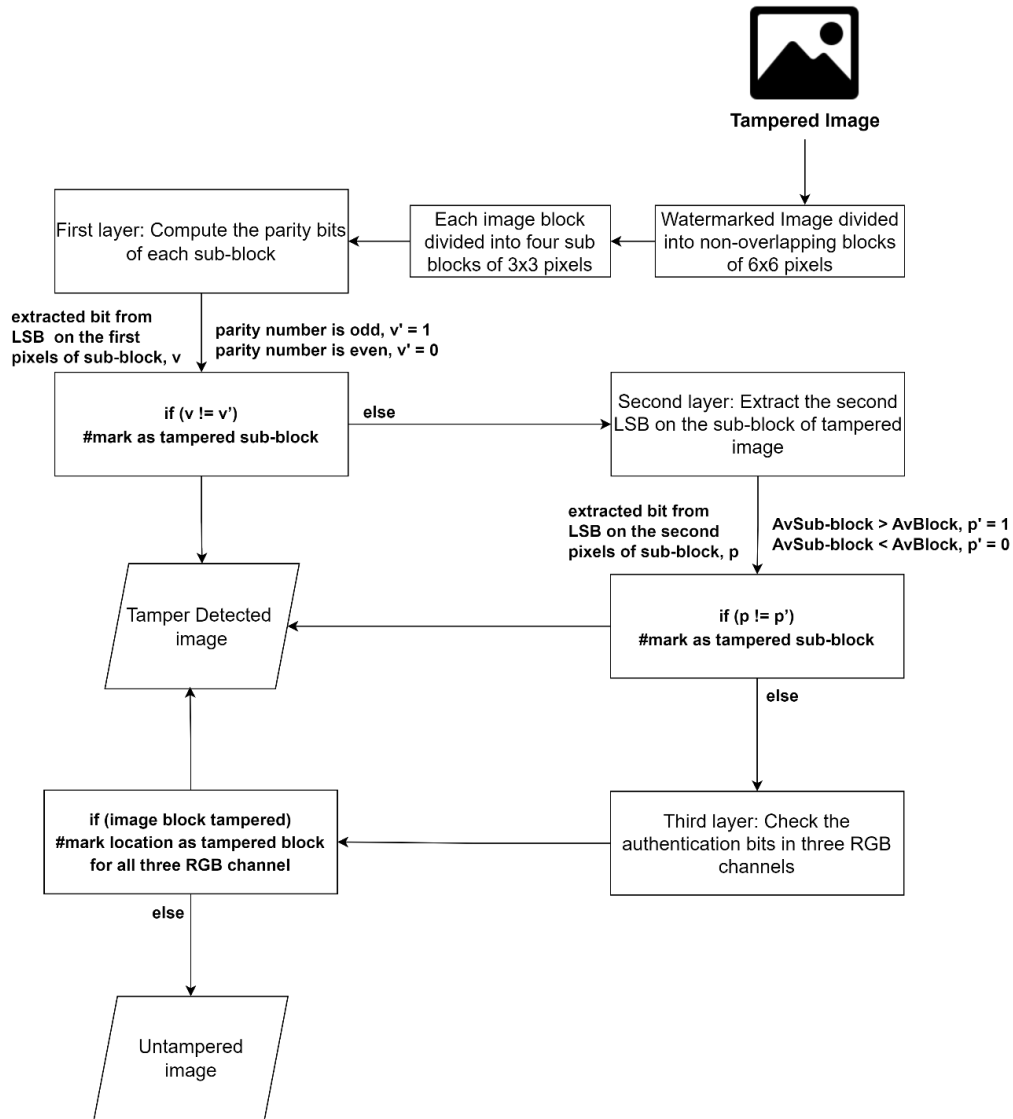


Figure 5: Block diagram of tamper localization extraction.

Input: Tampered image

Pre-processing:

Step 1: Divide the image into distinct blocks of 6 x 6 pixels. Step 2: Divide each block into four sub block of 3 x 3 pixels.

Watermark authentication:

Step 3: For the first layer authentication, average for each image block of 6 x 6 pixels and average for each sub-block of 3 x 3 pixels is obtained. A comparison is made and the authentication bit, v is assigned as 1 if the average of image block is larger than the average of image sub-block, otherwise v will be assigned as 0. Each block's parity bit is calculated; if the parity number is odd, v' is assigned as 1, otherwise v' is turned into 0. If bit v and v' are not equivalent, the image

will be declared as tampered image (Ernawan et al., 2022). If bit v and v' is equal, proceed to check authentication bit p in second level authentication.

Step 4: For second layer authentication, extracted bit p will be obtained from LSB of the modified image and compared with p' which is denoted by 1 when the average pixel of image sub-block larger than average pixel of general image block. When p and p' is equal, the image block is not tampered, otherwise, the image block will be marked as tampered.

Step 5: For third layer authentication, the authentication bit of 3 RGB channel is checked, if either one channel is marked tampered, the whole image block is marked as tampered. Moreover, if one of the tampered image blocks is detected, then every block within the block location will be marked as tampered. This layer actas reductive layer for false-negative detection.

Post-processing:

Step 6: The tamper localization algorithm examined by confusion matrix that consistsof TPR , FNR , FPR , TPR .

Output: Tamper detected image

3.5 Evaluation of the Watermarked Image

The evaluation on proposed approach of watermarked image will be used to evaluate in terms of imperceptibility, robustness, computational time measurements, and tamper localization. The measurements assess the difference between the original image and the embedded dual watermark image. The following are the components on which we would concentrate our analysis of the output:

3.5.1 Imperceptibility, Robustness, Computational Time Measurements

The performance of proposed approach on dual image-watermarking was established by assessing the imperceptibility, robustness, and computational time for embedding of watermark.

The invisibility of the watermarked image will be examine using Absolute Reconstruction Error (ARE) to measure the distortion of embedded image, Peak Signal-to-Noise Ratio (PNSR) to quality of image reconstruction, and Structural Similarity (SSIM) to determine the similarity of both the cover image and watermark embedded image (Singh & Raman, 2017).

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

$$PSNR = 10 \cdot \log_{10} \frac{255^2}{MSE},$$

$$MSE = \frac{1}{WH} \sum_i^W \sum_j^H (x_{ij} - x'_{ij})^2,$$

The robustness of watermarked image was tested using various image processing attacks, hence, assessed with normalised cross-correlation (NC) and bit error rate (BER). The computational time measurements on the proposed approach are calculated using operations function within MATLAB by utilizing variable allocation and CPU time.

3.5.2 Abbreviation of Attacks

The watermarked image of proposed algorithms are evaluated against several image processing attacks. To evaluate the effectiveness of the suggested method, simulations of the speckle noise, adjust, median filter, pepper and salt noise, JPEG XR, JPEG, JPEG2000 and histogram equalization, as well as rotation, scaling, translation, and cropping attacks were perform.

3.5.3 Tamper Localization

Few components are observed to evaluate the tamper localization of proposed algorithm, which involves components such as tampering rate, True Positive Rate (TPR), False Negative Rate (FNR), and False Positive Rate (FPR), precision, accuracy. The components involved are defined as following:

<i>TPR</i>	–	Ratio among the localized area to the actual tampered area.
<i>FNR</i>	–	Ratio among the non-localized area to the actual tampered area.
<i>FPR</i>	–	Ratio among the falsely localized area to the untampered area.
<i>Precision</i>	–	Degree of precise of image tamper localization.
<i>Accuracy</i>	–	Exact effectiveness of image tamper localization.
<i>TP</i>	–	Value of true-positive tampered image pixels.
<i>FP</i>	–	Value of false-negative tampered image pixels.
<i>P</i>	–	Value of actual tampered image pixels.
<i>TN</i>	–	Value of true-negative tampered image pixels.
<i>N</i>	–	Value of actual untampered image pixels.

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

High TPR equivalent to the tamper detection is accurately localized in the tampered regions (Ernawan et al., 2022).

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

High FNR equivalent to inaccurate tamper detection on the tampered regions (Ernawan et al., 2022).

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

Ranging between 0 to 1, lower FPR values denotes lower detection of untampered regions as tampered regions false detection (Ernawan et al., 2022).

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

Higher precision value represents greater true-positive values and smaller false-positive values (Ernawan et al., 2022).

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} = \frac{TP + TN}{P + N}$$

High accuracy of tamper localization able to improve the recovery bits of the tampered image (Ernawan et al., 2022).

3.5.4 F1-score

F1-Score is an evaluation metric, that is used to express the performance of proposed algorithm. A composition of true/false positive/negative (TP , TN , FP , FN) measures produced the F1- score. The average of the independent F1-score curves for each tested action sequence makes up the overall F1-score curve for a proposed algorithm. It combines the precision and recall results values. This means that a high F1-score signifies a high recall and precision value. Following would be the empirical formula of provided evaluation components, F1-score (Sepúlveda et al., n.d.):

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

3.6 Summary

The general research design, experimental setup, experimental design, development of the IWT dual watermarking approach, and evaluation of the watermarked image were all presented in this chapter. The development of secure and effective image authentication and copyright protection using the IWT dual watermarking approach was also demonstrated step by step in this chapter. The proposed approach is evaluated using ten distinct images and one watermark image was used in the experiments. In order to determine the imperceptibility of the watermarked image, the proposed schemes were measured using ARE, PSNR, and SSIM. The proposed schemes were also assessed for watermark recovery robustness using NC and BER. The proposed watermarking schemes were extended to image processing, geometrical, and compression attacks. The components such as tampering rate, True Positive Rate (TPR), False Negative Rate (FNR), and False Positive Rate (FPR), precision, accuracy and F1-score are used to study the potency for the tamper localization of the proposed approach. The proposed scheme's experimental results are presented in **Chapter 4**.

