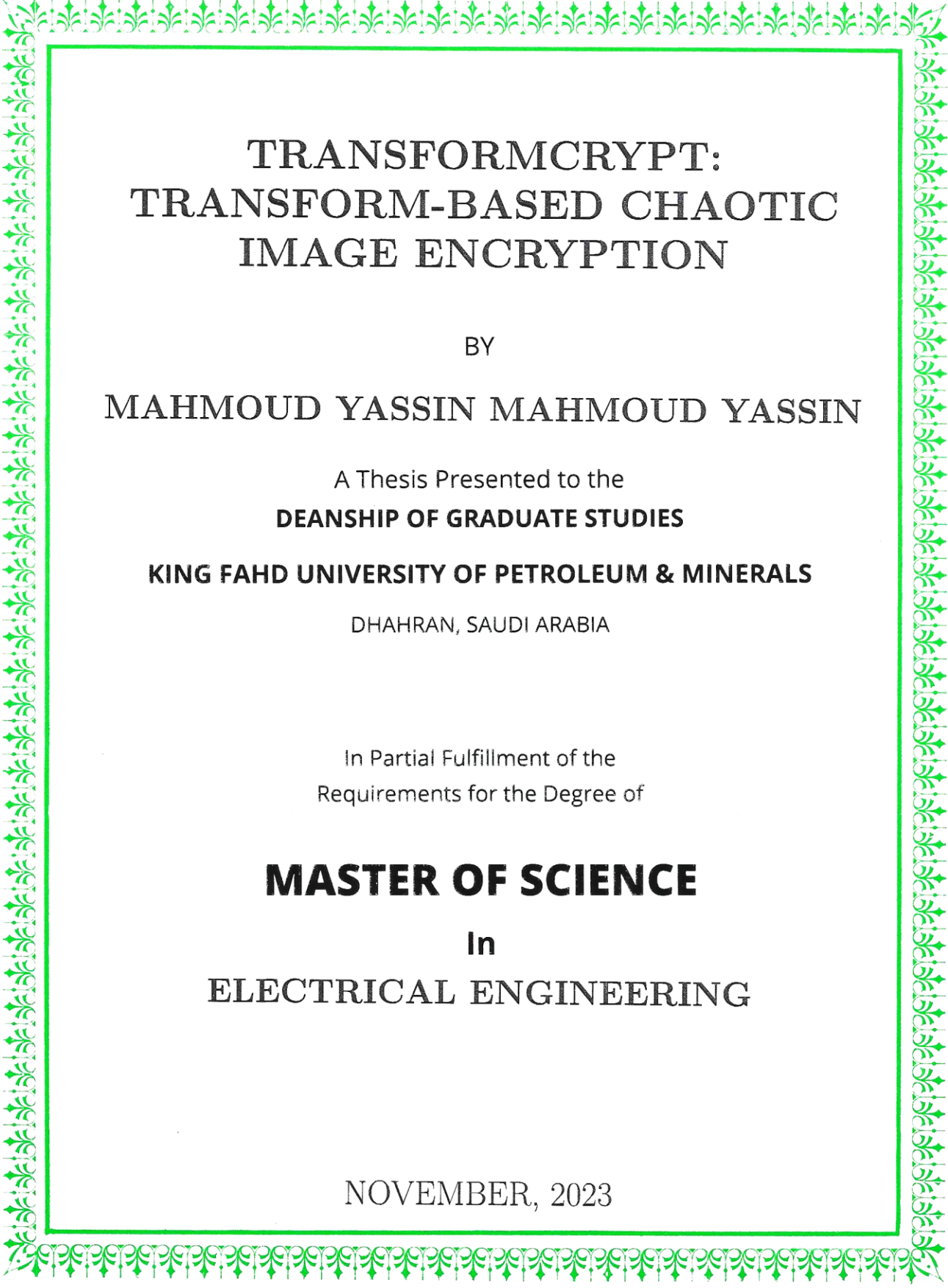




TRANSFORMCRYPT: TRANSFORM-BASED CHAOTIC IMAGE ENCRYPTION

BY

MAHMOUD YASSIN MAHMOUD YASSIN

A Thesis Presented to the
DEANSHIP OF GRADUATE STUDIES

KING FAHD UNIVERSITY OF PETROLEUM & MINERALS

DHAHRAN, SAUDI ARABIA

In Partial Fulfillment of the
Requirements for the Degree of

MASTER OF SCIENCE
In
ELECTRICAL ENGINEERING

NOVEMBER, 2023

KING FAHD UNIVERSITY OF PETROLEUM & MINERALS
DHAHRAN 31261, SAUDI ARABIA

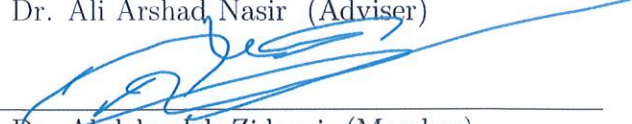
DEANSHIP OF GRADUATE STUDIES

This thesis, written by **MAHMOUD YASSIN MAHMOUD YASSIN** under the direction of his thesis adviser and approved by his thesis committee, has been presented to and accepted by the Dean of Graduate Studies, in partial fulfillment of the requirements for the degree of **MASTER OF SCIENCE IN ELECTRICAL ENGINEERING**.

Thesis Committee



Dr. Ali Arshad Nasir (Adviser)



Dr. Abdelmalek Zidouri (Member)



Dr. Mudassir Masood (Member)



Dr. Naveed Iqbal (Member)



Dr. Md Mahfuzur Rahman (Member)



Dr. Mohammad Mustafa

Al-Muhaini

Department Chairman



Prof. Suliman Saleh Al-

Homidan

Dean of Graduate Studies



Date

©Mahmoud Yassin
2023

To the person who stood by my side during all of life's challenges, my dearest friend who had faith in me when I lacked it in myself, the one who knows the untold stories of my life. To Mohamed Mostafa.

ACKNOWLEDGMENTS

I wish to convey my deep gratefulness to my esteemed supervisor, Dr. Ali Arshad Nasir, for his invaluable guidance, and boundless patience throughout the entirety of my research journey. Dr. Nasir's expertise, insights, and feedback have been pivotal in shaping the scope and direction of my thesis, leaving a lasting impact on my academic and professional pursuits. Additionally, I would like to convey my sincere thanks to all the members of my thesis committee for their valuable contributions and guidance. I want also to show my profound gratefulness to my father and friends. Their unwavering faith in my capabilities has been the driving passion behind my accomplishments. Furthermore, I extend my heartfelt acknowledgments to KFUPM for their generous financial support, which made it possible for me to pursue my graduate studies and successfully complete my thesis. Their investment in my education and future prospects has been truly invaluable, and I am deeply thankful for their continued support.

TABLE OF CONTENTS

ACKNOWLEDGMENTS	vi
LIST OF TABLES	xi
LIST OF FIGURES	xiii
LIST OF ABBREVIATIONS	xv
ABSTRACT (ENGLISH)	xvii
ABSTRACT (ARABIC)	xix
CHAPTER 1 INTRODUCTION	1
1.1 Preface	1
1.2 Problem Statement	3
1.3 Research Objectives	3
1.4 Organization of the Thesis	4
CHAPTER 2 BACKGROUND	6
2.1 Preface	6
2.2 Transformation Domain	6
2.2.1 Two-Dimensional Discrete Fourier Transform	6
2.2.2 Integer to Integer Wavelet Transform	7
2.3 Chaotic Maps	8
2.3.1 Two-Dimensional Chaotic Baker Map	9
2.3.2 One-Dimensional Logistic Map	10

2.3.3	Enhanced One-Dimensional Logistic Map	11
2.4	Basic Encryption Concepts	13
2.4.1	Symmetric-Key Cryptosystems	13
2.4.2	Block Cipher Cryptosystems	16
2.4.3	Image Cryptosystems	17
CHAPTER 3 TRANSFORM-BASED CHAOTIC IMAGE ENCRYP-		
TION		19
3.1	Preface	19
3.2	Chaotic Image Encryption in Spatial Domain	21
3.3	Chaotic Image Encryption Using Discrete Fourier Transform	22
3.4	Chaotic Image Encryption Using Discrete Wavelet Transform	23
3.5	Dual-Domain Chaotic Image Encryption	25
CHAPTER 4 ENHANCED DFT-BASED CHAOTIC IMAGE		
BLOCK CIPHER WITH SEVERAL MODES OF OPERATION		27
4.1	Preface	27
4.2	Proposed Enhanced Cryptosystem Scheme	29
4.2.1	Proposed Enhanced Cryptosystem in the Modified CBC Mode .	33
4.2.2	Proposed Enhanced Cryptosystem in the Modified CFB Mode .	34
4.2.3	Proposed Enhanced Cryptosystem in the Modified OFB Mode .	35
4.3	Simulation Results	36
4.3.1	Visual Test	36
4.3.2	Histogram Visualization	36
4.3.3	Correlation Coefficient Test	39
4.3.4	Histogram Deviation Test	39
4.3.5	Irregular Deviation Test	41
4.3.6	Information Entropy Test	42
4.3.7	Differential Analysis	42
4.3.8	Detailed Comparison with Existing Techniques	43
4.4	Chapter Summary	45

CHAPTER 5	NOVEL DUAL-DOMAIN CHAOTIC IMAGE CRYPTOSYSTEM FOR CYBERSECURITY APPLICATIONS	46
5.1	Preface	46
5.2	Proposed Dual-Domain Chaotic Image Cryptosystem	48
5.2.1	Generation of Chaotic Variables	48
5.2.2	Encryption Scheme for Proposed Dual-Domain Cryptosystem	53
5.2.3	Decryption Scheme for Proposed Dual-Domain Cryptosystem	62
5.2.4	Discussion	63
5.3	Simulation Results	65
5.3.1	Visual Test	66
5.3.2	General Correlation Coefficient Test	66
5.3.3	Correlation Coefficient of Adjacent Pixels	68
5.3.4	Correlation Coefficient between Plain and Ciphared Images	71
5.3.5	Histogram Visualization	73
5.3.6	Chi-Square Test	74
5.3.7	Uniformity Deviation Test	75
5.3.8	Histogram Deviation Test	77
5.3.9	Irregular Deviation Test	78
5.3.10	Mean Square Error Test	80
5.3.11	Global Entropy Test	81
5.3.12	Differential Analysis	83
5.3.13	Analysis of Ciphared Image Randomness	87
5.3.14	Immunity Analysis Against Cryptanalytic Attacks	87
5.3.15	Time Consumption Analysis	90
5.3.16	Comparative Analysis of Dual-Domain Chaotic Image Cryptosystem with Different Wavelets	92
5.4	Chapter Summary	93
CHAPTER 6	CONCLUSIONS & RECOMMENDATIONS	95
6.1	Conclusions	95

6.2 Recommendations	97
REFERENCES	99
VITAE	116

LIST OF TABLES

4.1	Visual test for the encryption and decryption process for the "Mandrill" image using the DFT-Baker and the proposed enhanced cryptosystem operates in several modes with various block sizes.	37
4.2	Histogram results for plain image, and ciphered images operates in several modes for the "Mandrill" image.	38
4.3	Correlation coefficient results between plain and ciphered image pixels for the "Mandrill" image operates in several modes with various block sizes.	40
4.4	Histogram deviation results	40
4.5	Irregular deviation results	41
4.6	Information entropy results	42
4.7	Lena image comparison with literature	44
5.1	Visual test for the encryption and decryption process for multiple images	67
5.2	General correlation coefficient results between plain images with different sizes and their corresponding ciphered ones.	69
5.3	General correlation coefficient results between plain and ciphered image pixels for the "Lena" image compared with the literature.	69
5.4	Results for correlation coefficients of adjacent pixels for multiple ciphered images.	70
5.5	Results for correlation coefficients of adjacent pixels for the ciphered version of "Cameraman" image compared with the literature	71
5.6	Results for correlation coefficients between plain images and their corresponding ciphered images pixels	72

5.7	Results for the coefficients of correlation between plain and ciphered pixels for the "Peppers" image compared with the literature.	73
5.8	Histogram distribution results for multiple plain images, and their corresponding ciphered ones	74
5.9	Chi-square test results.	75
5.10	Chi-square test results of the ciphered version of the "Peppers" image comparing the proposed cryptosystem with existing literature.	76
5.11	Uniformity deviation results for different grayscale test images.	77
5.12	Uniformity deviation test results of the ciphered version of the "Peppers" image comparing the proposed cryptosystem with existing literature.	78
5.13	Histogram deviation results for different test images	79
5.14	Irregular deviation results for different test images	80
5.15	Mean Square Error (MSE).	81
5.16	Mean Square Error (MSE) test results of the ciphered version of the "Mandrill" image comparing the proposed cryptosystem with existing literature.	81
5.17	Global entropy results for different test images	83
5.18	The Global Entropy results for the ciphered version of "Lena" image compared with the literature	83
5.19	UACI and NPCR results for different ciphered images	86
5.20	Comparison between proposed dual-domain cryptosystem and its corresponding in literature in terms of UACI and NPCR results	86
5.21	Tests' results of randomness for the ciphered 512×512 "Mandrill" image.	88
5.22	Time consumption results for multiple test images.	92
5.23	Time consumption test results performed on 256×256 "Lena" image comparing the proposed cryptosystem with existing literature.	92
5.24	Comparative Analysis of Dual-Domain Chaotic Image Cryptosystem with Different Wavelets	93

LIST OF FIGURES

2.1	A 2-level Integer to Integer Wavelet Transform (IIWT) decomposition.	9
2.2	The 2D Baker map encryption process of an 8×8 matrix with $key = (4, 2, 2)$.	10
2.3	Bifurcation diagram for the chaotic standard logistic map.	12
2.4	Bifurcation diagram for the enhanced logistic map in [1].	13
2.5	Basic encryption topology for a communication network. [2].	14
2.6	Simplified illustration of a symmetric-key-based cryptosystem[2].	14
3.1	The different research perspectives in image encryption using chaotic maps.	20
4.1	Basic encryption E_{k1} and decryption D_{k1} block diagrams adapted from [3].	28
4.2	The proposed enhanced image cryptosystem operating in various modes.	30
4.2	The proposed enhanced image cryptosystem operating in various modes.	31
4.2	The proposed enhanced image cryptosystem operating in various modes.	32
5.1	The proposed dual-domain image cryptosystem scheme.	55
5.1	The proposed dual-domain image cryptosystem scheme.	56
5.2	Results for the "All White" and "All Black" images and their ciphered version.	91

LIST OF ABBREVIATIONS

1D	One-Dimensional
1D-DFT	One-Dimensional Discrete Fourier Transform
2D	Two-Dimensional
2D-DFT	Two-Dimensional Discrete Fourier Transform
2D-IDFT	Two-Dimensional Inverse Discrete Fourier Transform
3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
Bior3.7	Biorthogonal 3.7 Wavelet
CBC	Cipher Block Chaining Mode
CFB	Cipher Feedback Mode
DES	Data Encryption Standard
DFT	Discrete Fourier Transform
DNA	Deoxyribonucleic acid
DWT	Discrete Wavelet Transform
FrFT	Fractional Fourier Transform
HH	High-High pass subband

HL	High-Low pass subband
IIWT	Integer to Integer Wavelet Transform
IV	Initial Vector
LH	Low-High pass subband
LL	Low-Low pass subband
MCBC	Modified Cipher Block Chaining Mode
MCFB	Modified Cipher Feedback Mode
NIST	National Institute of Standards and Technology
NPCR	Number of Pixels Change Rate
OFB	Output Feedback Mode
RC4	Rivest Cipher 4
RC5	Rivest Cipher 5
UACI	Unified Average Changing Intensity

THESIS ABSTRACT

NAME: Mahmoud Yassin Mahmoud Yassin

TITLE OF STUDY: TransformCrypt: Transform-Based Chaotic Image Encryption

MAJOR FIELD: Electrical Engineering

DATE OF DEGREE: November, 2023

Preserving the confidentiality of multimedia data remains a critical concern within the cybersecurity domain, growing in significance with the continuous evolution of multimedia applications. This thesis delves into the realm of chaotic image ciphers as a probable solution to this pressing problem. Previous research has explored chaotic image encryption in various transformation domains, such as spatial, Discrete Fourier Transform (DFT), and Wavelet Transform. Despite the favorable confusion properties of the frequency-based cryptosystems, they exhibit deficiencies in diffusion characteristics and susceptibility to some statistical tests, rendering them susceptible to various attacks. In response to these challenges, this thesis introduces two innovative solutions. The first work presents an enhanced block cipher image cryptosystem, incorporating the concept of bit reversal, a 2D chaotic baker map, and DFT. Experimental results demon-

strate the superiority of this enhancement across various quality metrics, including the achievement of uniform histograms in the two modes of operations and enhanced resistance against differential attacks. The second work introduces a dual-domain image cryptosystem, merging the wavelet and spatial domains, along with a novel diffusion process in the wavelet domain. This addresses the issue of weak resilience against statistical, analytical, and differential attacks. Remarkably, the proposed diffusion process operates efficiently. The suggested operation requires only $1/16$ of the plain image pixels in the wavelet domain. Furthermore, this cryptosystem resolves the bell-shaped histogram problem associated with frequency-based cryptosystems, as substantiated through comprehensive performance metrics in simulation results. Additionally, a novel key-dependent chaotic variable generator, which facilitates the generation of essential initial conditions and control parameters for an enhanced chaotic map, is introduced. The simulation results evaluate the proposed dual-domain cryptosystem against state-of-the-art methods, consistently demonstrating its superiority across a spectrum of performance metrics. These findings underscore the effectiveness and resilience of the suggested approach in strengthening the secrecy and confidentiality of multimedia data.

ملخص الرسالة

الاسم:

محمود يس محمود يس

عنوان الدراسة:

ترانسفورم كريت: تشفير الصور الفوضوي بناءً على التحويلات

التخصص:

الهندسة الكهربائية

تاريخ الدرجة العلمية: نوفمبر 2023

حماية سرية البيانات المتعددة الوسائط تظل قضية في غاية الأهمية ضمن مجال أمان المعلومات، وتزايد أهميتها مع استمرار تطور التطبيقات المتعددة الوسائط. تتعمق هذه الرسالة في عالم التشفير الفوضوي للصور كحلاً محتملاً لهذه المشكلة الملحة. قامت الأبحاث السابقة باستكشاف التشفير الفوضوي للصور في مجموعة متنوعة من المجالات التحولية، مثل المجال المكاني وتحويل فورييه المتقطع وتحويل الموجات. على الرغم من الخصائص الإرباكية المواتية لأنظمة التشفير القائمة على التردد، إلا أنها تظهر عيوباً في الخصائص التوزيعية وتفشل في بعض الاختبارات الإحصائية، مما يجعلها عرضة للهجمات المتنوعة. رداً على هذه التحديات، تقدم هذه الرسالة حلين مبتكرين. يقدم العمل الأول نظام تشفير صور معزز بنظام تشفير الكتل، حيث يتضمن مفهوم عكس البت، نظام يكرر الفوضوي ثنائي الأبعاد، وتحويل فورييه المتقطع. تظهر النتائج التجريبية تفوق هذا التحسين عبر مقاييس جودة متنوعة، بما في ذلك تحقيق توزيعات تكرارية موحدة وزيادة مقاومته ضد الهجمات التفاضلية. العمل الثاني يقدم نظام تشفير صور ثنائي المجال، حيث يجمع بين مجالي الموجات والمجال المكاني، مع عملية انتشار جديدة في مجال الموجات. يعالج هذا النظام مشكلة القدرة الضعيفة على التحمل ضد الهجمات الإحصائية والتحليلية والتفاضلية. ومن الملحوظ أن عملية الانتشار المقترحة تعمل بكفاءة على 16/1 فقط من بكسل الصورة الأصلية في مجال الموجات. بالإضافة إلى ذلك، يحل هذا النظام مشكلة التوزيع التكراري الذي على شكل جرس المتعلق بأنظمة التشفير القائمة على التردد، كما يتم تأكيده من خلال مقاييس الأداء الشاملة في نتائج المحاكاة. بالإضافة إلى ذلك، تم تقديم مُؤَلِّد متغير فوضوي يعتمد على المفتاح يُيسِّر إنشاء الظروف الابتدائية الضرورية ومعلومات التحكم انظام فوضوي محسن. تقوم نتائج البحث بمقارنة النظام الثنائي المقترح في مجالي

الموجات والمكاني بأحدث الطرق الموجودة، حيث تظهر بثبات تفوقه عبر مجموعة متنوعة من مقاييس الأداء. تُؤكد هذه النتائج فعالية ومرونة النهج

المقترح في تعزيز أمان وسرية البيانات المتعددة الوسائط.

CHAPTER 1

INTRODUCTION

1.1 Preface

The process of transforming an image into a code to prevent unauthorized access or change of the image is called image encryption. Image encryption is important because images include sensitive information that must be secured, such as personal identity, medical records, and surveillance footage [4].

One of the key reasons why image encryption is vital is to safeguard people's privacy. A medical image, for example, may include important information about a patient's health, and if it is not securely encrypted, it may slip into the hands of someone who should not have access to it. This might result in major privacy violations and potential harm to the individual.

Image integrity protection is another important aspect of image encryption which ensures that the image has not been tampered with or changed in any way and that the image is generated by the original or intended source. This is especially important in the case of surveillance footage, which must be validated [5].

Image encryption is critical for preserving image transmission security. It secures pictures during transmission by encrypting them so that anybody intercepting them cannot understand the content or make any meaning of it [6].

Another significant advantage of image encryption is that it allows the usage of cloud storage for photos to be kept on servers that are accessible from anywhere in the globe. This, however, raises the possibility of illegal access to these data. Image encryption can assist in safeguarding photographs saved in the cloud, making the unauthorized parties considerably more difficult for them to access [4].

Images can be ciphered by various approaches, e.g., symmetric-key and asymmetric-key ciphering. An asymmetric-key cipher employs 2 different keys for the ciphering and deciphering processes, whereas symmetric-key encryption employs the same key for both processes. Both forms of encryption have advantages and downsides, and which one to employ will be determined by the application's unique requirements [2].

Chaotic maps [6], also known as chaotic dynamical systems, can be considered a way to be utilized for both forms of image encryption. These maps are distinguished by their sensitive dependency on starting conditions, often called the butterfly effect. In this effect, a minor disturbance in early conditions can result in drastically different long-term results. Because of its unpredictability, chaotic maps are an effective tool for image encryption, allowing for secure communication by making it harder to decrypt the ciphered image by an attacker.