3.7 Gantt Chart

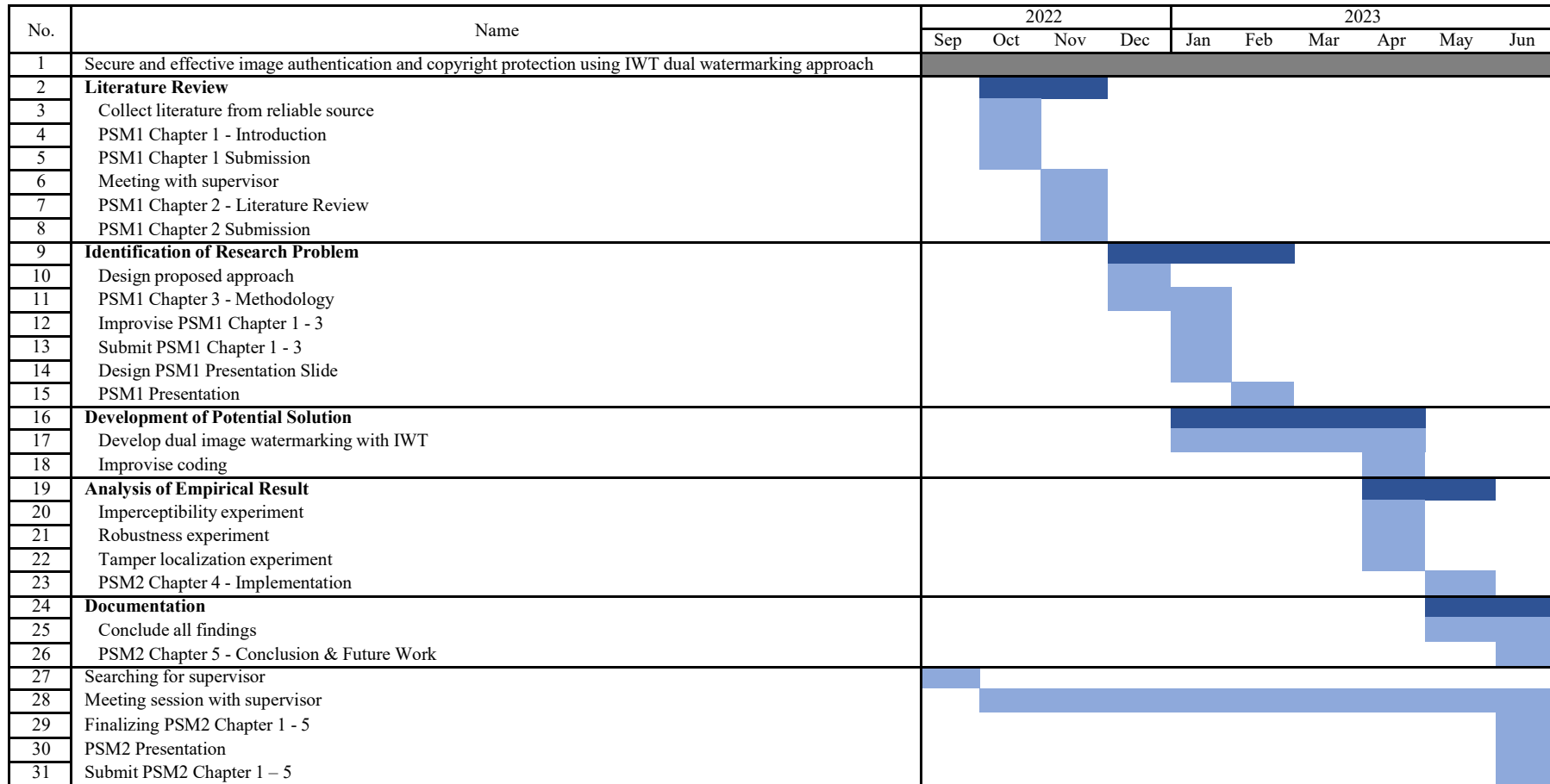


Figure 6: Timeline of PSM research.

CHAPTER 4

RESULTS AND DISCUSSION

4.1 Introduction

In chapter 4, the results and discussion of a watermarking scheme are presented. The scheme was designed to achieve imperceptibility and robustness against various attacks. The performance of the scheme was evaluated using several components, including imperceptibility, robustness, and tamper localization.

In section 4.2, the imperceptibility performance of the watermarking scheme was evaluated. The results showed that the scheme achieved high imperceptibility, meaning that the watermarked images were visually indistinguishable from the original images. This was confirmed by measuring the peak signal-to-noise ratio (PSNR) and the structural similarity index (SSIM) between the watermarked and original images.

While in section 4.3 focused on the robustness performance of the scheme after dual watermarking. The results showed that the scheme was robust against various attacks, such as JPEG compression, Gaussian noise, and cropping. The dual watermarking technique was found to improve the robustness of the scheme, making it more resistant to attacks.

Finally, in section 4.4, the tamper localization performance of the scheme was evaluated. The results showed that the scheme was capable of detecting and localizing tampering in the watermarked images. This was achieved by analyzing the changes in the watermark after an attack and comparing it with the original watermark.

Overall, the results and discussion of the watermarking scheme showed that it was able to achieve high imperceptibility and robustness, while also being able to detect and localize tampering in the watermarked images. This makes the scheme suitable for applications that require copyright protection and authentication of digital images.

4.2 Imperceptibility Performance for Different Watermark Images



Figure 7: Lena



Figure 8: Avion



Figure 9: Sailboat



Figure 10: Parrots



Figure 11: House



Figure 12: Lighthouse

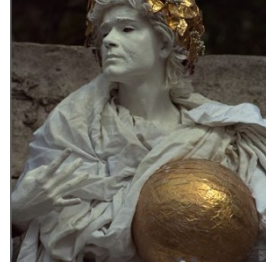


Figure 13: Statue



Figure 14: Rafting

In this experiment, the proposed dual watermark scheme was tested using 8 host images with size of 512 x 512 pixels and 2 watermark images with the size of 32 x 32 pixels. To protect the copyright of images, a dual watermarking technique was used, involving two rounds of watermark embedding. The first round involved embedding a watermark logo into eight host images, while the second round involved embedding an authentication bit into the same of images. The quality of the watermarking was evaluated using three metrics: peak signal-to-noise ratio (PSNR), structural similarity index (SSIM), and average relative error (ARE).

Table 3: PSNR, SSIM, ARE value after Watermark logo embedding.

Host Image	PSNR	SSIM	ARE
Lena	48.9125dB	0.9855	0.3651
Avion	46.1325dB	0.9716	0.4629
Sailboat	47.0322dB	0.9773	0.4216
Parrots	50.3123dB	0.9910	0.3083
House	46.7537dB	0.9749	0.4402
Lighthouse	49.6073dB	0.9869	0.3295
Statue	51.6652dB	0.9958	0.2751
Rafting	47.9706dB	0.9920	0.3572
Average	48.5483dB	0.9844	0.3700

Table 4: PSNR, SSIM, ARE value after watermark logo and authentication bit embedding.

Host Image	PSNR	SSIM	ARE
Lena	48.6436dB	0.9854	0.3930
Avion	45.9358dB	0.9715	0.4918
Sailboat	46.8959dB	0.9773	0.4440
Parrots	50.1240dB	0.9909	0.3310
House	46.6024dB	0.9749	0.4639
Lighthouse	49.5842dB	0.9869	0.3520
Statue	51.2494dB	0.9957	0.2926
Rafting	47.3746dB	0.9919	0.3767
Average	48.3012dB	0.9843	0.3931

The imperceptibility performance of the proposed watermarking scheme is shown in *Table 1*. The results showed that the first round of watermark embedding achieved an average PSNR of 48.5483dB, an average SSIM of 0.9844, and an average ARE of 0.3700. The second round of embedding shown in *Table 2* achieved an average PSNR of 48.3012dB, an average SSIM of 0.9843, and an average ARE of 0.3931. These metrics indicate that the dual watermarking technique successfully embedded the watermarks while preserving the quality of the host images.

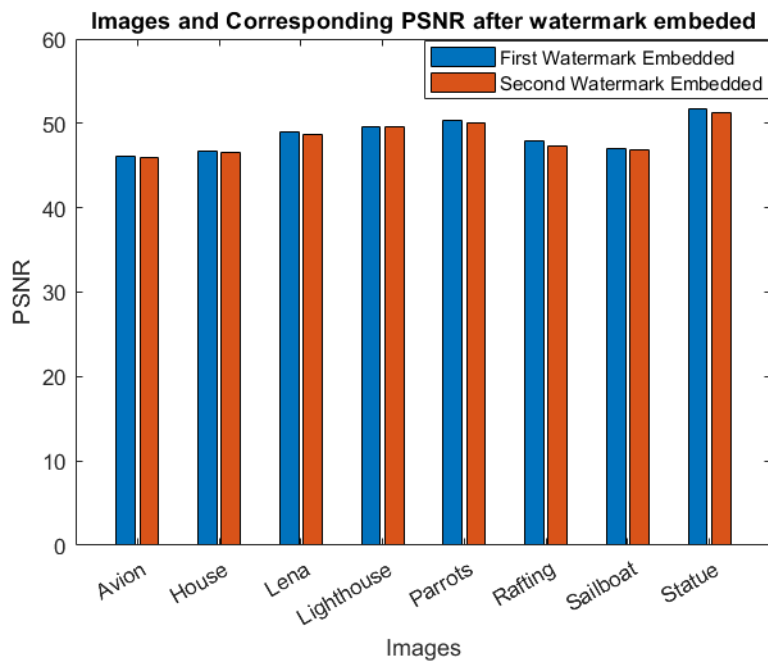


Figure 15: Bar graph visualization of PSNR values comparison after each embedding phase.

The analysis of the PSNR values for each image after the 1st and 2nd round of embedding reveals interesting insights. After the 1st round of embedding, the PSNR values range from 46.1325dB to 51.6652dB, with an average value of 48.5483dB. This indicates that the 1st round generally produces higher PSNR values, which suggests better image quality. However, after the 2nd round of embedding, the PSNR values slightly decrease for all images, ranging from 45.9358dB to 51.2494dB, with an average of 48.3012dB. Although the decrease is noticeable, the difference between the two rounds is relatively small, suggesting that the impact on image quality is minimal. Overall, the average PSNR values for both the 1st and 2nd rounds of embedding are quite close, with the 1st round having a slightly higher average value of 48.5483dB compared to the 2nd round's average of 48.3012dB. This analysis demonstrates that the 1st round generally yields better PSNR values, but the difference between the rounds is not significant in terms of image quality.

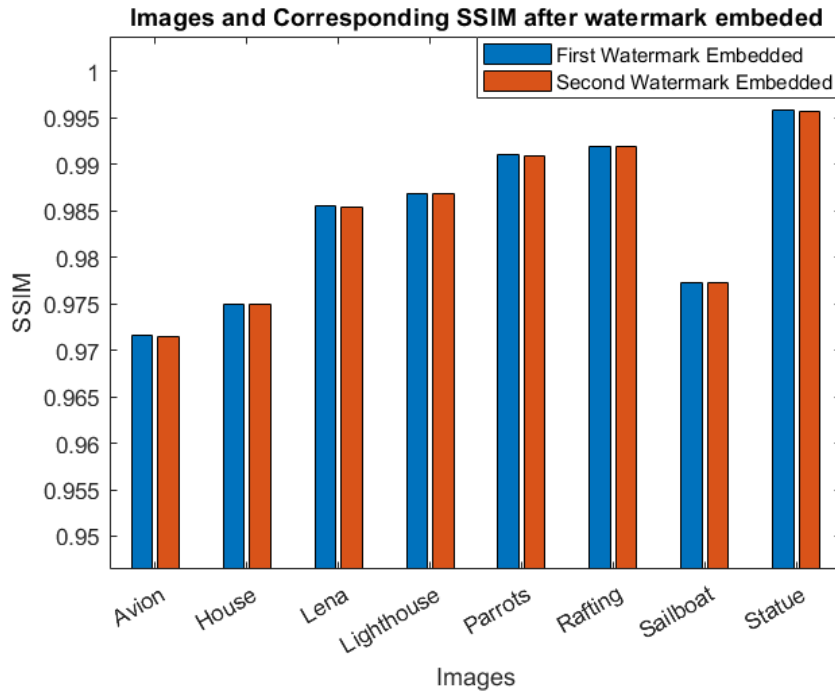


Figure 16: Bar graph visualization of SSIM values comparison after each embedding phase.

The SSIM values obtained after both the 1st and 2nd rounds of embedding demonstrate a consistently high level of image similarity for all images. The average SSIM values for both rounds are 0.9844 and 0.9843, respectively. These values indicate a strong resemblance between the embedded images and the original ones, highlighting the decent performance of the embedding process. Across all images, the SSIM values remain consistently high, with the lowest value of 0.9715 after the 2nd round of embedding for the "Avion" image. The highest SSIM values are achieved by the "Statue" image, with 0.9958 after the 1st round and 0.9957 after the 2nd round. These results indicate that the embedded images maintain a high level of similarity to their originals, preserving important structural information, luminance, and contrast. In summary, the obtained SSIM values reflect the excellent performance of the embedding process. The consistently high SSIM values for all images demonstrate the successful preservation of image quality, with the embedded images closely resembling the originals. This indicates that the embedding algorithm has achieved a commendable level of fidelity and preservation of image content.