1.2 Problem Statement

Chaotic image encryption has been investigated in the literature using different transformation domains, such as spatial, Discrete Fourier Transform (DFT), wavelet transform, etc. Although frequency-based cryptosystems demonstrate favorable confusion properties, they introduce poor diffusion properties, fail in terms of some statistical characteristics, and exhibit non-uniform histograms. Therefore, they are vulnerable to many attacks.

This work studies such cryptosystems, solves the aforementioned problems, improves these systems, and introduces a novel dual-domain cipher.

1.3 Research Objectives

Although many transform-based chaotic image cryptosystems have been introduced in the literature; many of these ciphers lack a good merge between the properties of these transformations and the encryption requirements in terms of obscuring the relationship between ciphered image and key (which is called confusion [7]) and the spread of the impact of one symbol of the plain image over various ciphered image symbols to hide the statistical properties of the plain-image (which is called diffusion [7]).

In this thesis, we investigate the use of some of these transformation methods in terms of chaotic image encryption. We can summarize this thesis's objectives as follows:

- Study the use of different transformations on chaotic image encryption.
- Explore and develop a transform-based chaotic image cryptosystem.
- Assess the developed transform-based chaotic image cryptosystem on the following aspects:
 - Statistical Analysis.
 - Encryption quality metrics.
- Examine and test the developed transform-based chaotic image cryptosystem resistance to various attack scenarios.

1.4 Organization of the Thesis

The thesis structure can be illustrated as follows:

- **Chapter 2:** introduces a concise illustration of the employed transformation domains, chaotic maps, and basic cryptography concepts; thereby laying the groundwork for a comprehensive comprehension of the forthcoming chapters.
- **Chapter 3:** presents a survey of various works introduced in the literature. This Chapter will focus on the perspective of performing the image encryption process in different transformation domains.
- **Chapter 4:** presents an enhanced block cipher image cryptosystem with several modes of operation based on the concept of bit reversal using the 2D chaotic

Baker map and DFT. This chapter also introduces a description of the simulation results of the proposed cryptosystem and evaluates them with different performance metrics.

- **Chapter 5:** introduces a novel dual-domain (wavelet and spatial domains, respectively) chaotic image cryptosystem suitable for cybersecurity applications. The simulation findings of this cryptosystem are presented, which are assessed by various performance metrics.
- **Chapter 6:** provides final conclusions on the presented work in this thesis followed by some recommended research points to be pursued by future researchers in this domain.

CHAPTER 2

BACKGROUND

2.1 Preface

The upcoming sections provide a concise illustration of the employed transformation domains, utilized chaotic maps, and basic cryptography concepts; thereby laying the groundwork for a comprehensive comprehension of the forthcoming chapters.

2.2 Transformation Domain

2.2.1 Two-Dimensional Discrete Fourier Transform

The DFT is an effective tool for analyzing and manipulating frequency-domain information, and the Two-Dimensional Discrete Fourier Transform (2D-DFT) is an extension of the One-Dimensional Discrete Fourier Transform (1D-DFT) technique that allows for the study of two-dimensional signals such as pictures. The 2D-DFT of an Two-Dimensional (2D)-signal as a function $f(x, y)$, which its dimensions is $(M \times N)$

is calculated by [8]:

$$F(u, v) = \frac{1}{M \times N} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y) e^{-j2\pi\left(\frac{ux}{M} + \frac{vy}{N}\right)} \quad (2.1)$$

This equation is calculated for $u = 0, 1, 2, \dots, M-1$ and $v = 0, 1, 2, \dots, N-1$. In the same manner $f(x, y)$ is retrieved from $F(u, v)$ by the use of Two-Dimensional Inverse Discrete Fourier Transform (2D-IDFT), which is calculated by [9]:

$$f(x, y) = \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} F(u, v) e^{j2\pi\left(\frac{ux}{M} + \frac{vy}{N}\right)}, \quad (2.2)$$

where $x = 0, 1, 2, \dots, M-1$ and $y = 0, 1, 2, \dots, N-1$.

2.2.2 Integer to Integer Wavelet Transform

Traditional Wavelet Transform is a transform commonly employed to simultaneously analyze images in both time (or spatial) and frequency domains [10]. This analysis is done by decomposing the image into different bands or resolutions, each of which contains information about both the time localization (similar to time-domain analysis) and frequency content (similar to frequency-domain analysis) of the image [11].

Sweldens and Daubechies in 1994 introduced the IIWT using the lifting scheme concept [12]. In contrast to the traditional wavelet transform, IIWT preserves the multi-band attributes inherent in the traditional wavelet transform while offering a significant enhancement in computational efficiency. Moreover, this refinement is primarily attributed to the conversion of traditional wavelet transform coefficients from

floating-point to integer values, thereby mitigating the computational speed delay associated with floating-point arithmetic [13].

IIWT can be implemented in terms of multiple decompositions. to implement these decompositions, the input image undergoes segmentation via the utilization of filters [14]. Each stage within the filter consists of both low-pass and high-pass filters. As a result, a subband related to each filtration level is produced. These generated image subbands encompass two primary categories: low and high-pass subbands. Among the latter, exist three distinct types of high-pass subbands oriented horizontally, vertically, and diagonally.

Typically, Low-Low pass subband (LL) denotes the low-pass subband, Low-High pass subband (LH) signifies the vertical high-pass subband, High-Low pass subband (HL) designates the horizontal high-pass subband, and High-High pass subband (HH) represents the diagonal high-pass subband. In the context of multi-layer IIWT decomposition, the 'LL' low-pass subband is subject to analogous decomposition steps. This process continues up to the culmination of multi-layer IIWT decomposition, yielding a matrix of coefficients.

The proposed dual-domain image cryptosystem adapts the lifting scheme of the Biorthogonal 3.7 Wavelet (Bior3.7) to calculate the IIWT to prove the concept. Figure 2.1 demonstrates an example of two levels of IIWT decomposition.

2.3 Chaotic Maps

Chaotic maps, also known as chaotic dynamical systems, are distinguished by their

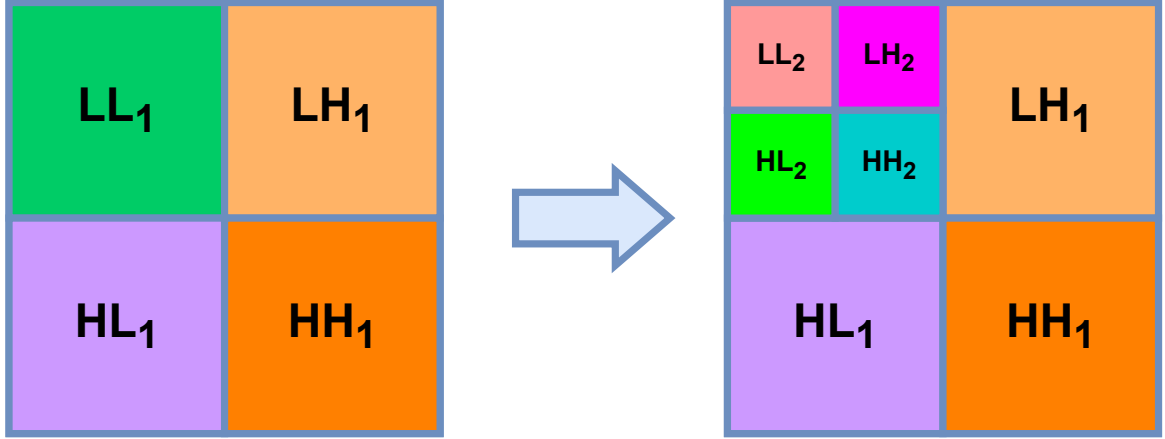


Figure 2.1: A 2-level IIWT decomposition.

sensitive dependency on starting conditions, often known as the butterfly effect, in which a minor disturbance in early conditions results in drastically different long-term outcomes [6]. Due to their unpredictability, chaotic maps are an effective tool for cryptography. They allow secure communication by making it harder to decrypt the ciphertext by an attacker.

2.3.1 Two-Dimensional Chaotic Baker Map

The 2D discrete chaotic Baker map is a chaotic encryption process that is based on a permutation procedure for a square image with $M \times M$ pixels [6]. This square image is split into k vertical rectangles with M pixels in height and m_i pixels in width. The horizontal partition of the image is determined by a pattern of k integers, $m_1, m_2, \dots, m_k$. M is split by each integer m_i , where $i = 1, 2, \dots, k$. In addition, $M_i = m_1 + m_2 + \dots + m_i$ and $M = m_1 + m_2 + \dots + m_k$. For the discrete time t , let l_t and $s_t = 0, 1, 2, \dots, M - 1$ denote the horizontal and vertical indices of a specific image pixel, in that order. A pixel at (l_t, s_t) of the i_{th} rectangle, is moved to a new

position (l_{t+1}, s_{t+1}) governed by the general discrete version of the baker map, with $M_{i-1} \leq l_t < M_i$ and $0 \leq s_t < M[6]$:

$$(l_{t+1}, s_{t+1}) = \left(\frac{M}{m_i} (l_t - M_{i-1}) + s_t \bmod \frac{M}{m_i}, \right. \\ \left. \frac{m_i}{M} \left(s_t - s_t \bmod \frac{M}{m_i} \right) + M_{i-1} \right) \quad (2.3)$$

The distribution of the horizontal partitions m_i can be considered as the encryption key. Fig. 2.2 shows the 2D Baker map encryption process of an 8×8 matrix for $key = (4, 2, 2)$.

Key =	4				2		2									
	PX ₁	PX ₂	PX ₃	PX ₄	PX ₅	PX ₆	PX ₇	PX ₈	PX ₃₁	PX ₂₃	PX ₁₅	PX ₇	PX ₃₂	PX ₂₄	PX ₁₆	PX ₈
	PX ₉	PX ₁₀	PX ₁₁	PX ₁₂	PX ₁₃	PX ₁₄	PX ₁₅	PX ₁₆	PX ₆₃	PX ₅₅	PX ₄₇	PX ₃₉	PX ₆₄	PX ₅₆	PX ₄₈	PX ₄₀
	PX ₁₇	PX ₁₈	PX ₁₉	PX ₂₀	PX ₂₁	PX ₂₂	PX ₂₃	PX ₂₄	PX ₂₉	PX ₂₁	PX ₁₃	PX ₅	PX ₃₀	PX ₂₂	PX ₁₄	PX ₆
	PX ₂₅	PX ₂₆	PX ₂₇	PX ₂₈	PX ₂₉	PX ₃₀	PX ₃₁	PX ₃₂	PX ₆₁	PX ₅₃	PX ₄₅	PX ₃₇	PX ₆₂	PX ₅₄	PX ₄₆	PX ₃₈
	PX ₃₃	PX ₃₄	PX ₃₅	PX ₃₆	PX ₃₇	PX ₃₈	PX ₃₉	PX ₄₀	PX ₉	PX ₁	PX ₁₀	PX ₂	PX ₁₁	PX ₃	PX ₁₂	PX ₄
	PX ₄₁	PX ₄₂	PX ₄₃	PX ₄₄	PX ₄₅	PX ₄₆	PX ₄₇	PX ₄₈	PX ₂₅	PX ₁₇	PX ₂₆	PX ₁₈	PX ₂₇	PX ₁₉	PX ₂₈	PX ₂₀
	PX ₄₉	PX ₅₀	PX ₅₁	PX ₅₂	PX ₅₃	PX ₅₄	PX ₅₅	PX ₅₆	PX ₄₁	PX ₃₃	PX ₄₂	PX ₃₄	PX ₄₃	PX ₃₅	PX ₄₄	PX ₃₆
	PX ₅₇	PX ₅₈	PX ₅₉	PX ₆₀	PX ₆₁	PX ₆₂	PX ₆₃	PX ₆₄	PX ₅₇	PX ₄₉	PX ₅₈	PX ₅₀	PX ₅₉	PX ₅₁	PX ₆₀	PX ₅₂

(a) Plain Matrix.

(b) Ciphred Matrix.

Figure 2.2: The 2D Baker map encryption process of an 8×8 matrix with $key = (4, 2, 2)$.

2.3.2 One-Dimensional Logistic Map

Cryptography has embraced the logistic map as an intuitive, highly efficient, chaotic map with countless applications [6]. With the appropriate control parameters, it can exhibit a behavior chaotically. Iteratively, the logistic map is computed in the

following manner [15]:

$$y_{j+1} = \Psi_{logistic}(y_j, r) = (1 - y_j) \times y_j \times r, \quad (2.4)$$

where y_j is a real number that ranges between $[0,1]$, y_0 is the initial value for the iterative operation, and r is the chaotic map's control parameter; in the range $[0,4]$.

Despite its proven benefits, the logistic map suffers from a limited chaotic range and periodic windows. These limitations are clearly observed in the logistic map's bifurcation diagram in Fig.2.3. The logistic map chaotically behaves when the r range is between approximately $[3.57, 4]$ [16]. The 3.57 point is called the accumulation point, which marks the transition from periodic orbits to chaotic orbits.

Another problem that logistic map suffers from is the non-ergodicity issue. That leads to the y values not covering every possible point in the phase space of $[0,1]$, except when r approximately equals 4.0. Accordingly, some attractors are skipped within the trajectory [17].

Therefore, the previously mentioned problems need to be tackled before the use of this chaotic map in the design of any cryptosystem to avoid future potential security breaches.

2.3.3 Enhanced One-Dimensional Logistic Map

To tackle the aforementioned challenges that the standard logistic map suffers from, authors in [1] presented an enhanced version of the logistic map. This improved version relies on the combination and cascade of the logistic map with a function

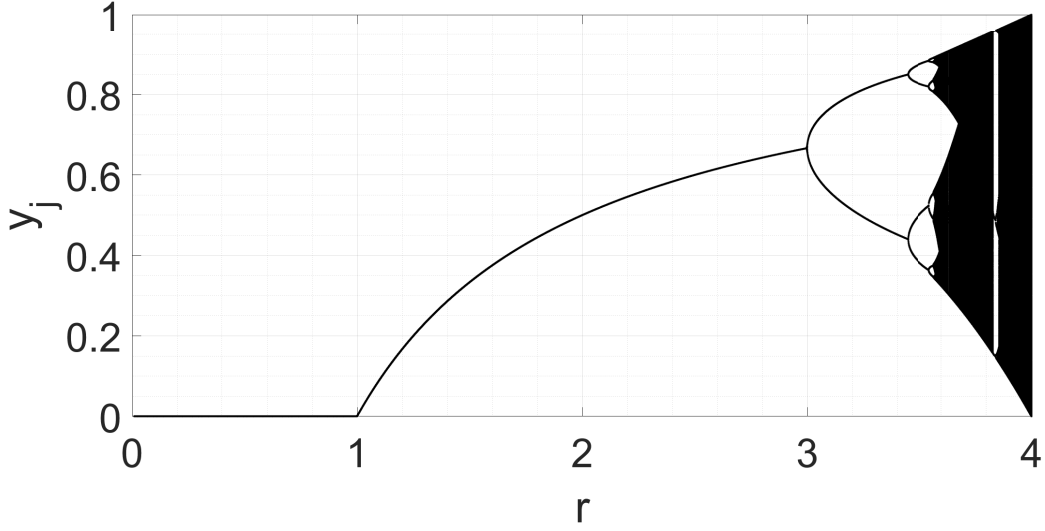


Figure 2.3: Bifurcation diagram for the chaotic standard logistic map.

that exhibits nonlinear behavior. This simple yet effective solution is advantageous in terms of computational cost. Mathematically, this enhanced logistic map is calculated in the following manner:

$$U(y_i, r) = r \times y_i, \quad (2.5)$$

$$\Psi_{logistic}(U(y_i, r), r) = r \times U(y_i, r) \times [1 - U(y_i, r)], \quad (2.6)$$

$$y_{i+1} = [\frac{r}{U(y_i, r)} + \Psi_{logistic}(U(y_i, r), r)] \bmod 1, \quad (2.7)$$

where $i = 1, 3, 4, \dots, I$, I is total number of iterations, and $r \in [0, \infty]$ is the parameter that controls the chaotic map. As shown in Fig.2.4, the bifurcation diagram of the enhanced logistic map covers the entire range of the control parameter r , indicating the disappearance of any periodic windows in that range.

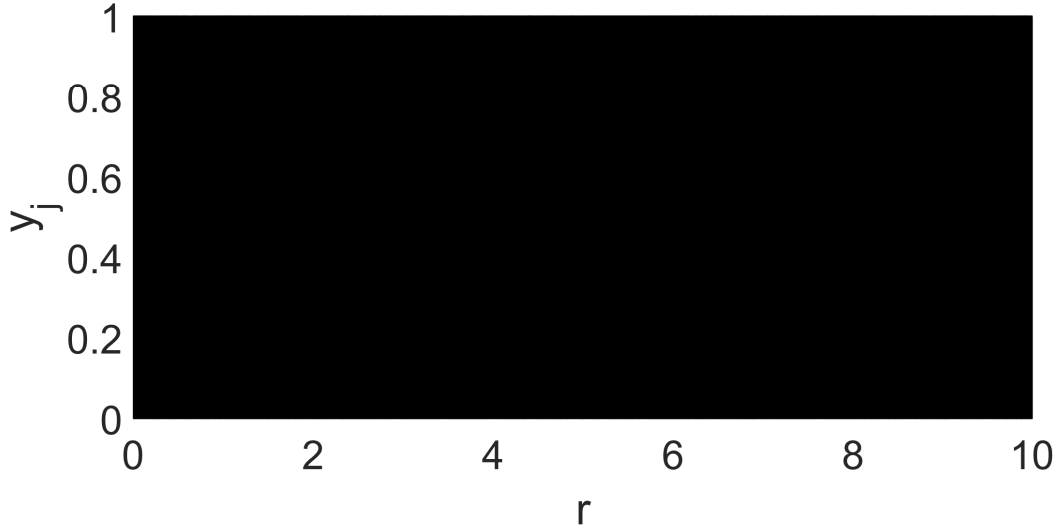


Figure 2.4: Bifurcation diagram for the enhanced logistic map in [1].

2.4 Basic Encryption Concepts

Encryption is a vital technique employed to craft confidential messages accessible exclusively to designated individuals or groups. To be effective, the encryption procedure must possess robust security measures that discourage unauthorized decoding while remaining easily accessible to authorized parties [2]. In today's era, encryption is indispensable for safeguarding crucial data and sensitive information. This includes data such as private network access, website passwords, and credit card numbers as failure to protect them can result in malicious manipulation of sensitive data, leading to undesirable consequences caused by vicious cyber attackers. Figure 2.5 shows a basic topology for an encryption process in a communication network scenario.

2.4.1 Symmetric-Key Cryptosystems

Symmetric-key-based cryptosystems are a classical type of cryptosystem by which a

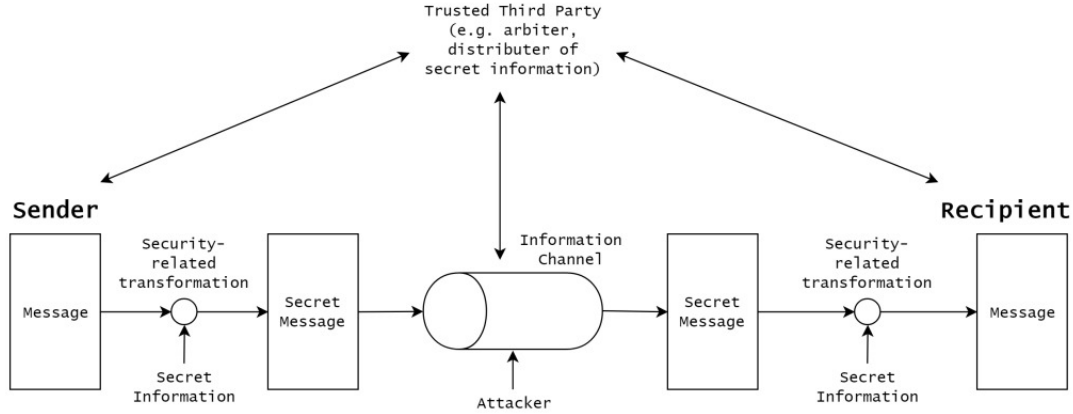


Figure 2.5: Basic encryption topology for a communication network. [2].

sender can securely transmit a confidential message to an authorized recipient. Such a type of cryptosystem closely resembles the overall encryption process in the communication network scenario illustrated in Fig. 2.5. However, it relies on a similar secret key for both cryptography processes: encryption and decryption, as the confidential piece of information [18]. Figure 2.6 provides a simplified characterization of a symmetric-key-based cryptosystem.

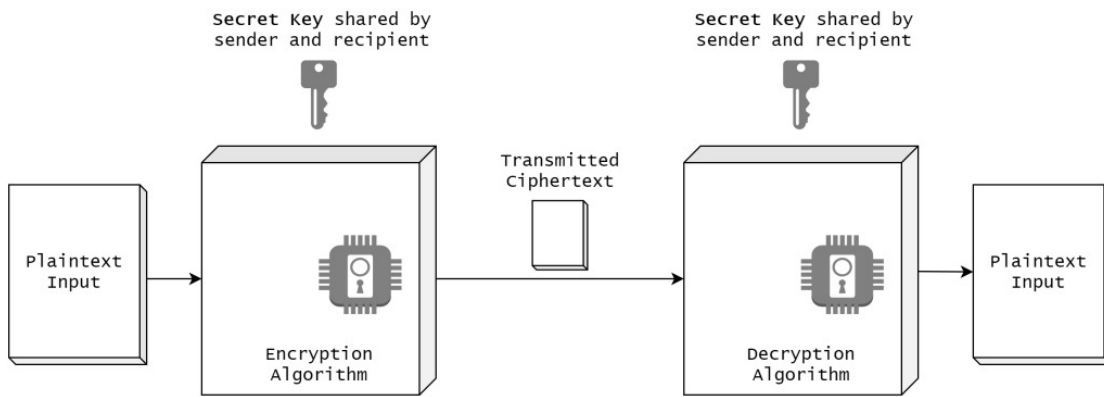


Figure 2.6: Simplified illustration of a symmetric-key-based cryptosystem[2].

As shown in Fig. 2.6, the primary elements of a symmetric-key-based cryptosystem are as outlined below:

- **Plaintext:** This is the message that the sender intends to transmit exclusively to the authorized recipient. It serves as the input to the encryption scheme.
- **Encryption Algorithm:** This is a set of procedures that execute various data manipulations and transformations on the plaintext for the purpose of making it ambagious.
- **Shared Key (Secret Key):** A key of a specific length, distributed securely between the sender and the recipient. It has an essential role in the process of ciphering, ensuring the uniqueness and authenticity of the resulting ciphered data. Moreover, the choice of such a key should satisfy that the reversing operation of the ciphered text (decryption) will not be successful without the use of the same exact key for this process.
- **Ciphered Data (Ciphertext):** This is the outcome produced by the ciphering scheme. The ciphertext is dependent on the plaintext, the ciphering scheme, and the key. It should appear indecipherable and seemingly random.
- **Decryption Algorithm:** This is the reverse operation of the encryption algorithm, which reverts the ciphertext back into the original plaintext.