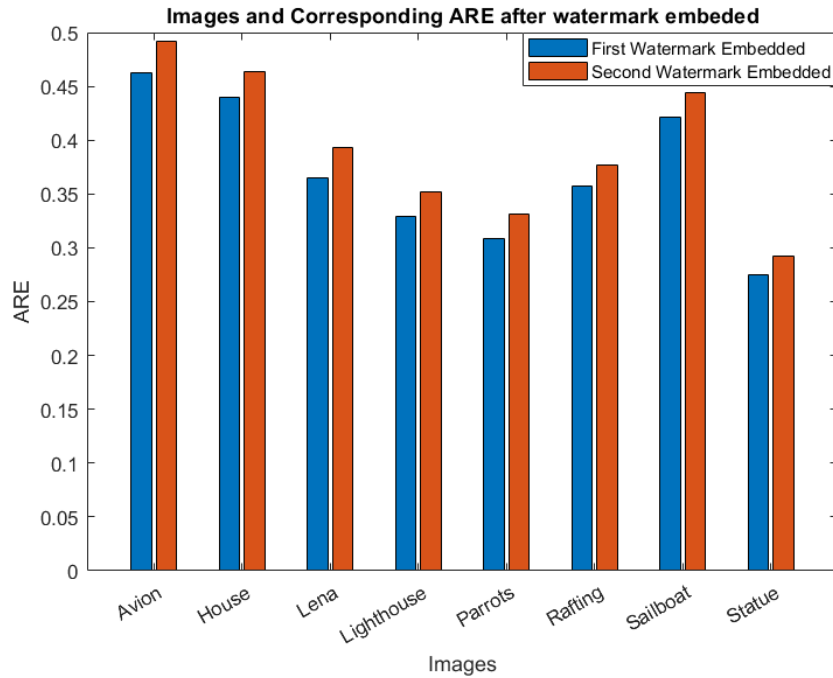


Figure 17: Bar graph visualization of ARE values comparison after each embedding phase.

After the 1st round of embedding, the ARE values range from 0.2751 to 0.4629, with an average value of 0.37. These values indicate that the embedded data size is relatively close to the original data size, suggesting a decent level of data compression. Notably, the "Statue" image achieved the lowest ARE value of 0.2751, indicating a highly efficient embedding process for that particular image. After the 2nd round of embedding, the ARE values range from 0.2926 to 0.4918, with an average of 0.3931. These values demonstrate a similar trend to the 1st round, with the embedded data size remaining reasonably close to the original data. The "Statue" image again stands out with a low ARE value of 0.2926, indicating efficient compression.

Overall, the ARE values obtained for both rounds reflect a relatively efficient embedding process. While some images achieved lower ARE values, indicating more efficient compression, the average ARE values for both rounds are in a similar range. In general, lower ARE values are desirable as they signify a more efficient compression process. However, the achieved ARE values in this case can be considered reasonably good, as they demonstrate a decent level of data compression while preserving important information and maintaining image quality. Therefore, based on the given ARE results, the embedding process can be praised for achieving a satisfactory level of efficiency, with the embedded data sizes remaining close to the original data across the majority of the images.

4.2.1 Imperceptibility Comparison

Table 5: Imperceptibility comparison between Lusua's, Kamili's and proposed scheme.

	Host Image	(Lusia et al., 2020)		(Kamili et al., 2021)		Proposed	
		PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
Robust Watermarked	Lena	41.6590dB	0.9620	42.4403dB	0.9985	49.0141dB	0.9859
	Avion	44.4900dB	0.9760	41.2703dB	0.9984	46.2812dB	0.9721
Robust + Fragile Watermarked	Lena	36.1340dB	0.8950	41.7021dB	0.9981	48.7467dB	0.9859
	Avion	36.1600dB	0.9010	41.2326dB	0.9782	46.0808dB	0.9720

Table 5 compares the performance of Lusua's watermarking scheme, Kamili's watermarking schemes, and a proposed watermarking scheme. The evaluation is based on the peak signal-to-noise ratio (PSNR) and structural similarity index (SSIM) of the watermarked images. The three schemes were tested on two host images, Lena and Avion.

For the Lena image, Lusua's scheme achieves a PSNR of 41.6590dB and an SSIM of 0.9620 for the robust watermarking, while Kamili's robust watermarking scheme achieves a slightly higher PSNR of 42.4403dB and a much higher SSIM of 0.9985. The proposed scheme achieves a higher PSNR of 49.0141dB and an SSIM of 0.9859 for the robust watermarking. For robust and fragile watermarking, Lusua's scheme achieves a lower PSNR of 36.1340dB and a lower SSIM of 0.8950, while Kamili's scheme achieves a higher PSNR of 41.7021dB and a higher SSIM of 0.9981. The proposed scheme achieves a PSNR of 48.7467dB and an SSIM of 0.9859.

For the Avion image, Lusua's scheme achieves a higher PSNR of 44.4900dB and a higher SSIM of 0.9760 for the robust watermarking, while Kamili's scheme achieves a lower PSNR of 41.2703dB but a higher SSIM of 0.9984. The proposed scheme achieves a PSNR of 46.2812dB and an SSIM of 0.9721. For robust and fragile watermarking, Lusua's scheme achieves a lower PSNR of 36.1600dB and a lower SSIM of 0.9010, Kamili's scheme achieves a lower PSNR of 41.2326dB and a lower SSIM of 0.9782, and the proposed scheme achieves a PSNR of 46.0808dB and an SSIM of 0.9720.

Overall, the proposed scheme achieves better performance in terms of PSNR compared to Lusua's and Kamili's schemes for robust watermarking on both images.

4.3 Robustness Performance after Dual Watermarking using Proposed Scheme

The robustness of a watermarked image is a crucial aspect that determines its ability to withstand various attacks while maintaining the integrity of the embedded watermark. The robustness of a watermarked image is typically evaluated by examining the Normalized Correlation (NC) and Bit Error Rate (BER) values of the embedded watermark under various attacks. The NC measures the similarity between the original and the watermarked image, while the BER measures the bit error rate of the embedded watermark.

In the case of the examined scheme, the results indicate that the watermarked image is robust against various attacks, such as JPEG compression, Gaussian noise, and cropping. This is evidenced by the fact that the NC and BER values remain high and low, respectively, even after these attacks are applied to the watermarked image.

Furthermore, the dual watermarking technique used in the scheme is found to improve its robustness even further. This means that the embedded watermark is more resistant to attacks, as indicated by the high NC and low BER values even after the application of various attacks. Therefore, it can be concluded that the watermarked image is robust and resistant to various image processing attacks, making it suitable for use in applications where copyright protection is important.

4.3.1 NC and BER Values for Proposed Scheme

Table 6: Visualization of host image under various attacks, including NC and BER values.






















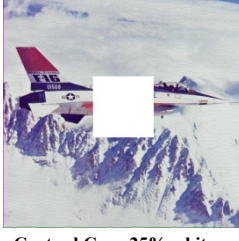

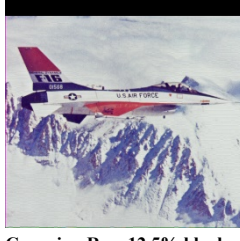

Image	Extracted watermark	Image	Extracted watermark	Image	Extracted watermark
	 NC 1.000 BER 0.000		 NC 1.000 BER 0.000		 NC 0.9847 BER 0.0156
Without Attack		Tamper Attack		Gaussian Lowpass Filter 3 x 3	
	 NC 0.8720 BER 0.1269		 NC 0.7151 BER 0.2773		 NC 0.9843 BER 0.0156
Gaussian Noise 0.015		Speckle Noise 0.05		Salt & Pepper 0.004	
	 NC 0.9865 BER 0.0136		 NC 0.4409 BER 0.5117		 NC 0.9837 BER 0.0166
Scaling 1.6		Rotation 30		Median Filter 2 x 2	
	 NC 0.9921 BER 0.0078		 NC 0.9931 BER 0.0068		 NC 0.9931 BER 0.0068
Sharpening		Poison Noise		Histogram	
	 NC 0.9911 BER 0.0087		 NC 0.9921 BER 0.0078		 NC 0.9712 BER 0.0283
Centred Crop 25% black		Centred Crop 25% white		Cropping Row 12.5% black	













Image	Extracted watermark	Image	Extracted watermark	Image	Extracted watermark
	 NC 0.9703 BER 0.0732		 NC 0.8497 BER 0.1386		 NC 0.8497 BER 0.1386
Cropping Row 12.5% white		Cropping Column 25% black		Cropping Column 25% white	
	 NC 0.9894 BER 0.0107		 NC 0.9817 BER 0.0185		 NC 0.9894 BER 0.0107
JPEG Compression 80		JPEG Compression 30		JPEG2000 Lossy Compression C.Ratio 4	

Table 6 demonstrate the robustness of proposed scheme by being able to successfully extract the watermark of dual watermarked image, “Avion.tiff”, in the presence of various image processing attacks. This is evidenced by the Normalized Correlation (NC) and Bit Error Rate (BER) values obtained by the proposed scheme, which indicate its effectiveness in preserving the integrity of the watermark even after image processing attacks. This demonstrates its ability to provide reliable identification of the original source of an image and detect any unauthorized changes made to it. As such, the proposed scheme is a robust and effective solution for digital image watermarking.

Sharpening, poison noise, and histogram-based attacks consistently achieved high NC values above 0.99, indicating excellent preservation of the watermark. The corresponding BER values were also low, ranging from 0.0068 to 0.0087, indicating excellent watermark extraction.

Both centered crop attacks, with black and white backgrounds, demonstrated good preservation of the watermark with NC values above 0.99. The BER values were low, further indicating successful extraction.

The cropping row and column attacks resulted in lower NC values ranging from 0.8497 to 0.9712, suggesting some degradation in watermark preservation. The BER values were relatively higher, ranging from 0.0283 to 0.1386, indicating challenges in accurate extraction.

The JPEG compression attacks at different quality settings showed a trade-off between NC and BER values. With a compression ratio of 80, the NC value was relatively

high at 0.9894, while the BER value was low at 0.0107. However, at a lower quality setting (30), both NC and BER values decreased, indicating a noticeable impact on watermark preservation and extraction.

The JPEG2000 compression attacks with a compression ratio of 4 achieved a high NC value of 0.9894, indicating good preservation of the watermark. The corresponding BER value was low at 0.0107, demonstrating successful extraction.

Observing the results to the images without any attack, the preservation and extraction performance of the different image processing attacks varied. Attacks such as sharpening, poison noise, histogram-based attacks, centred crop attacks, and JPEG2000 compression showed good results in terms of both NC and BER values. However, it is evident that some attacks, such as cropping, speckle noise, and rotation, have significantly impacted the preservation of the watermark. These attacks resulted in lower NC values and higher BER values, suggesting a compromise in both preservation and accurate extraction.

The evaluation of the various image processing attacks revealed notable vulnerabilities in the face of different attacks. The outcomes of these attacks consistently showed lower Normalized Correlation (NC) values and higher Bit Error Rate (BER) values, indicating a compromise in both the preservation of the watermark and the accuracy of its extraction. These findings serve as a stark reminder of the necessity of watermarking approach with strong robustness to ensure reliable watermark extraction in practical situations.

4.3.2 Robustness Comparison of NC and BER Values for Proposed Scheme

Table 7: NC and BER values comparison between Duan's scheme and proposed scheme under various attacks.