It's noteworthy to mention that any cryptosystem must be able to withstand any attack. In essence, this implies that an attacker, even if he was equipped with knowledge of the cipher scheme and a collection of ciphertexts and their corresponding plaintexts, would remain incapable of deciphering the ciphertext if he did not have the cipher key. The robustness of such a cryptosystem stems from two fundamental

properties [7]:

- **Confusion:** is the property of making the relation between the ciphertext and its corresponding plaintext and cipher key as complicated as feasible.
- **Diffusion:** is the property of maximizing the spreading of the statistical characteristics of the plaintext through its corresponding ciphered one. To put it differently, a minor change in the plaintext, even in the resolution of one bit, can be able to have a drastic change in its corresponding ciphered version.

2.4.2 Block Cipher Cryptosystems

A Symmetric-key-based cryptosystem can be implemented through the concept of block cipher. In this method, data is divided into fixed-length chunks called "blocks". Each one of them is applied to a block cipher scheme to be encrypted, which can either be transmitted directly through a communication channel or combined with other cipher blocks before being sent to the recipient. Generally, the size of a block varies from 64 bits to 1024 bits in length.

Rivest Cipher 4 (RC4), Blowfish, Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), Rivest Cipher 5 (RC5), and Advanced Encryption Standard (AES) are all examples of Symmetric-key-based block ciphers. In 2001, National Institute of Standards and Technology (NIST) formally adopted the AES supplanting 3DES [2].

Several general attributes can serve as criteria for configuring the parameters and design aspects of a specific block cipher scheme some of them are as follows [2]:

- **Number of Rounds:** it refers to the repetition of data transformations to augment complexity and, consequently, strengthen security.
- **Key Size:** Enlarging the key size generally boosts security by minimizing the likelihood of brute-force attacks. Key size often aligns with the block size.
- **Subkey Generation:** Once more, the process of generating a new key for each round serves to elevate complexity and, in turn, enhance cryptosystem secrecy.
- **Block Size:** Enhancing the size of the block in terms of bits typically enhances security through heightened complexity in the transformation of data. However, it's essential to note that increasing the size may lead to a reduction in the speed efficiency of the cryptosystem.

2.4.3 Image Cryptosystems

Image encryption is a process that converts an image into an ambiguous coded format with the purpose of preventing any manipulation or unauthorized access [4]. This type of cryptosystem is an essential part of various applications in numerous vital and sensitive domains, including video surveillance and medical imaging. Moreover, image cryptosystems also focus on preserving the authenticity of ciphered images, as various applications rely on them to make decisions in real-time scenarios. Consequently, it becomes crucial to prevent potential attackers from tampering with plain images. Hence, these image cryptosystems must, therefore, generate incomprehensible ciphered images by employing appropriate transformations. Some noteworthy distinctions between images and conventional data are as follows [5]:

1. **Two-Dimensional Correlation:** Since images possess a two-dimensional structure, pixels exhibit strong correlations with neighboring pixels in both vertical and horizontal orientations, as well as diagonally. Consequently, effective image cryptosystems need to prioritize achieving the lowest level of correlation for the data.

2. **Data Redundancy:** Images also tend to contain a significant amount of information in a duplicated (redundant) manner, which can pose challenges for conventional symmetric ciphers. Therefore, image cryptosystems must employ extensive confusion mechanisms to ensure the widest possible pixel range, even when dealing with redundant data.

CHAPTER 3

TRANSFORM-BASED CHAOTIC IMAGE ENCRYPTION

3.1 Preface

Generally speaking, the process of converting an image to an ambiguous coded format with the purpose of preserving its confidentiality is called image encryption [5]. For example, authors in [19] introduced an image cryptosystem that relies on a finite state machine merged with a Deoxyribonucleic acid (DNA)-based operation.

Furthermore, an image cryptosystem based on dynamical chaotic systems is called a chaotic image cryptosystem. These dynamical chaotic systems are known as chaotic maps. Their dependence on initial conditions characterizes them. This characteristic occurs when an early status can have severe consequences on long-term outcomes due to a phenomenon namely, the butterfly effect [6]. As a result of their ability to exhibit unpredictable behavior, chaotic maps are a powerful and influential part of designing image cryptosystems. Hence, secure communication is made possible by

making attacking the ciphered image more difficult.

There is a lot of work in the literature has been done on chaotic image encryption. These works have been done in three different directions [4]: chaos, images, and encryption.

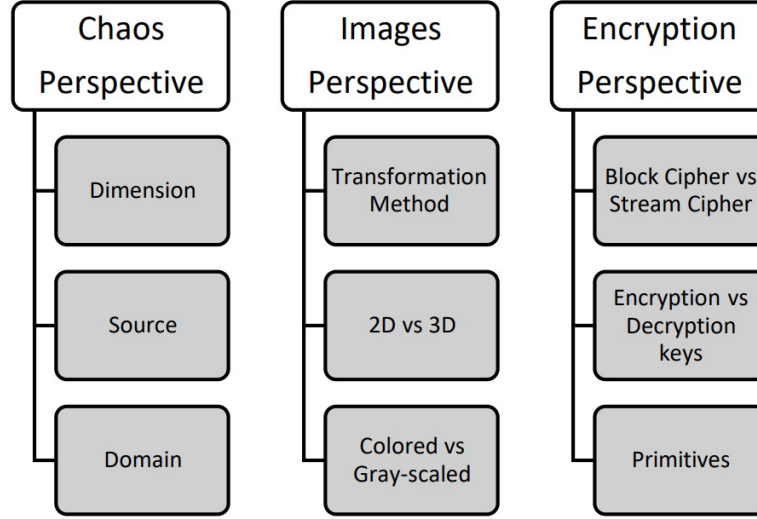


Figure 3.1: The different research perspectives in image encryption using chaotic maps.

Figure 3.1 depicts the nature of the chaos perspective, which encompasses dimensions, sources, and domains. Specifically, in the chaotic image encryption field, chaos can be examined across various domains, including space, time, and space-time domains. Additionally, the generation of chaos can be accomplished through mathematical means, such as chaotic maps, or physical means, such as optical chaos. The dimensionality of a chaotic map is determined by the number of functions it comprises. Furthermore, diverse dimensions of chaotic functions are employed in various chaotic image encryption techniques. Images Perspective investigates the image transformation method, two-dimensional versus three-dimensional images, and gray-scaled versus colored images. Furthermore, the encryption perspective is associated with

block ciphers versus stream ciphers, encryption vs. decryption keys which is related to symmetric and asymmetric encryption, and the different primitives of cryptography such as confusion, and diffusion. This research will focus on the perspective of performing the image encryption process in different transformation domains.

3.2 Chaotic Image Encryption in Spatial Domain

The implementation of a chaotic image cryptosystem can be done in the spatial domain. For example, in [20], a comprehensive examination has been conducted to assess the efficiency of cryptographic systems based on three distinct standard chaotic maps within the spatial domain. These are the Baker, the Arnold cat, and the logistic maps. The authors encompasses an in-depth analysis of the cryptosystems relying only on these chaotic maps, focusing on various aspects such as ciphered photographic quality, general correlation coefficients, entropy characteristics, differential analysis, and histogram performance. The primary limitations of this research lie in its absence of proper diffusion and confusion mechanisms, as well as the observation that the histogram of the ciphered image does not change compared to the plain image.

In [21], an effort is made to address these challenges through the introduction of an image encryption procedure that entails the segmentation of the plain image into smaller partitions, followed by a standard 2D chaotic Baker map encryption algorithm for each of these partitions. The authors employed their encryption technique in three distinct block cipher modes. In spite of their approach successfully mitigating the issue of non-changeable histogram distributions within the ciphered images, promoting

convergence toward a uniform distribution, their cryptosystem still suffers from weak diffusion and confusion processes. In addition, it subverts with some of the partition sizes.

One way to solve this problem is the work in [22], [23], where the authors introduce image cryptosystems that implement a standard logistic map-based permutation and a single AES S-Box for substitution. The required initial conditions for the chaotic map are generated depending on the output of a hashing function which its inputs is the plain image. This approach increases the cryptosystem immunity to differential and statistical attacks.

3.3 Chaotic Image Encryption Using Discrete Fourier Transform

Moving on from the spatial domain; the implementation of a chaotic image cryptosystem can be accomplished in the frequency domain by means of different types of Fourier transform. For instance, work in [3] illustrates an image cryptosystem implemented using the two-dimensional chaotic Baker Map in the frequency domain using Discrete Fourier Transform (DFT). It uses the Baker map to perform a shuffling operation on the transformed image coefficients, creating a more secure encryption.

The authors in [20] and [24] undertook an investigation into an image cryptosystem that utilizes various chaotic maps within the Fractional Fourier Transform (FrFT) domain. In their approach, the transformation parameters were employed as additional supplementary keys to encrypt data. The encryption techniques they introduced ex-

hibited superior efficiency and security when compared to complementary methods applied in the spatial domain.

However, it is noteworthy to mention that both of the aforementioned chaotic image cryptosystems exhibit a limited diffusion process, rendering them susceptible to differential attacks. In addition, the encrypted image's histogram distribution tends to display a non-uniform pattern (resembling a bell-shaped distribution).

Furthermore, Authors in [25] presented a chaotic image cryptosystem that relies on a dynamical coding DNA-based operation implemented in the frequency domain. The transformed image coefficients are separated into two groups of coefficients: amplitude and phase coefficients. Then, each group of these coefficients is scrambled and diffused with the help of a multi-dimensional hyperchaotic map. Although the authors of this work claim that this approach provides immunity against brute force and differential attacks, it is very clear this method introduces approximately double the encryption computational complexity due to the separation of the transformation coefficients.

3.4 Chaotic Image Encryption Using Discrete Wavelet Transform

Another procedure is the implementation of a chaotic image cryptosystem using the wavelet transform. Authors in [26] proposed a chaotic image cryptosystem that implements an XORing and key-dependant scrambling operations at the bit level using Integer to Integer Wavelet Transform (IIWT). Results demonstrated the ability of the cryptosystem to pass some encryption statistical tests.

In [27], the Authors created a method that combines the use of a Discrete Wavelet Transform (DWT), chaotic image encryption, and a chaotic binary stream to enhance security. This approach uses DWT for both the plaintext image and the chaotic watermarked ciphered image. Only the approximation coefficients of the encrypted image, rather than the entire image, are embedded to achieve improved robustness. According to the authors, their findings indicate that the integration of wavelet technology, chaos, and digital watermarking is capable of meeting encryption standards and producing robust encryption, even when faced with challenges such as noise attacks, and lowpass filters.

In [28], the Authors introduced a new method for scrambling images, called the "new chaos transform". An encryption algorithm for images is also proposed, which combines the use of the two-dimensional Wavelet Transform and the new chaos transform. The algorithm consists of three steps: breaking down the image into four sub-images using the 2D wavelet transform, using the same keys to scramble the low and high-frequency sub-images using the new chaos transform, and then using the Inverse Wavelet Transform to obtain the final encrypted image.

A DWT based colored chaotic image encryption technique is proposed in [29]. The color plain image is first broken down into red, green, and blue elements. Then, an updated 3D chaotic cat map is presented to shuffle the wavelet coefficients of the red, green, and blue components, causing these three components to interact and mix unpredictably. To increase the performance of the cryptosystem, the linked map lattice scheme is used in the spatial domain to perform a diffusion process. These operations are repeated multiple times (rounds) to reach a satisfactory result.

In [30], the authors suggested an image encryption approach using a two-dimensional discrete wavelet transform and a chaotic system. The scheme involves wavelet decomposition of the target image using Bior3.7 wavelet to obtain approximation and details coefficients, reordering of approximation coefficient matrix using One-Dimensional (1D) logistic chaos sequence, and inverse wavelet transform to generate the encrypted image.

In [31], the authors proposed an enhanced chaotic image encryption technique based on four chaotic maps and the Haar wavelet packet decomposition. Firstly, a permutation process is executed by the Baker chaotic map for scrambling wavelet packets. Then a process composed of 2 chaotic maps - (the three-dimensional Arnold map, applied twice, and the tent map paired with the logistic map) is used to boost the entropy of the ciphered picture and the key's space of the cryptosystem.

3.5 Dual-Domain Chaotic Image Encryption

An alternative method explored in the existing body of literature involves the development of a chaotic image cryptosystem with a dual-domain perspective, encompassing both spatial and wavelet domains.

For instance, in [32], authors presented a dual-domain cryptosystem for images that relies on a hyperchaotic map. The image cryptosystem was implemented in the frequency and spatial domains using a wavelet decomposition in a dynamic manner. Results showed the ability of this cryptosystem to mitigate different attacks.

In [13], authors introduced a dual-domain lightweight chaotic image cryptosystem

that performs the diffusion process only on the first level of the low-low band of the IIWT. Then, a permutation process is applied to the diffused image in the spatial domain after returning from the wavelet domain. Results revealed that although the cryptosystem demonstrated satisfactory performance in certain metrics, there were concerning patterns of poor histogram uniformity observed in the ciphered images.

CHAPTER 4

ENHANCED DFT-BASED CHAOTIC IMAGE BLOCK CIPHER WITH SEVERAL MODES OF OPERATION

4.1 Preface

Chaotic image encryption has been investigated extensively in the literature in different domains, including the frequency domain using DFT. Despite DFT-based chaotic image cryptosystems exhibiting good confusion properties, they suffer from poor diffusion characteristics and non-uniform histograms. Therefore, they are vulnerable to many attacks, such as differential attacks, and statistical cryptanalytic attacks. This chapter presents an enhanced block cipher image cryptosystem with several modes of

operation based on the concept of bit reversal using the 2D chaotic Baker map and DFT. The proposed enhancement develops an improved image encryption scheme that involves properly diffusion-confusion enhanced operations within modified versions of the known block cipher modes of operation, namely Cipher Block Chaining Mode (CBC), Cipher Feedback Mode (CFB), and Output Feedback Mode (OFB). These enhanced operations are based on a 2D chaotic baker map in the Fourier domain. This work adapts the cryptosystem presented in [3] as the main encryption block E_{k1} to illustrate the concept. However, the main encryption block can be any symmetric encryption scheme applied in any discrete version of the Fourier transform. A block diagram for the adapted main encryption (E_{k1}) and decryption (D_{k1}) is illustrated in Fig.4.1.

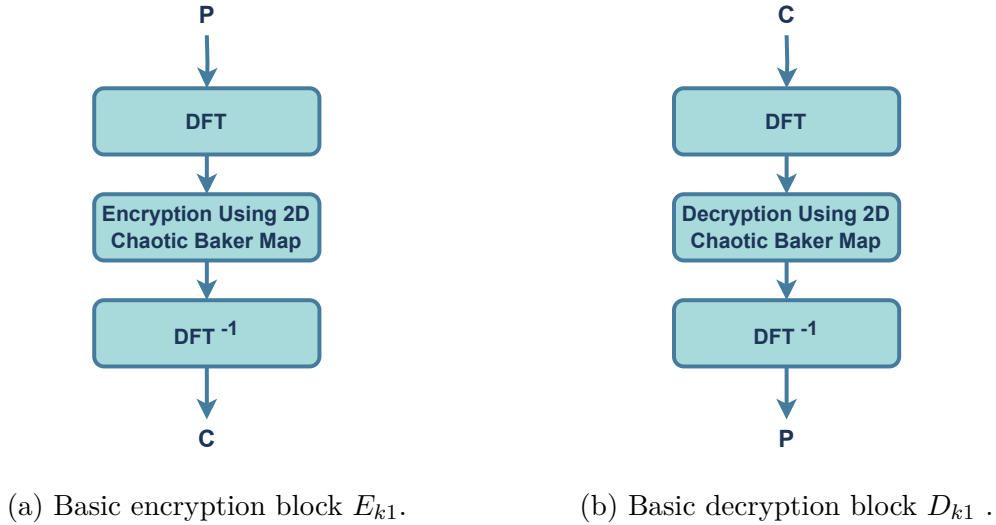


Figure 4.1: Basic encryption E_{k1} and decryption D_{k1} block diagrams adapted from [3].

The proposed enhancement is validated using a MATLAB simulation. Results show that the proposed work manages to overcome the abovementioned problems

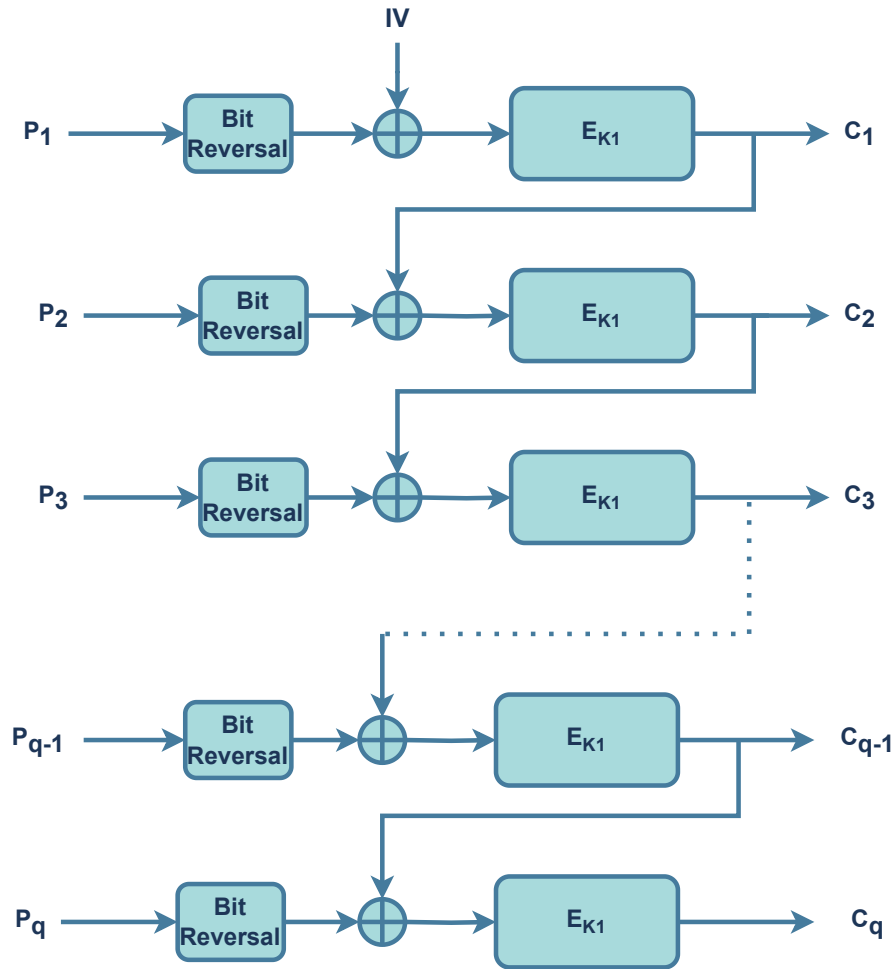
outstandingly and outperforms the existing results in the literature in many encryption quality metrics.

4.2 Proposed Enhanced Cryptosystem Scheme

An illustration of the enhanced proposed image cryptosystem is given in this section. Firstly, a general and simple summary of the enhanced proposed image cryptosystem is as follows:

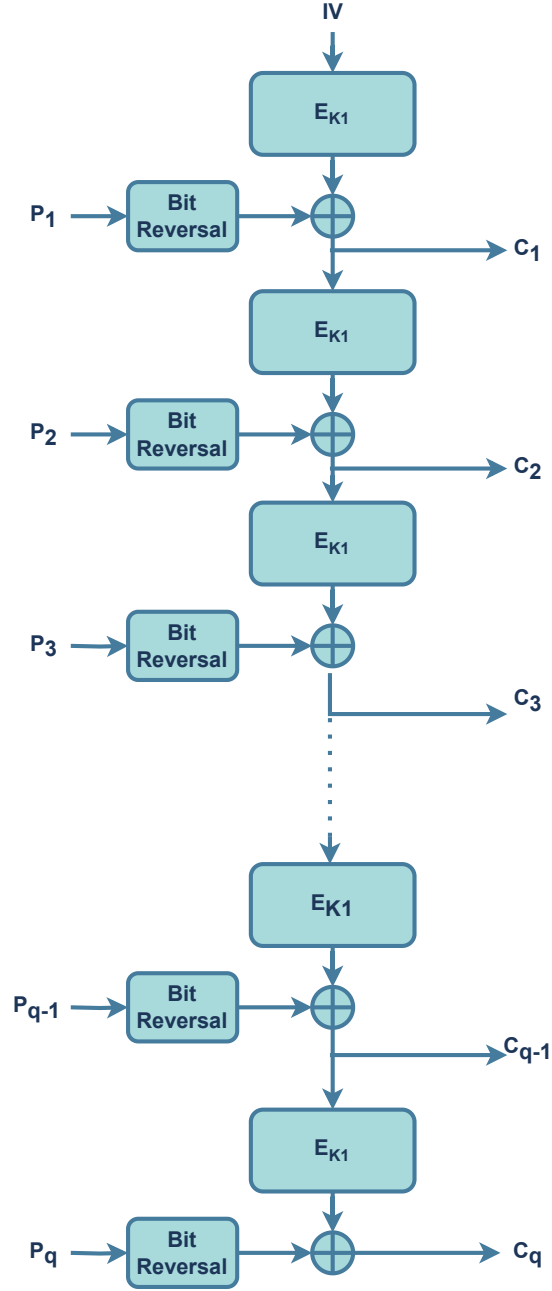
1. Load the image, and divide it into q plain-image blocks of $M \times M$ pixels size, with proper padding as needed.
2. Apply one of the proposed enhanced image cryptosystems to P_i block in one of the 3 different proposed modified versions of the standard block cipher modes of operation (CBC, CFB, and OFB), as illustrated in Fig.4.2.
3. Each mode of operation contains an encryption block E_{k1} , which is a symmetric encryption scheme applied in the DFT domain.

An elaboration on each modified mode is illustrated in the following subsections.