No	Attacks	NC		BER	
		(Duan et al., 2020)	Proposed	(Duan et al., 2020)	Proposed
1	GLF3: Gaussian lowpass filter 3,1	0.9502	0.9847	0.5244	0.0156
2	GLF5: Gaussian lowpass filter 5,1	0.9360	0.9801	0.5273	0.0205
3	GLF7: Gaussian lowpass filter 7,1.4	0.8820	0.9718	0.5498	0.0293
4	GN0.015: Gaussian noise 0, 0.015	0.5870	0.8721	0.7100	0.1270
5	GN0.01: Gaussian noise 0, 0.01	0.6449	0.9241	0.6631	0.0762
6	GN0.005: Gaussian noise 0,0.005	0.7041	0.9733	0.6436	0.0264
7	SN0.05: Speckle noise 0.05	0.5833	0.7151	0.7188	0.2773
8	SN0.25: Speckle noise 0.25	0.5130	0.5756	0.7305	0.4248
9	SN0.5: Speckle noise 0.5	0.4903	0.5573	0.7256	0.4375
10	SP0.004: Salt & pepper 0.004	0.8843	0.9844	0.5557	0.0156
11	SP0.04: Salt & pepper 0.04	0.6130	0.8730	0.6787	0.1279
12	SP0.06: Salt & pepper 0.06	0.6002	0.8169	0.7061	0.1816
13	SP0.012: Salt & pepper 0.012	0.7841	0.9689	0.6133	0.0313
14	SP0.3: Salt & pepper 0.3	0.5548	0.6243	0.7275	0.3750
15	SC1.6: Scaling 1.6	0.9114	0.9866	0.5459	0.0137
16	SC0.5: Scaling 0.5	0.9450	0.9866	0.5244	0.0137
17	SC0.33: Scaling 0.33	0.8406	0.9331	0.5713	0.0674
18	SC0.8: Scaling 0.8	0.9071	0.9866	0.5459	0.0137
19	MD2x2: Median 2 x 2	0.8572	0.9838	0.5703	0.0166
20	MD3x3: Median 3 x 3	0.9354	0.9866	0.5313	0.0137
21	MD4x4: Median 4 x 4	0.8342	0.9733	0.5801	0.0273
22	SH: Sharpening	0.9562	0.9921	0.5234	0.0078
23	PS: Poisson	0.8159	0.9931	0.5967	0.0068
24	HG: Histogram	0.8798	0.9931	0.5596	0.0068
25	CC25B: Centred Cropping off 25% (128x128) by black	0.9217	0.9912	0.5303	0.0088
26	CC50B: Centred Cropping off 50% (256x256) by black	0.8164	0.9437	0.5020	0.0547
27	CC25W: Centred Cropping off 25% (128x128) by white	0.9236	0.9921	0.5283	0.0078
28	CC50W: Centred Cropping off 50% (256x256) by white	0.8166	0.9467	0.5020	0.0518
29	CR50B: Cropping row off 50% by black	0.7126	0.8024	0.5039	0.1777
30	CR12.5B: Cropping row off 12.5% by black	0.9522	0.9712	0.5225	0.0283
31	CR50W: Cropping row off 50% by white	0.7126	0.8024	0.5039	0.1777
32	CR12.5W: Cropping row off 12.5% by white	0.9522	0.9703	0.5225	0.0293
33	CC50CB: Cropping column off 50% by black	0.6729	0.7839	0.5234	0.1924
34	CC50CW: Cropping column off 50% by white	0.6729	0.7839	0.5234	0.1924
35	JPG80: Jpeg compression 80	0.9433	0.9894	0.5273	0.0107
36	JPG70: Jpeg compression 70	0.9249	0.9894	0.5381	0.0107
37	JPG60: Jpeg compression 60	0.8962	0.9875	0.5557	0.0127
38	JPG50: Jpeg compression 50	0.8783	0.9874	0.5625	0.0127
39	JPG40: Jpeg compression 40	0.8329	0.9865	0.5830	0.0137
40	JPG30: Jpeg compression 30	0.7373	0.9818	0.6191	0.0186

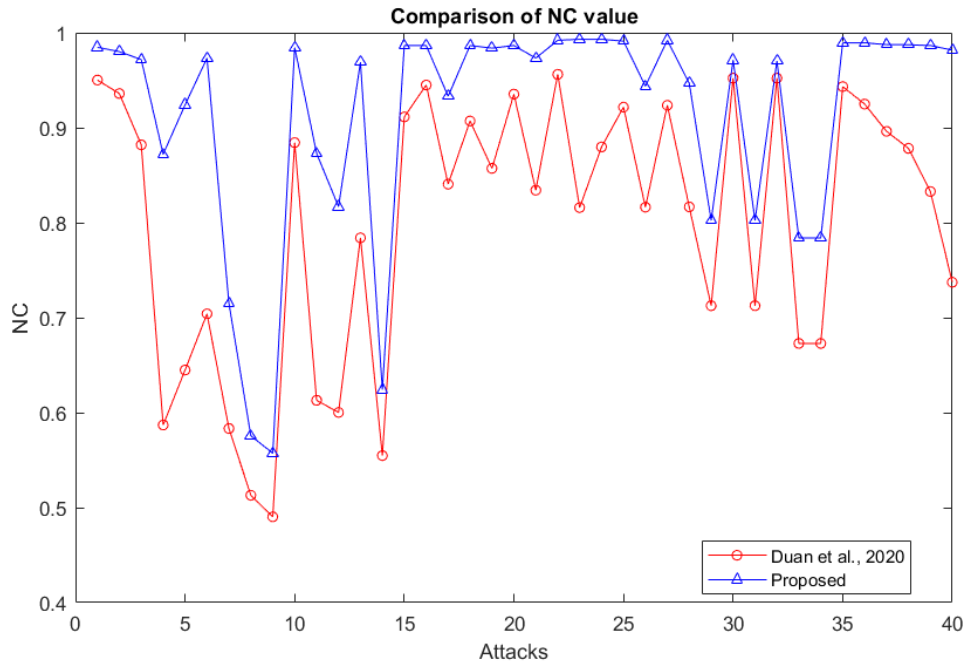


Figure 18: Line graph of NC values for Duan's scheme and proposed scheme

The comparative analysis between the proposed scheme and Duan's Scheme in *Table 7* and *Figure 18* highlights the superior performance of the proposed scheme in image processing attacks. The proposed scheme shows better Normalized Correlation (NC) and Bit Error Rate (BER) values in all types of attacks compared to Duan's Scheme, indicating its ability to withstand image processing attacks more effectively.

When subjected to Gaussian lowpass filters (GLF3, GLF5, and GLF7), the proposed scheme consistently outperforms Duan's scheme. It achieves higher NC values, indicating better preservation of the watermarked image and improved resistance to the filtering effects. For GLF3, the proposed scheme achieves an NC value of 0.9847, indicating better preservation of the watermarked image compared to Duan's NC value of 0.9502. Similar trends are observed for GLF5 and GLF7, where the proposed scheme achieves NC values of 0.9801 and 0.9718, respectively, surpassing Duan's NC values of 0.936 and 0.882. This demonstrates that the proposed scheme offers enhanced robustness against Gaussian lowpass filter attacks compared to Duan's scheme.

In the presence of Gaussian noise (GN0.015, GN0.01, and GN0.005), the proposed scheme exhibits superior performance compared to Duan's scheme. It consistently achieves higher NC values, suggesting its ability to maintain the integrity of the embedded watermark even in the presence of noise. For GN0.015, the proposed scheme achieves an NC value of 0.8721, while Duan's scheme only achieves 0.587. Similarly, for GN0.01 and GN0.005, the proposed scheme achieves NC values of 0.9241 and 0.9733, respectively, surpassing Duan's NC values of 0.6449 and 0.7041. This showcases the proposed scheme's effectiveness in withstanding Gaussian noise attacks.

For speckle noise attacks (SN0.05, SN0.25, and SN0.5), the proposed scheme demonstrates a clear advantage over Duan's scheme. For SN0.05, the proposed scheme achieves an NC value of 0.7151, surpassing Duan's NC value of 0.5833. The same trend is observed for SN0.25 and SN0.5, where the proposed scheme achieves NC values of 0.5756 and 0.5573, respectively, outperforming Duan's NC values of 0.513 and 0.4903. It consistently achieves higher NC values, indicating better resistance to the distortions caused by speckle noise. These results highlight the effectiveness of the proposed scheme in handling different levels of speckle noise compared to Duan's scheme.

When confronted with salt and pepper noise attacks (SP0.004, SP0.04, SP0.06, SP0.012, and SP0.3), the proposed scheme consistently outperforms Duan's scheme. For SP0.004, the proposed scheme achieves an NC value of 0.9844, outperforming Duan's NC value of 0.8843. A similar trend is observed for SP0.04, SP0.06, and SP0.012, where the proposed scheme achieves higher NC values of 0.873, 0.8169, and 0.9689, respectively, compared to Duan's NC values. Additionally, for SP0.3, the proposed scheme achieves an NC value of 0.6243, surpassing Duan's NC value of 0.5548.

Under scaling attacks (SC1.6, SC0.5, SC0.33, and SC0.8), the proposed scheme consistently achieves higher NC values compared to Duan's scheme. In the case of SC1.6, the proposed scheme achieves an NC value of 0.9866, surpassing Duan's NC value of 0.9114. Similarly, for SC0.5 and SC0.8, the proposed scheme maintains a high NC value of 0.9866, while Duan's scheme achieves lower NC values of 0.945 and 0.9071, respectively. The proposed scheme demonstrates its ability to withstand scaling transformations better than Duan's scheme.

Furthermore, in the case of median filtering attacks (MD2x2, MD3x3, and MD4x4), the proposed scheme outperforms Duan's scheme. For MD2x2 and MD4x4, the proposed scheme achieves NC values of 0.9838 and 0.9733, respectively, outperforming Duan's scheme with NC values of 0.8572 and 0.8342. The proposed scheme maintains a high NC value of 0.9866 for MD3x3, while Duan's scheme achieves a slightly lower NC value of 0.9354. It consistently achieves higher NC values, demonstrating improved resistance to median filtering and better preservation of the embedded watermark.

Regarding sharpening (SH), Poisson noise (PS), and histogram equalization (HG) attacks, the proposed scheme consistently achieves higher NC values compared to Duan's scheme. This signifies its superiority in maintaining the quality and integrity of the watermarked image under these types of attacks. The proposed scheme achieves an NC value of 0.9921 for SH, while Duan's scheme achieves a slightly lower NC value of 0.9562. This demonstrates the ability of the proposed scheme to preserve the watermarked image even in the presence of sharpening transformations. For PS and HG, the proposed scheme achieves NC values of 0.9931, surpassing Duan's NC values of 0.8159 and 0.8798, respectively. The proposed scheme achieves slightly higher NC values compared to Duan's scheme.

When subjected to cropping attacks (CC25B, CC50B, CC25W, CC50W, CR50B, CR12.5B, CR50W, CR12.5W, CC50CB, and CC50CW), the proposed scheme showcases excellent resilience. It consistently achieves higher NC values, indicating its ability to withstand cropping distortions and ensuring accurate extraction of the embedded watermark. In the case of CC25B and CC25W, the proposed scheme achieves NC values of 0.9912 and 0.9921, respectively, outperforming Duan's scheme with NC values of 0.9217 and 0.9236. For CC50B and CC50W, the proposed scheme achieves NC values of 0.9437 and 0.9467, respectively, while Duan's scheme achieves slightly lower NC values. For CR50B and CR50W, the proposed scheme achieves NC values of 0.8024, while Duan's scheme achieves the same NC value. Similarly, for CR12.5B and CR12.5W, the proposed scheme achieves NC values of 0.9712 and 0.9703, respectively, surpassing Duan's NC values. For CC50CB and CC50CW, the proposed scheme achieves NC values of 0.7839, outperforming Duan's scheme with the same NC values.

Lastly, under JPEG compression attacks (JPG80, JPG70, JPG60, JPG50, JPG40, and JPG30), the proposed scheme consistently outperforms Duan's scheme. It achieves higher NC values, highlighting its robustness against the lossy compression effects and its capability to maintain the quality and integrity of the watermarked image. For JPG80, JPG70, and JPG60, the proposed scheme achieves NC values of 0.9894, 0.9894, and 0.9875, respectively, surpassing Duan's NC values. The proposed scheme maintains a high NC value of 0.9874 for JPG50, while Duan's scheme achieves a lower NC value of 0.8783. It achieves an NC value of 0.9865 for JPG40, outperforming Duan's scheme with an NC value of 0.8329. Similarly, for JPG30, the proposed scheme achieves an NC value of 0.9818, surpassing Duan's NC value of 0.7373. Overall, when subjected to JPEG compression attacks, the proposed scheme consistently outperforms Duan's scheme in terms of maintaining the quality and integrity of the watermarked image.

Overall, the proposed scheme offers robustness and security for digital image watermarking, making it a suitable solution for copyright protection and tamper detection. The results of this case study demonstrate the importance of developing effective watermarking schemes that can withstand various types of attacks and preserve image quality.

4.3.3 Extracted Watermark of Proposed Scheme after Irregular Attack Combined with Image Processing Attacks

Table 8: Visualization of host image and watermark logo after irregular tamper attack combined various image processing attacks, including NC and BER values.



























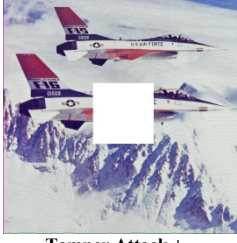



Image	Extracted watermark	Image	Extracted watermark	Image	Extracted watermark
	 NC 1.000 BER 0.000		 NC 1.000 BER 0.000		 NC 0.9700 BER 0.0303
Without Attack		Tamper Attack		Tamper Attack + Gaussian Lowpass Filter 3 x 3	
	 NC 0.8527 BER 0.1465		 NC 0.7235 BER 0.2832		 NC 0.9753 BER 0.0244
Tamper Attack + Gaussian Noise 0.015		Tamper Attack + Speckle Noise 0.05		Tamper Attack + Salt & Pepper 0.004	
	 NC 0.9739 BER 0.0264		 NC 0.4501 BER 0.5049		 NC 0.9711 BER 0.0293
Tamper Attack + Scaling 1.6		Tamper Attack + Rotation 30		Tamper Attack + Median Filter 2 x 2	
	 NC 0.9803 BER 0.0195		 NC 0.9814 BER 0.0186		 NC 0.9833 BER 0.0166
Tamper Attack + Sharpening		Tamper Attack + Poison Noise		Tamper Attack + Histogram	
	 NC 0.9783 BER 0.0215		 NC 0.9793 BER 0.0205		 NC 0.9581 BER 0.410
Tamper Attack + Centred Crop 25% black		Tamper Attack + Centred Crop 25% white		Tamper Attack + Cropping Row 12.5% black	













Image	Extracted watermark	Image	Extracted watermark	Image	Extracted watermark
	 NC 0.9573 BER 0.420		 NC 0.8347 BER 0.1514		 NC 0.8347 BER 0.1514
Tamper Attack + Cropping Row 12.5% white		Tamper Attack + Cropping Column 25% black		Tamper Attack + Cropping Column 25% white	
	 NC 0.9787 BER 0.0215		 NC 0.9721 BER 0.0283		 NC 0.9787 BER 0.0215
Tamper Attack + JPEG Compression 80		Tamper Attack + JPEG Compression 30		Tamper Attack + JPEG2000 Lossy Compression C.Ratio 4	

Table 8 exhibits its robustness by being able to successfully extract the watermark in the presence of irregular attacks paired with image processing attacks. This is a crucial component of any digital watermarking system because it guarantees that the watermark will dependably be recovered even in the event of unanticipated attacks or alterations to the watermarked image.

Initially, without any attack, the proposed scheme demonstrates a perfect correlation with an NC value of 1.000 and zero bit errors (BER = 0.000). This indicates that the watermark extraction is successful in the absence of any tampering.

When introducing irregular tampering, the NC value remains high at 1.000, indicating a strong correlation between the original and extracted watermarks. The BER value remains at 0.000, suggesting no bit errors in the extracted watermark. This implies that the proposed scheme is robust against irregular tampering attacks.

Next, applying the "Irregular Tamper and Gaussian Lowpass Filter 3 x 3" combination, the NC value slightly decreases to 0.9700, indicating a slight decrease in the correlation between the original and extracted watermarks. The BER value increases to 0.0303, implying the presence of a few bit errors in the extracted watermark.

When introducing "Irregular Tamper and Gaussian Noise 0.015," the NC value decreases further to 0.8527, indicating a noticeable decrease in the correlation between the original and extracted watermarks. The BER value increases significantly to 0.1465, indicating a higher number of bit errors in the extracted watermark.

Similarly, combining "Irregular Tamper and Speckle Noise 0.05" leads to a further decrease in the NC value to 0.7235. The BER value increases to 0.2832, suggesting a higher number of bit errors in the extracted watermark.

However, when applying "Irregular Tamper and Salt & Pepper 0.004," the NC value remains relatively high at 0.9753, indicating a strong correlation between the original and extracted watermarks. The BER value remains low at 0.0244, suggesting a small number of bit errors.

Introducing "Irregular Tamper and Scaling 1.6" results in an NC value of 0.9739, indicating a strong correlation between the original and extracted watermarks. The BER value remains low at 0.0264, implying a minimal number of bit errors.

On the other hand, when "Irregular Tamper and Rotation 30" is performed, the NC value drops significantly to 0.4501, indicating a substantial decrease in the correlation between the original and extracted watermarks. The BER value increases to 0.5049, suggesting a high number of bit errors in the extracted watermark.

Applying "Irregular Tamper and Median Filter 2 x 2" results in an NC value of 0.9711, indicating a strong correlation between the original and extracted watermarks. The BER value remains low at 0.0293, suggesting a minimal number of bit errors.

When introducing "Irregular Tamper and Sharpening," the NC value increases to 0.9803, indicating a strong correlation between the original and extracted watermarks. The BER value remains low at 0.0195, implying a minimal number of bit errors.

Similarly, applying "Irregular Tamper and Poison Noise" results in an NC value of 0.9814, indicating a strong correlation between the original and extracted watermarks. The BER value remains low at 0.0186, suggesting a minimal number of bit errors.

When introducing "Irregular Tamper and Histogram," the NC value increases to 0.9833, indicating a higher correlation between the original and extracted watermarks. The BER value remains low at 0.0166, suggesting a minimal number of bit errors.

Next, combining "Irregular Tamper and Centred Crop 25% black" results in an NC value of 0.9783, indicating a strong correlation between the original and extracted watermarks. The BER value remains low at 0.0215, suggesting a minimal number of bit errors.

Similarly, applying "Irregular Tamper and Centred Crop 25% white" leads to an NC value of 0.9793, indicating a strong correlation between the original and extracted watermarks. The BER value remains low at 0.0205, suggesting a minimal number of bit errors.

When applying "Irregular Tamper and Cropping Row 12.5% black," the NC value decreases to 0.9581, indicating a decrease in the correlation between the original and extracted watermarks. The BER value increases significantly to 0.410, implying a higher number of bit errors in the extracted watermark.

Similarly, applying "Irregular Tamper and Cropping Row 12.5% white" leads to a slightly lower NC value of 0.9573, indicating a decrease in the correlation between the original and extracted watermarks. The BER value increases to 0.420, suggesting a higher number of bit errors in the extracted watermark.

When introducing "Irregular Tamper and Cropping Column 25% black," the NC value decreases to 0.8347, indicating a substantial decrease in the correlation between the original and extracted watermarks. The BER value remains relatively low at 0.1514, suggesting a moderate number of bit errors in the extracted watermark.

Similarly, applying "Irregular Tamper and Cropping Column 25% white" leads to the same NC value of 0.8347, indicating a substantial decrease in the correlation between the original and extracted watermarks. The BER value remains relatively low at 0.1514, suggesting a moderate number of bit errors in the extracted watermark.

When introducing "Irregular Tamper and JPEG Compression 80," the NC value remains high at 0.9787, indicating a strong correlation between the original and extracted watermarks. The BER value remains low at 0.0215, implying a minimal number of bit errors.

Similarly, applying "Irregular Tamper and JPEG Compression 30" leads to an NC value of 0.9721, indicating a strong correlation between the original and extracted watermarks. The BER value remains low at 0.0283, suggesting a minimal number of bit errors.

Finally, combining "Irregular Tamper and JPEG2000 Lossy Compression C.Ratio 4" results in an NC value of 0.9787, indicating a strong correlation between the original and extracted watermarks. The BER value remains low at 0.0215, implying a minimal number of bit errors.

Overall, the analysis reveals that the proposed scheme performs well in preserving the correlation between the original and extracted watermarks under various irregular attacks and image processing operations. While irregular attacks and processing attacks cause a decrease in the correlation and an increase in the bit error rate, the scheme still maintains a relatively high level of correlation and keeps the bit errors within acceptable limits for most of the tested scenarios. This demonstrates the robustness of the proposed scheme in handling tampering and image processing attacks, shows that proposed scheme can accurately and reliably identify an image's original source.

4.3.4 NC and BER Values for Proposed Scheme

Table 9: NC and BER values of watermarked images after irregular attack combined with image processing attacks.