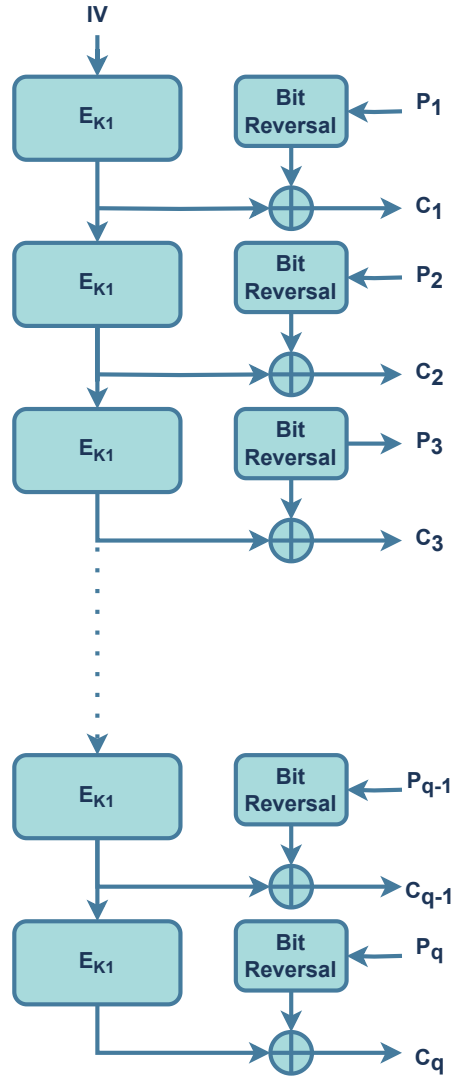
(a) MCBC mode.

Figure 4.2: The proposed enhanced image cryptosystem operating in various modes.



(b) MCFCB mode.

Figure 4.2: The proposed enhanced image cryptosystem operating in various modes.



(c) MOFB mode.

Figure 4.2: The proposed enhanced image cryptosystem operating in various modes.

4.2.1 Proposed Enhanced Cryptosystem in the Modified CBC Mode

As shown in Fig.4.2a, Modified Cipher Block Chaining Mode (MCBC) is a block cipher encryption mode where instead of forming an XORing operation in the bit level between the pixels in the Initial Vector (IV) and its corresponding ones in the first block, the XORing is done between the IVs' pixels and the bit reversal of the corresponding ones in the first block. The proposed insertion of the simple low computational burden bit reversal operation experimentally leads to significantly improved randomness and statistical characteristics of the overall ciphering process (as illustrated in Section 4.3). The output of this operation is chaotically encrypted to produce the first ciphered block C_1 . Next, the encrypted pixels C_1 are employed in place of the IV to encrypt the subsequent block. This process is iterated until the final segment is attained, which can be expressed mathematically in the ensuing manner:

$$\begin{aligned} C_i &= E_{k1} [C_{i-1} \oplus \check{P}_i], i = 1, 2, 3, \dots q, \\ \check{P}_i &= R[P_i], \end{aligned} \tag{4.1}$$

where, R is the bit reversal operator, i.e. for a 8-bit pixel, $R[b_0, b_1, b_2, b_3, b_4, b_5, b_6, b_7] = [b_7, b_6, b_5, b_4, b_3, b_2, b_1, b_0]$, $\check{P}_i$ is the bit reversed block, $C_0 = IV$, C_i is the corresponding encryption of the block P_i , $\oplus$ indicates the XOR operation, and E_{k1} refers to the chaotic operation of encryption. This realization utilizes a chaining mechanism,

resulting in every block cipher in the ciphered image being reliant on all preceding segments of the previous ciphered ones. As a result, the next ciphered block contains the results of all previous blocks. The decryption process can be implemented as follows:

$$P_i = R[D_{k1}(C_i) \oplus C_{i-1}], i = 1, 2, 3, \dots q \quad (4.2)$$

where D_{k1} indicates the chaotic operation of decryption.

4.2.2 Proposed Enhanced Cryptosystem in the Modified CFB Mode

The Modified Cipher Feedback Mode (MCFB) begins by performing the encryption chaotically on the pixels of the IV using the E_{k1} , followed by XORing the encrypted version of the IV with the bit reversal of the first block of the plain image $\check{P}_1$ to produce C_1 , as illustrated in Fig. 4.2b. The following ciphered block C_2 is obtained by chaotically encrypting the previous ciphered block C_1 . Then, the result is XORed with the pixel-wise bit reversal of the next plain-image block $\check{P}_2$. The same process is applied to obtain the remaining ciphered blocks.

The MCFB can be expressed mathematically as follows:

$$C_i = \check{P}_i \oplus E_{k1}(C_{i-1}), i = 1, 2, 3, \dots q, \quad (4.3)$$

and the decryption is accomplished as follows:

$$P_i = R [C_i \oplus E_{k1} (C_{i-1})], i = 1, 2, 3, \dots q, \quad (4.4)$$

4.2.3 Proposed Enhanced Cryptosystem in the Modified OFB Mode

The Modified Output Feedback Mode (OFB) is the same as MCFB mode as shown in Fig. 4.2c, but instead of feedback ciphered block C_i as input for E_{k1} in the chaining process, the output of E_{k1} itself is the one that is taken as feedback for the upcoming stages. The process of encryption and decryption is expressed mathematically as follows:

$$C_i = \check{P}_i \oplus E_{k1} (I_{i-1}), i = 1, 2, 3, \dots q, \quad (4.5)$$

$$P_i = R [C_i \oplus E_{k1} (I_{i-1})], i = 1, 2, 3, \dots q, \quad (4.6)$$

where $I_i = E_{k1} (I_{i-1}), i = 1, 2, 3, \dots q$, and $I_0 = IV$.

4.3 Simulation Results

A discussion and analysis using different encryption quality metrics are carried on to the obtained results. This analysis is firstly done with a comparison among the proposed enhancement in three different block sizes (16 x16), (32x 32),(64 x 64) pixels, and the DFT-Baker method, respectively, using 512×512 gray-scale "Mandrill" image and MATLAB 2022. Then in Subsection 4.3.8, a comparison between the proposed enhanced cryptosystem and the work presented in the literature in[20], [21], [3], [33], [34], [25], [35] is being held, using 512×512 "Lena" image.

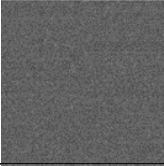
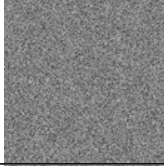
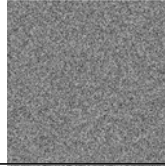
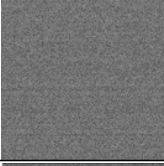
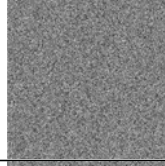
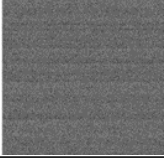
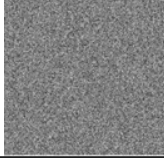
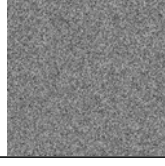
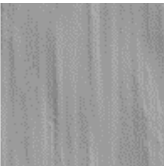
4.3.1 Visual Test

One of the easiest assessment techniques is the visual test, which involves looking for flaws with the human eyes. It is less technologically sophisticated than other ways, yet it is one of the most dependable methods for detecting all manifestations [24]. Table 4.1 shows the Ciphared results of the "Mandrill" image using the suggested enhanced cryptosystem in different modes of operation with different block sizes. In the suggested approach, the features of the resulting encrypted "Mandrill" image have totally gone from their complementary plain image, ensuring its encryption effectiveness.

4.3.2 Histogram Visualization

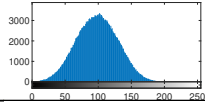
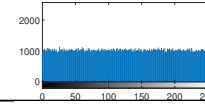
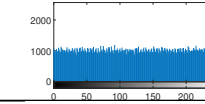
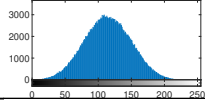
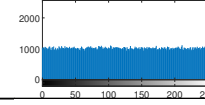
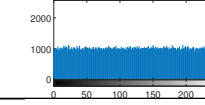
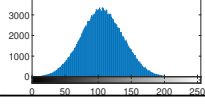
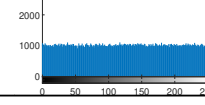
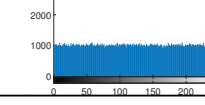
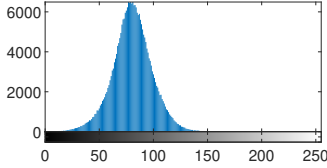
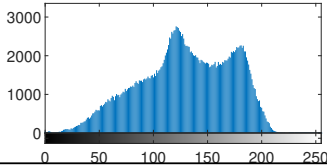
The encrypted image's histogram is utilized to evaluate the data encryption excellency.

Table 4.1: Visual test for the encryption and decryption process for the "Mandrill" image using the DFT-Baker and the proposed enhanced cryptosystem operates in several modes with various block sizes.

Block size	Mode of operation		
	MCBC	MCFB	MOFB
16 x 16			
32 x 32			
64 x 64			
E_{k1} (DFT-Baker without modes of operation)			
Deciphered image			

The cryptosystem delivers a greater level of security by enhancing the uniformity of the histogram [22]. Table 4.2 shows the resulting histogram for the encryption of the "Mandrill" image. Both MCFB and OFB modes manage to obtain a uniform histogram compared to the inherent Central Limit Theorem-based bell shape histogram that has been obtained by the MCBC mode and the DFT-Baker scheme.

Table 4.2: Histogram results for plain image, and ciphered images operates in several modes for the "Mandrill" image.

Block size	Mode of operation		
	MCBC	MCFB	MOFB
16 x 16			
32 x 32			
64 x 64			
E_{k1} (DFT-Baker without modes of operation)			
Deciphered image			

4.3.3 Correlation Coefficient Test

The correlation coefficient between plain and encrypted image's pixels is estimated in the subsequent way [21]:

$$r_{pc} = \frac{\text{cov}(p, c)}{\sqrt{G(p)}\sqrt{G(c)}}, \quad (4.7)$$

$$E(p) = \frac{1}{A \times B} \sum_{i=1}^{A \times B} p_i, \quad (4.8)$$

$$G(p) = \frac{1}{A \times B} \sum_{i=1}^{A \times B} (p_i - E(p))^2, \quad (4.9)$$

$$\text{cov}(p, c) = \frac{1}{A \times B} \sum_{i=1}^{A \times B} (p_i - E(p)) (c_i - E(c)), \quad (4.10)$$

where, p is the plain image, c is the ciphered image, and $A \times B$ is the total number of pixels. r_{pc} has a value between -1 and 1. As shown in Table 4.3, the OFB mode has better correlation coefficient values than the other two modes for the same block size. Then comes MCFB which is better than MCBC mode. Generally, all modes of operation outperform the DFT-Baker cryptosystem in terms of correlation.

4.3.4 Histogram Deviation Test

The histogram deviation is a metric that measures how much the histogram of the ciphered image is deviated from the plain one. This metric should be as large as

Table 4.3: Correlation coefficient results between plain and ciphered image pixels for the "Mandrill" image operates in several modes with various block sizes.

Block size	Mode of operation		
	MCBC	MCFB	MOFB
16 x 16	1.5×10^{-3}	1.7×10^{-3}	-1.1×10^{-3}
32 x 32	-2.2×10^{-3}	-1.1×10^{-3}	4.06×10^{-5}
64 x 64	4×10^{-3}	1.87×10^{-4}	1.45×10^{-4}
E_{k1} (DFT-Baker without modes of operation)	0.0274		

feasible [5]. The histogram deviation is calculated using the formula[20]:

$$D_H = \frac{\left(\frac{\delta_0 + \delta_{255}}{2} + \sum_{i=1}^{254} \delta_i\right)}{A \times B}, \quad (4.11)$$

where $A \times B$ denotes the plain image size and δ_i denotes the amplitude of the absolute difference between the histogram values of the plain and ciphered images at the i_{th} pixel color. As shown in Table 4.4, the MCBC outperforms the other two modes in terms of histogram deviation.