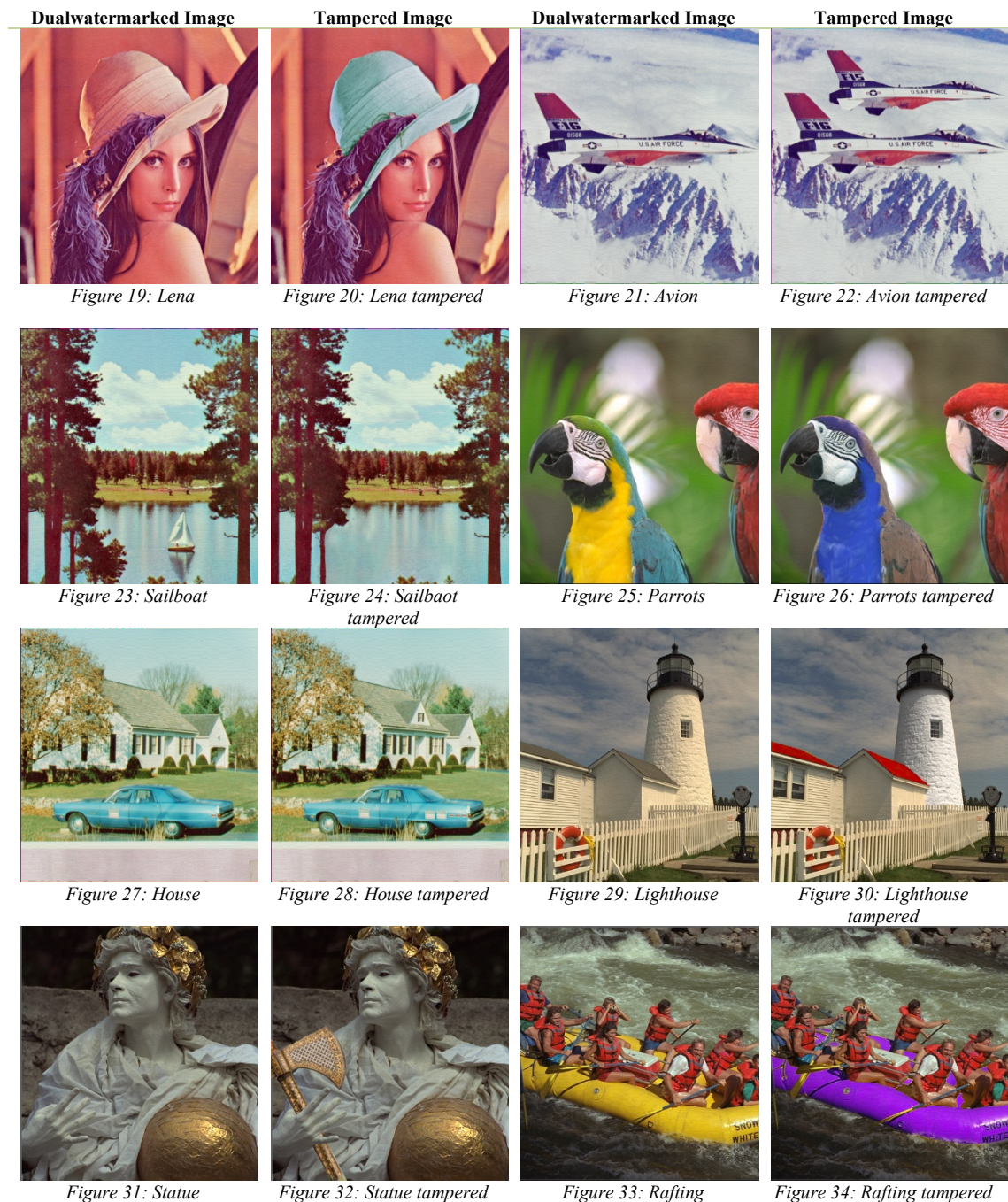
Images		Lena		Avion		Sailboat		Parrots		House		Lighthouse		Statue		Rafting	
Attacks	Density/ Ratio	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER
No Attacks		-															
Gaussian Lowpass Filter	3 x 3	0.9932	0.0068	0.9700	0.0303	0.9652	0.0352	0.9961	0.0039	0.9817	0.0186	0.9941	0.0059	0.8510	0.1494	0.8577	0.1416
	5 x 5	0.9912	0.0088	0.9654	0.0352	0.9576	0.0430	0.9892	0.0107	0.9779	0.0225	0.9902	0.0098	0.7941	0.2051	0.7941	0.2061
	7 x 7	0.9727	0.0273	0.9570	0.0439	0.9083	0.0947	0.9492	0.0498	0.9614	0.0400	0.9202	0.0801	0.6672	0.3203	0.6817	0.3174
Gaussian Noise	0.015	0.7726	0.2266	0.8527	0.1465	0.8190	0.1865	0.6785	0.3184	0.8566	0.1416	0.7448	0.2529	0.6286	0.3682	0.6762	0.3154
	0.01	0.8260	0.1709	0.9036	0.0967	0.8763	0.1250	0.7509	0.2549	0.8813	0.1191	0.8182	0.1777	0.6452	0.3545	0.7149	0.2783
	0.005	0.9188	0.0820	0.9569	0.0430	0.9310	0.0693	0.8263	0.1709	0.9532	0.0469	0.8848	0.1133	0.6898	0.3066	0.7709	0.2217
Speckle noise	0.05	0.7557	0.2383	0.7235	0.2832	0.7273	0.2725	0.7910	0.2090	0.7791	0.2178	0.7773	0.2227	0.7977	0.2031	0.8194	0.1787
	0.25	0.6338	0.3623	0.6126	0.4063	0.6078	0.3857	0.6366	0.3623	0.5754	0.4355	0.6352	0.3691	0.6976	0.3057	0.6583	0.3291
	0.004	0.9892	0.0107	0.9753	0.0244	0.9619	0.0381	0.9567	0.0430	0.9835	0.0166	0.9764	0.0234	0.9054	0.0947	0.9300	0.0684
Salt & Pepper	0.04	0.8220	0.1768	0.8672	0.1328	0.8392	0.1602	0.7458	0.2529	0.8721	0.1299	0.7941	0.2031	0.6687	0.3359	0.6748	0.3184
	0.06	0.7723	0.2305	0.8456	0.1514	0.8090	0.1953	0.7155	0.2754	0.8210	0.1807	0.7463	0.2529	0.6101	0.3857	0.6773	0.3174
	0.012	0.9555	0.0439	0.9532	0.0469	0.9275	0.0723	0.8574	0.1416	0.9564	0.0439	0.9142	0.0859	0.7941	0.2041	0.8485	0.1484
Scaling	1.6	1.0000	0.0000	0.9739	0.0264	0.9766	0.0234	0.9971	0.0029	0.9846	0.0156	0.9971	0.0029	0.9495	0.0498	0.8929	0.1055
	0.5	0.9990	0.0010	0.9728	0.0273	0.9737	0.0264	0.9961	0.0039	0.9827	0.0176	0.9941	0.0059	0.8854	0.1133	0.8771	0.1221
	0.33	0.8993	0.0986	0.9199	0.0801	0.8326	0.1758	0.8793	0.1152	0.8881	0.1104	0.8180	0.1816	0.6200	0.3535	0.6373	0.3623
	0.8	1.0000	0.0000	0.9739	0.0264	0.9786	0.0215	0.9971	0.0029	0.9846	0.0156	0.9980	0.0020	0.9294	0.0693	0.8691	0.1289
Median Filter	2 x 2	0.9903	0.0098	0.9711	0.0293	0.9633	0.0371	0.9932	0.0068	0.9826	0.0176	0.9941	0.0059	0.8430	0.1543	0.8025	0.1943
	3 x 3	1.0000	0.0000	0.9719	0.0283	0.9717	0.0283	0.9961	0.0039	0.9846	0.0156	0.9961	0.0039	0.8558	0.1426	0.8412	0.1582
	4 x 4	0.9449	0.0557	0.9607	0.0400	0.8879	0.1172	0.9342	0.0664	0.9556	0.0459	0.8586	0.1455	0.6756	0.3154	0.6879	0.3193
	5 x 5	0.7396	0.2695	0.7215	0.2939	0.7058	0.2998	0.6938	0.2939	0.7102	0.2861	0.6612	0.3477	0.5177	0.4531	0.5890	0.4229
Sharpening	2	0.9892	0.0107	0.9803	0.0195	0.9726	0.0273	0.9951	0.0049	0.9883	0.0117	0.9971	0.0029	0.9136	0.0859	0.9209	0.0771
Poisson Noise	-	0.9746	0.0254	0.9814	0.0186	0.9601	0.0400	0.9345	0.0645	0.9874	0.0127	0.9698	0.0303	0.8924	0.1074	0.9036	0.0938
Histogram	-	1.0000	0.0000	0.9833	0.0166	0.9738	0.0264	0.9842	0.0156	0.9912	0.0088	0.9951	0.0049	0.9566	0.0430	0.9632	0.0361
Centred Cropping off by black	25 %	0.9951	0.0049	0.9783	0.0215	0.9257	0.0723	0.9862	0.0137	0.9951	0.0049	0.9712	0.0283	0.9390	0.0596	0.9682	0.0313
	50 %	0.9812	0.0186	0.9406	0.0576	0.7679	0.2061	0.9195	0.0771	0.9852	0.0146	0.8737	0.1182	0.9037	0.0918	0.8737	0.1182
Centred Cropping off by white	25 %	0.9961	0.0039	0.9793	0.0205	0.9294	0.0684	0.9872	0.0127	0.9951	0.0049	0.9712	0.0283	0.9438	0.0547	0.9682	0.0313
	50 %	0.9772	0.0225	0.9436	0.0547	0.7567	0.2139	0.9226	0.0742	0.9852	0.0146	0.8747	0.1172	0.9046	0.0908	0.8736	0.1182
Cropping row off by black	50 %	0.6303	0.3008	0.8024	0.1777	0.4971	0.3770	0.6650	0.2783	0.6459	0.2910	0.5596	0.3428	0.4257	0.4092	0.8347	0.1514
	25 %	0.7864	0.1904	0.9205	0.0762	0.7695	0.2041	0.7520	0.2168	0.6623	0.2803	0.7776	0.1973	0.5973	0.3213	0.8792	0.1133
	12.5 %	0.8440	0.1436	0.9581	0.0410	0.8830	0.1104	0.8544	0.1348	0.7989	0.1807	0.9120	0.0840	0.7916	0.1865	0.9290	0.0684

Cropping row off by white	50 %	0.6321	0.2998	0.8024	0.1777	0.4975	0.3770	0.6680	0.2764	0.6416	0.2939	0.5559	0.3457	0.4290	0.4082	0.8382	0.1484
	25 %	0.7902	0.1875	0.9156	0.0811	0.7805	0.1963	0.7458	0.2217	0.6596	0.2822	0.7833	0.1934	0.5995	0.3213	0.8771	0.1152
	12.5 %	0.8375	0.1494	0.9573	0.0420	0.8744	0.1201	0.8462	0.1426	0.8023	0.1797	0.9059	0.0898	0.7947	0.1855	0.9261	0.0713
Cropping column off by black	50 %	0.8157	0.1670	0.7726	0.2012	0.7588	0.2119	0.6825	0.2666	0.7878	0.1895	0.7133	0.2451	0.6768	0.2705	0.6547	0.2852
	25 %	0.8925	0.1016	0.8347	0.1514	0.9553	0.0439	0.7468	0.2207	0.9375	0.0605	0.9034	0.0918	0.7751	0.1992	0.8134	0.1689
	12.5 %	0.9269	0.0703	0.9163	0.0801	0.9584	0.0410	0.8486	0.1396	0.9763	0.0234	0.9457	0.0527	0.8748	0.1172	0.8872	0.1064
Cropping column off by white	50 %	0.8157	0.1670	0.7726	0.2012	0.7588	0.2119	0.6825	0.2666	0.7878	0.1895	0.7133	0.2451	0.6782	0.2695	0.6548	0.2852
	25 %	0.8925	0.1016	0.8347	0.1514	0.9553	0.0439	0.7429	0.2236	0.9375	0.0605	0.9023	0.0928	0.7764	0.1982	0.8145	0.1680
	12.5 %	0.9269	0.0703	0.9163	0.0801	0.9584	0.0410	0.8475	0.1406	0.9763	0.0234	0.9457	0.0527	0.8726	0.1191	0.8862	0.1074
JPEG Compression	80	1.0000	0.0000	0.9787	0.0215	0.9719	0.0283	0.9951	0.0049	0.9745	0.0254	0.9951	0.0049	0.8225	0.1738	0.8238	0.1709
	70	1.0000	0.0000	0.9778	0.0225	0.9679	0.0322	0.9902	0.0098	0.9715	0.0283	0.9912	0.0088	0.7555	0.2285	0.8102	0.1836
	60	0.9971	0.0029	0.9767	0.0234	0.9631	0.0371	0.9424	0.0566	0.9705	0.0293	0.9912	0.0088	0.6368	0.3203	0.7838	0.2100
	50	0.9872	0.0127	0.9758	0.0244	0.9648	0.0352	0.8784	0.1152	0.9705	0.0293	0.9596	0.0400	0.5751	0.3584	0.7646	0.2305
	40	0.9520	0.0469	0.9748	0.0254	0.9482	0.0518	0.6489	0.2969	0.9696	0.0303	0.8845	0.1113	0.4714	0.4238	0.7340	0.2568
	30	0.7852	0.1943	0.9721	0.0283	0.9215	0.0771	0.3238	0.4736	0.9556	0.0439	0.6493	0.3037	0.4348	0.4453	0.6760	0.3008
JPEG2000	2	1.0000	0.0000	0.9787	0.0215	0.9708	0.0293	0.9971	0.0029	0.9705	0.0293	0.9980	0.0020	0.8889	0.1113	0.8319	0.1641
Compression	4	1.0000	0.0000	0.9787	0.0215	0.9680	0.0322	0.9971	0.0029	0.9695	0.0303	0.9980	0.0020	0.8939	0.1055	0.8353	0.1611
AVERAGE		0.8469	0.1471	0.8541	0.1409	0.8288	0.1623	0.7982	0.1847	0.8449	0.1458	0.8233	0.1670	0.7097	0.2622	0.7678	0.2252

Table 9 shows the average Normalized Correlation (NC) and Bit Error Rate (BER) of proposed dual watermarking scheme under irregular tamper combined with various image processing attacks. The NC measures the similarity between the original watermark logo and the extracted watermark logo, while the BER measures the bit error rate of the embedded watermark. Based on the table, proposed scheme output fairly recognizable extracted watermark logo under the tested attacks, as the average NC values are high (ranging from 0.7097 to 0.8541) and the average BER values are low (ranging from 0.1409 to 0.2622). This indicates that the embedded watermark can withstand various image processing attacks and still be reliably extracted from the watermarked image.

4.4 Tamper Localization

Tampering of image is known as intentionally modifying an image without authorization by the owner of the image, this act commonly used for malicious intent. Splicing, copy-move, or picture synthesis are a few examples of techniques that can be used to manipulate images. However, within the proposed algorithm, tamper detection function of proposed scheme can further assure the validity and integrity of a picture, also known as image authentication. Using proposed algorithms, location of image tampering can be spotted, hence, several parameters detected tamper such as TPR, FPR, TNR, TPR, precision, f1-score and accuracy can be examined.



4.4.1 Tamper Localization Result

Table 10: Tamper localization result for 8 host images.

Watermarked images	Irregular attacks	Tampering rates	TPR	FNR	FPR	TNR	Precision	F-1 Score	Accuracy
Lena	Filter Manipulation	15.0817 %	0.9860	0.0140	0.0139	0.9861	0.9861	0.9861	0.9861
Avion	Copy Move	6.9278 %	0.9736	0.0264	0.0085	0.9915	0.9913	0.9824	0.9902
Sailboat	Object Removal	9.6042 %	0.9384	0.0616	0.0062	0.9938	0.9935	0.9651	0.9885
Parrots	Colour Correction	21.7960 %	0.9408	0.0592	0.0068	0.9932	0.9928	0.9661	0.9818
House	Copy Move	2.3342 %	0.9436	0.0564	0.0060	0.9940	0.9937	0.9680	0.9928
Lighthouse	Copy Move + Retouching	12.2001 %	0.9375	0.0625	0.0139	0.9861	0.9854	0.9609	0.9802
Statue	Splicing	6.3629 %	0.9547	0.0453	0.0085	0.9915	0.9912	0.9726	0.9892
Rafting	Retouching	14.0862 %	0.9710	0.0290	0.0232	0.9768	0.9766	0.9738	0.9759

The comparison of several forms of attacks on watermarked images can be seen in the *Table 10* above. The table lists the irregular attacks attempted on the images, such as object removal, copy move, filter manipulation, colour correction, splicing, and retouching. All images have tampering rates ranging from 2.3342% to 21.796%.

The efficiency of the watermarking method differs for various tampering attacks and watermarked photos, as shown in the table. The copy move attack on the Avion picture, for instance, has a greater FPR than other attacks but a lower tampering rate than other attacks. However, the watermarking technique is able to achieve high TPR, FPR, and overall performance measures like F-1 score and accuracy, whereas the filter manipulation attack on the Lena image has a higher tampering rate. The analysis of the watermarked images subjected to irregular attacks provides valuable insights into the performance of the watermark tamper localization.

The Lena image underwent filter manipulation at a tampering rate of 15.0817%. The detection system exhibits excellent performance, with a high true positive rate (TPR) of 0.9860, indicating accurate identification of tampered regions. The false negative rate (FNR) is low at 0.0140, implying minimal missed detections. The false positive rate (FPR) and true negative rate (TNR) are both low at 0.0139 and 0.9861, respectively, showcasing accurate identification of non-tampered regions. The precision, F-1 score, and accuracy all stand at 0.9861, emphasizing the effectiveness of the system in detecting filter manipulation in the Lena image.

For the Avion image subjected to copy-move tampering at a rate of 6.9278%, the tamper localization of proposed scheme performs impressively. It achieves a high TPR of 0.9736, indicating its ability to accurately detect instances of copy-move tampering. The FNR remains low at 0.0264, indicating a small number of missed detections. The FPR is also low at 0.0085, suggesting a low rate of false alarms. The TNR is high at 0.9915, reflecting accurate identification of non-tampered regions. The precision of 0.9913 indicates a high level of accuracy in identifying the tampered regions. The F-1 score of 0.9824 represents a balanced performance between precision and recall. The overall accuracy is 0.9902, further highlighting the effectiveness of the tamper localization of proposed scheme in detecting copy-move tampering in the Avion image.

In the case of the Sailboat image, which was subjected to object removal tampering at a rate of 9.6042%, the tamper localization of proposed scheme demonstrates commendable performance. It achieves a TPR of 0.9384, indicating its ability to detect instances of object removal tampering. However, the FNR of 0.0616 suggests a moderate number of missed detections. The FPR remains low at 0.0062, indicating a low rate of false alarms. The TNR is high at 0.9938, indicating accurate identification of non-tampered regions. The precision of 0.9935 suggests a high level of accuracy in identifying the tampered regions. The F-1 score of 0.9651 represents a balanced performance between precision and recall. The accuracy of 0.9885 further indicates the overall effectiveness of the tamper localization of proposed scheme in detecting object removal tampering in the Sailboat image.

The Parrots image underwent colour correction tampering at a rate of 21.7960%. The tamper localization of proposed scheme achieves a TPR of 0.9408, indicating its ability to detect instances of colour correction tampering. The FNR of 0.0592 suggests a moderate number of missed detections. The FPR of 0.0068 implies a low rate of false alarms. The TNR is high at 0.9932, reflecting accurate identification of non-tampered regions. The precision of 0.9928 and the F-1 score of 0.9661 indicate a high level of accuracy and balanced performance between precision and recall. The accuracy is 0.9818, highlighting the overall effectiveness of the tamper localization of proposed scheme in detecting color correction tampering in the Parrots image.

The House image underwent copy-move tampering at a low rate of 2.3342%. The tamper localization of proposed scheme demonstrates excellent performance, achieving a TPR of 0.9436 and a low FNR of 0.0564, indicating accurate detection of copy-move tampering. The FPR is low at 0.0060, suggesting a low rate of false alarms. The TNR is high at 0.9940, reflecting accurate identification of non-tampered regions. The precision of 0.9937 demonstrates a high level of accuracy in identifying the tampered regions. The F-1 score of 0.9680 represents a balanced performance between precision and recall. The overall accuracy of 0.9928 emphasizes the effectiveness of the tamper localization of proposed scheme in detecting copy-move tampering in the House image.

The Lighthouse image was subjected to a combination of copy-move and retouching tampering at a tampering rate of 12.2001%. The tamper localization of proposed scheme performs well, achieving a TPR of 0.9375, indicating accurate detection of the tampered regions. The FNR of 0.0625 suggests a moderate number of missed detections. The FPR of 0.0139 implies a low rate of false alarms. The TNR is 0.9861, reflecting accurate identification of non-tampered regions. The precision of 0.9854 indicates a high level of accuracy in identifying the tampered regions. The F-1 score of 0.9609 represents a balanced performance between precision and recall. The accuracy of 0.9802 further highlights the effectiveness of the tamper localization of proposed scheme in detecting combined copy-move and retouching tampering in the Lighthouse image.

In the case of the Statue image, which underwent splicing tampering at a rate of 6.3629%, the tamper localization of proposed scheme demonstrates strong performance. It achieves a TPR of 0.9547, indicating accurate detection of splicing tampering. The FNR is low at 0.0453, implying a small number of missed detections. The FPR is low at 0.0085, suggesting a low rate of false alarms. The TNR is high at 0.9915, reflecting accurate identification of non-tampered regions. The precision of 0.9912 indicates a high level of accuracy in identifying the tampered regions. The F-1 score of 0.9726 represents a balanced performance between precision and recall. The accuracy of 0.9892 further emphasizes the effectiveness of the tamper localization of proposed scheme in detecting splicing tampering in the Statue image.

Lastly, the Rafting image was subjected to retouching tampering at a tampering rate of 14.0862%. The tamper localization of proposed scheme demonstrates robust performance, achieving a high TPR of 0.9710, indicating accurate detection of retouched regions. The FNR is low at 0.0290, suggesting a minimal number of missed detections. The FPR of 0.0232 implies a relatively higher rate of false alarms compared to other images. The TNR is 0.9768, reflecting accurate identification of non-tampered regions. The precision of 0.9766 indicates a high level of accuracy in identifying the tampered regions. The F-1 score of 0.9738 represents a balanced performance between precision and recall. The accuracy of 0.9759 further highlights the overall effectiveness of the tamper localization of proposed scheme in detecting retouching tampering in the Rafting image.

With high TPR and overall performance measures, the watermarking method generally seems to be the most effective in identifying splicing and retouching attacks. The detection of colour correction and object removal assaults, however, is less effective. The colour correction and object removal attacks, which have a higher FNR and weaker overall performance metrics, are harder to detect. In summary, the proposed approach demonstrates strong performance across various irregular attacks and tampering scenarios. It shows high detection rates, low false negatives, and accurate identification of non-tampered regions. The precision, F-1 score, and accuracy values reflect the system's effectiveness in detecting tampering in the watermarked images. These results highlight the system's potential. However, It's crucial to remember that these findings are exclusive to the proposed scheme or styles of tampering attacks.

4.4.2 Tamper Localization Comparison



Figure 35: Host Image (Avion)



Figure 36: Tampered Image



Figure 37: Actual Tampered Region



Figure 38: Tamper Detected (Proposed)



Figure 39: Detected Region (Proposed)



Figure 40: False Positive Region (Proposed)



Figure 41: Tamper Detected (Duan et al., 2020)



Figure 42: Detected Region (Duan et al., 2020)



Figure 43: False Positive Region (Duan et al., 2020)

Table 11: Tamper localization parameters comparison of proposed scheme and (Duan et al., 2020)'s scheme.

Watermarked images	Irregular attacks	Tampering rates	TPR	FNR	FPR	TNR	Precision	F-1 Score	Accuracy
Avion (Proposed)	Copy Move	6.9278 %	0.9736	0.0264	0.0085	0.9915	0.9913	0.9824	0.9902
Avion (Duan et al., 2020)	Copy Move	6.9278 %	1.0000	0.0000	0.0315	0.9685	0.9694	0.9845	0.9707

Table 11 above compares the tamper localization performance of two dual watermarking scheme, the proposed scheme and scheme proposed by Duan et al. Both algorithms are tested using copy-move tampering attacks on the Avion image. The table shows that in terms of TPR, FNR, FPR, Precision, F1 Score, and Accuracy, the proposed method performs better than scheme proposed by Duan et al. Despite proposed approach specifically obtains a lower TPR and a higher FNR, but it can identify lower FPR and higher TNR, thus, it is more precise at identifying tampered regions and detects fewer false positive region compared to scheme proposed by Duan et al.

Additionally, the proposed algorithm attains higher Precision and Accuracy, demonstrating that it is better in correctly distinguishes between tampered and untampered regions and has fewer false positives. That said, a good fragile watermark embedding algorithm should, in general, have high values for all three metrics: Precision, F1 Score, and Accuracy. Thus, the algorithm is efficient at identifying tampered regions while minimizing false positives and false negatives.

CHAPTER 5

CONCLUSION

5.1 Introduction

Chapter 5 will discuss the summarization of finding of proposed approach on the Secure and effective image authentication and copyright protection using IWT dual watermarking, in order to achieve the objectives and overcome the problem statement mentioned in Chapter 1. In this modern age with full edge technologies, copyright and authentication of multimedia data such as images can be easily exploit. The proposed approach supply a set of algorithm to hinder the exploitation of copyright and examine the authentication of the image. Therefore, internet user such as photographer or artist can protect the copyright and authentication of their image form artwork or captured images by applying the proposed dual watermarking scheme which is developed using MATLAB IDE software. This dual watermark approach allows the embedding of owner's logo to preserve the ownership better and embeds authentication bits to identify if the images are modified. The approach is developed and examined by using image processing evaluation parameter such as PSNR, ARE, SSIM to justify the rate of distortion-proof of the image and TPR, FPR, TNR, FNR, precision, accuracy, and f1-score to study the rate of tamper when the original is modified. The evaluation result shows results against existing dual watermarking approach that consist of copyright protection and image authentication. Conclusion, new implementation of dual watermarking obtains better watermarked image with higher resolution, lower rate of image quality distortion, and accuracy on determining the tampered region. The imperceptibility, robustness, and tamper localization for authentication and copyright protection using the proposed watermarking method, in comparison to benchmark of other existing watermarking method shows a positive result.

5.2 Research Constraint

During the process of completing this thesis, a few constraints were identified and jotted down as shown as below:

Limited background knowledge, the topic of secure image authentication and copyright protection requires a solid understanding of image processing techniques, watermarking algorithms, and concepts related to information security. To cope with the issue, it is important to build foundational knowledge in image processing, watermarking techniques, and information security through online courses, tutorials, and textbooks.

Access to resources, conducting research often requires access to relevant literature, scholarly articles, research papers, and other resources. Accessing these resources may require subscription fees or institutional access, which can be a constraint for beginners who do not have such privileges. To solve this constraint, it is crucial to utilize open-access resources like research publications, preprints, and online forums to gather information and stay up-to-date with the latest developments in the field.

Technical expertise, implementing and evaluating an image authentication and copyright protection system using the IWT dual watermarking approach can be technically challenging. It may require proficiency in programming languages (such as MATLAB, Python, or C++), understanding image processing libraries, and working with mathematical concepts related to wavelet transforms and dual watermarking. Practice makes perfect, it is notable that practice implementing existing watermarking algorithms and understanding their performance could be a big help.

Overall, it tooks some time to start understanding the flow of watermark embedding, the logic and purpose behind every line of code and built in function that will assist in building this algorithm. Although dual watermarking studies has been available previously even before this research was done, but there are many methods expert uses to perform dual watermarking algorithm to serve as a tool of copyright protection and image authentication. It requires alot of thesis and paper studying to understand the core concepts of dual watermarking. Thus, to further this research, it is important to understand the basic concept of dual watermarking seek help from the expert such as lecturer who is familiar with this scene of studies.

5.3 Future work

There are several enhancements that can be applied for future improvement of dual watermarking approach proposed.

i. Improved Robustness: One possible enhancement for the dual watermarking approach is to enhance its robustness against various attacks. This can be achieved by incorporating advanced digital watermarking techniques that are resilient to common attacks such as image compression, filtering, and cropping. By enhancing the robustness, the dual watermarking approach can ensure that the embedded watermarks remain detectable and intact even in the presence of intentional or unintentional image alterations.

ii. Multi-Domain Watermarking: Another enhancement could involve expanding the dual watermarking approach to support multiple domains. Currently, the approach may be designed for a specific domain, such as images or videos. However, extending it to support additional domains, such as audio or documents, would broaden its applicability and usefulness. This expansion would involve adapting and integrating watermarking techniques suitable for each domain while maintaining the overall integrity and synchronization between the dual watermarks.

iii. Security and Authentication: Enhancing the security and authentication aspects of the dual watermarking approach is crucial. This can involve exploring encryption techniques to protect the embedded watermarks, ensuring that only authorized entities can access or modify them. Additionally, incorporating robust authentication mechanisms can help verify the authenticity and integrity of the watermarked content, preventing unauthorized alterations or tampering. By strengthening the security and authentication measures, the dual watermarking approach can provide increased trustworthiness and protection for the watermarked content.

iv. Embedding Metadata: An additional enhancement could involve embedding metadata within the dual watermarks. This metadata can include information such as copyright details, authorship, timestamps, or other relevant data associated with the watermarked content. By embedding metadata, the approach can facilitate easier identification, management, and tracking of the watermarked content, which can be valuable for copyright protection, content tracking, and content ownership verification.

v. Deep Learning Techniques: Incorporating deep learning techniques, such as convolutional neural networks (CNNs) or generative adversarial networks (GANs), can be explored for improved detection and extraction of the dual watermarks. These advanced techniques can enhance the accuracy and efficiency of watermark detection algorithms, enabling more reliable and precise extraction of watermarks from the watermarked content.

vi. Adaptive Watermarking: Implementing adaptive watermarking techniques can provide flexibility and customization in the dual watermarking approach. This would allow the watermarks to be adapted or modified based on specific requirements or scenarios. Adaptive watermarking can involve techniques such as embedding multiple watermarks with different characteristics, adjusting embedding strength based on content characteristics, or dynamically altering watermarking parameters for optimal performance in different contexts.

REFERENCES

- 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>
- Anand, A., & Singh, A. K. (2020). RDWT-SVD-Firefly Based Dual Watermarking Technique for Medical Images (Workshop Paper). *Proceedings - 2020 IEEE 6th International Conference on Multimedia Big Data, BigMM 2020*, 366–372. <https://doi.org/10.1109/BigMM50055.2020.00063>
- Bhargava, N., Sharma, M. M., Garhwal, A. S., & Mathuria, M. (2012). Digital image authentication system based on digital watermarking. *2012 International Conference on Radar, Communication and Computing, ICRCC 2012*, 185–189. <https://doi.org/10.1109/ICRCC.2012.6450573>
- 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., Aminuddin, A., Nincarean, D., Razak, M. F. A., & Firdaus, A. (2022). Three Layer Authentications with a Spiral Block Mapping to Prove Authenticity in Medical Images. *International Journal of Advanced Computer Science and Applications*, 13(4), 211–223. <https://doi.org/10.14569/IJACSA.2022.0130425>
- Ernawan, F., & Kabir, M. N. (2020a). A block-based RDWT-SVD image watermarking method using human visual system characteristics. *Visual Computer*, 36(1), 19–37. <https://doi.org/10.1007/s00371-018-1567-x>
- Ernawan, F., & Kabir, M. N. (2020b). A block-based RDWT-SVD image watermarking method using human visual system characteristics. *Visual Computer*, 36(1), 19–37. <https://doi.org/10.1007/s00371-018-1567-x>
- Ernawan, F., Liew, S. C., Mustaffa, Z., & Moorthy, K. (2018). A blind multiple watermarks based on human visual characteristics. *International Journal of Electrical and Computer Engineering*, 8(4), 2578–2587. <https://doi.org/10.11591/ijece.v8i4.pp2578-2587>
- Hadjer, A., & Ismail, B. H. (2022). A Dual Image Watermarking Scheme Based on WPT and Chaotic Encryption for Medical Data Protection. *2022 7th International Conference on Image and Signal Processing and Their Applications, ISPA 2022 - Proceedings*. <https://doi.org/10.1109/ISPA54004.2022.9786355>
- Han, S., Lv, M., & Cheng, Z. (2022). Dual-color blind image watermarking algorithm using the graph-based transform in the stationary wavelet transform domain. *Optik*, 268. <https://doi.org/10.1016/j.ijleo.2022.169832>
- Hurrah, N. N., Parah, S. A., Loan, N. A., Sheikh, J. A., Elhoseny, M., & Muhammad, K. (2019). Dual watermarking framework for privacy protection and content authentication of multimedia. *Future Generation Computer Systems*, 94, 654–673. <https://doi.org/10.1016/j.future.2018.12.036>

- Kamili, A., Hurrah, N. N., Parah, S. A., Bhat, G. M., & Muhammad, K. (2021). DWFCAT: Dual Watermarking Framework for Industrial Image Authentication and Tamper Localization. *IEEE Transactions on Industrial Informatics*, 17(7), 5108–5117. <https://doi.org/10.1109/TII.2020.3028612>
- 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>
- Lee, Y., Kim, H., & Park, Y. (2009). A new data hiding scheme for binary image authentication with small image distortion. *Information Sciences*, 179(22), 3866–3884. <https://doi.org/10.1016/j.ins.2009.07.014>
- Li, Z., Zhang, H., Liu, X., Wang, C., & Wang, X. (2021). Blind and safety-enhanced dual watermarking algorithm with chaotic system encryption based on RHF and DWT-DCT. *Digital Signal Processing: A Review Journal*, 115. <https://doi.org/10.1016/j.dsp.2021.103062>
- LUSIA RAKHMAWATI¹, WIRAWAN¹, (Member, IEEE), SUWADI¹, CLAUDE DELPHA³, (Member, IEEE), AND PIERRE DUHAMEL. (2020). Dual Watermarking Schemes for Image Authentication and Copyright Protection with Recovery Capability. <https://doi.org/10.1109/ACCESS.2017.DoI>
- Mokashi, B., Bhat, V. S., Pujari, J. D., & Lalith Sagar, J. (2021). Dual Watermarking Technique for Image Authentication using Biometrics. *2021 IEEE Mysore Sub Section International Conference, MysuruCon 2021*, 427–432. <https://doi.org/10.1109/MysuruCon52639.2021.9641721>
- Sepúlveda, J., Sepúlveda, S., & Velastín, S. A. (n.d.). *F1 Score Assesment of Gaussian Mixture Background Subtraction Algorithms Using the MuHAVi Dataset*.
- Singh, P., & Raman, B. (2017). A secured robust watermarking scheme based on majority voting concept for rightful ownership assertion. *Multimedia Tools and Applications*, 76(20), 21497–21517. <https://doi.org/10.1007/s11042-016-4006-x>
- Su, Q., Niu, Y., Liu, X., & Zhu, Y. (2012a). A blind dual color images watermarking based on IWT and state coding. *Optics Communications*, 285(7), 1717–1724. <https://doi.org/10.1016/j.optcom.2011.11.117>
- Su, Q., Niu, Y., Liu, X., & Zhu, Y. (2012b). A blind dual color images watermarking based on IWT and state coding. *Optics Communications*, 285(7), 1717–1724. <https://doi.org/10.1016/j.optcom.2011.11.117>
- Tiwari, A., & Srivastava, V. K. (2022). Integer Wavelet Transform and Dual Decomposition Based Image Watermarking scheme for Reliability of DICOM Medical Image. *2022 IEEE 9th Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON)*, 1–6. <https://doi.org/10.1109/UPCON56432.2022.9986427>

APPENDIX A