Table 4.4: Histogram deviation results

Block size	Mode of operation		
	MCBC	MCFB	MOFB
16 x 16	0.8373	0.7529	0.7573
32 x 32	0.8273	0.7533	0.7527
64 x 64	0.8091	0.7524	0.7553
E_{k1} (DFT-Baker without modes of operation)	1.1024		

4.3.5 Irregular Deviation Test

The irregular deviation metric measures the amount of irregularity that the ciphered image exhibits. The value of this metric must be as low as feasible in order to get extremely near to the ideal encryption mode [5]. The irregular deviation is calculated using the formula[20]:

$$D_I = \frac{\sum_0^{255} H_D(i)}{A \times B}, \quad (4.12)$$

where $H_D = |H(i) - M_H|$, H is the histogram for the absolute value difference between the plain image and the equivalent enciphered one, and M_H is the mean of H . As shown in Table 4.5, all modes of operation exhibit better behavior than the DFT-Baker one.

Table 4.5: Irregular deviation results

Block size	Mode of operation		
	MCBC	MCFB	MOFB
16 x 16	0.6149	0.7244	0.7245
32 x 32	0.6317	0.7227	0.7240
64 x 64	0.6578	0.7234	0.7236
E_{k1} (DFT-Baker without modes of operation)	1.0387		

4.3.6 Information Entropy Test

The entropy in image encryption is a metric that measures how much information in the bits of the ciphered image, which is mathematically expressed as [23]:

$$\text{IE}(x) = \sum_{i=1}^{2^N-1} P(x_i) \log_2 \frac{1}{P(x_i)}, \quad (4.13)$$

where, $\text{IE}(x)$ is the value of information entropy in bits, $P(x_i)$ is the probability that X_i occurs, and N is number of bits required to represent one pixel. The ideal value for $\text{IE}(x)$ for a ciphered image equals 8 as explained in [23]. Table 4.6 shows that the proposed enhanced cryptosystem outperforms the DFT-Baker one.

Table 4.6: Information entropy results

Block size	Mode of operation		
	MCBC	MCFB	MOFB
16 x 16	7.8619	7.9992	7.9975
32 x 32	7.8641	7.9992	7.9990
64 x 64	7.8598	7.9993	7.9993
E_{k1} (DFT-Baker without modes of operation)	6.3843		

4.3.7 Differential Analysis

The differential attack is one of the famous attacks to estimate the relationship between a ciphered image and its corresponding plain image. The Unified Average Changing Intensity (UACI), and Number of Pixels Change Rate (NPCR) are cal-

culated to measure the immunity of the proposed cryptosystem to such an attack. Consider two plain images P_1 and P_2 , which their size is $A \times B$. The only difference between both P_1 and P_2 is the value of one pixel. Let C_1 and C_2 be the corresponding ciphered versions of P_1 and P_2 , respectively. The UACI and NPCR are calculated as follows [26]:

$$UACI = \frac{1}{A \times B} \left[\sum_{i,j} \frac{C_1(i,j) - C_2(i,j)}{255} \right] \times 100\%, \quad (4.14)$$

$$NPCR = \frac{\sum_{i,j} f(i,j)}{A \times B} \times 100\%, \quad (4.15)$$

where,

$$f(i,j) = \begin{cases} 1 & \text{if } C_1(i,j) \neq C_2(i,j) \\ 0 & \text{if } C_1(i,j) = C_2(i,j) \end{cases} \quad (4.16)$$

The results of these tests compared to the literature are discussed in the following subsection.

4.3.8 Detailed Comparison with Existing Techniques

In this subsection, a comparison between the proposed enhanced cryptosystem and the work presented in the literature is being held. The "Lena" image with dimensions 512×512 is used as the plain image for the cryptosystem. We reproduced the results of research works in [20], [21], [3] to achieve a fair comparison. As shown in Table 4.7, the proposed enhancement behaves very similarly to the work in the literature in terms of histogram deviation. But in terms of irregular deviation, the proposed work is more superior. MCBC is better in this aspect by 44.41 %, 16%, and 44.67% compared

to [20], [21], [3]. In terms of correlation, the proposed enhancement exhibits values in the range of 10^{-4} compared to 10^{-3} in the proposed work in [20], [21], [3], [33], [34], [25], [35]. MCFB mode introduces larger values for the entropy metric compared to [20], [21], [3], [33], [34], [25], [35]. Finally, regarding the NPCR and UACI, MCBC and MCFB introduce a huge improvement compared to the work in [3] by approximately 14 times for the NPCR values, and 686 and 683 times for the UACI.

Table 4.7: Lena image comparison with literature

Scheme	Performance Metric*					
	D_H	D_I	r_{pc}	Entropy	NPCR	UACI
DFT-Baker (MCBC)	0.8851	0.5880	-2.6×10^{-4}	7.8383	99.610	33.1249
DFT-Baker (MCFB)	0.6450	0.6879	-3.12×10^{-4}	7.9993	99.5754	33.0122
DFT-Baker (MOFB)	0.6444	0.6892	2.1×10^{-4}	7.9991	95.4765	29.3409
Implementation of Baker-FrFT [20]	0.7936	1.0577	0.0017	7.7190	24.0177	0.1653
Implementation of Baker-CBC [21]	0.6443	0.7	-0.0018	7.7937	95.4990	3.6867
Implementation of Baker-CFB [21]	0.6453	0.71	0.00902	7.7190	95.4395	3.3259
Implementation of DFT Baker [3]	0.4961	1.0628	0.0416	6.6131	6.6311	0.0482
[33]	-	-	0.0159	7.992	99.579	33.422
[34]	-	-	0.0110	7.999	99.5975	33.4582
[25]	-	-	0.0011	7.9923	99.6387	33.6129
[35]	-	-	0.0026	7.9874	99.5376	32.5738

* D_H is the histogram deviation; a higher value is preferable.

* D_I is the irregular deviation; lower values are preferable.

* r_{pc} is the correlation coefficient; lower values are preferable.

4.4 Chapter Summary

The development of new multimedia applications necessitates the need for their security. Several chaotic image cryptosystems have been proposed in the literature, either in the spatial domain or in other domains, such as the frequency domain, using a variety of versions of the Discrete Fourier Transform. However, these schemes suffer from weak diffusion characteristics, and some exhibit a non-uniform histogram. The abovementioned drawbacks make these schemes vulnerable to many attacks, including differential attacks, and statistical cryptanalytic attacks, etc. For overcoming these challenges, this chapter introduced an enhanced block cipher image cryptosystem with several modes of operation based on the bit reversal concept using a 2D chaotic baker map and DFT. The experimental results generally show that the proposed enhancement is superior in terms of most quality metrics. Specifically, it was able to exhibit a uniform histogram in the MCFB and OFB modes. In addition, it offers a huge improvement in immunity to differential attacks.

CHAPTER 5

NOVEL DUAL-DOMAIN CHAOTIC IMAGE CRYPTOSYSTEM FOR CYBERSECURITY APPLICATIONS

5.1 Preface

This paper introduces a novel dual-domain chaotic image cryptosystem suitable for cybersecurity applications. The proposed cryptosystem employs an enhanced version of the standard logistic map to control proper diffusion and confusion processes, larger key space, and enhanced chaotic properties. These operations are implemented

in dual-domain, i.e., wavelet and spatial domains, respectively, to benefit from the advantages of both domains. A summary of the contributions of this chapter is as follows:

- A novel diffusion process is introduced in the wavelet domain to address the problem of weak resilience against differential attacks, which existed in the existing treatise [20], [24], [21], [3]. The proposed process in the wavelet domain is applied only on 1/16 of the pixels of the plain image, which makes it computationally more efficient compared to the other similar wavelet domain-based works, e.g., [26], where the implementation of the diffusion process was done on the whole image.
- The proposed cryptosystem solves the bell shape histogram problem associated with frequency-based cryptosystems such as in [20], [24], [3]. Particularly, the resulting histogram from the proposed cryptosystem demonstrates a favorable uniform behavior. Though uniform behavior is also achieved by a similar wavelet domain-based work [13], however, their cryptosystem exhibited poor histogram uniformity. This property is verified visually and objectively using various performance metrics in our simulation results.
- A novel key-dependent chaotic variable generator is introduced to generate the required chaotic variables for the adapted enhanced chaotic map.
- The superiority of the proposed algorithm compared to the existing state-of-the-art has been verified through various performance metrics, e.g., visual test,

different types of correlation coefficients, histogram visualization, histogram deviation, irregular deviation, mean square error, chi-square test, global entropy, and differential, randomness, cryptanalytic, and time consumption analysis.

A more elaboration on the advantages of the proposed dual-domain chaotic image cryptosystem is going to be shown in Section 5.2.4.

The upcoming sections of this chapter are organized as follows: Section 5.2 explains the detailed steps of the proposed dual-domain chaotic image cryptosystem with a discussion about its advantages, followed by Section 5.3 that introduces the simulation results and a detailed comparison with other related work in the literature. Finally, Section 5.4 delivers concluded remarks on this work.

5.2 Proposed Dual-Domain Chaotic Image Cryptosystem

In this chapter, an explanation of the proposed Dual-Domain Chaotic Image Cryptosystem is provided. As shown in Fig.5.1, the proposed dual-domain cryptosystem is implemented in two domains: wavelet, and spatial domains, respectively.

5.2.1 Generation of Chaotic Variables

The enhanced version of the logistic map mentioned in Section 2.3.3, is used throughout the proposed dual-domain image cryptosystem. The detailed role of the use of this enhanced chaotic map throughout the proposed scheme will be explained in the

upcoming section.

However, this improved chaotic map requires an initial condition and control parameter to work, both of which will be called chaotic variables. In this section, we introduce a Key Chaotic Variable Generator (KCVG).

The KCVG is fed with a secret key to generate the desired abovementioned chaotic variables. The fundamental objective is to design an algorithm that provokes secret key-sensitive chaotic variables.

In previous image chaos-based algorithms [36], [37], [38], [39], [40], [23], [22] , the chaotic variables were constructed directly by changing the fixed or floating point representation of the chaotic variables with the secret key bits. However, the proposed KCVG modifies the chaotic point indirectly; in which a chaotic perturbation method that uses the secret key bits' value and location is used to achieve this goal.

Generally speaking, in order to resist brute force attacks, a secret key should have a minimum length of 128 bits, and for future quantum computers-based ones, it should be a minimum length of 256 bits [41], [42], [43]. Therefore, the proposed KCVG adapts a 512-bit secret key to ensure its immunity against current and future quantum-powered brute force attacks. Regardless and diverging from traditional block ciphers, the KCVG demonstrates a noteworthy characteristic, wherein the secret key's dimensionality remains adaptable, affording users the prerogative to select a secret key size that aligns precisely with the exigencies of their specific application. Later in this section, we will provide more insight into this matter.

Firstly, the 512-bit secret key is divided into overlapped, bit-reversed 201-bit blocks. Every single block introduces a chaotic variable in the range between 0 and 1.

Secondly, the 201-bit value is utilized to modify the control parameter as well as the initial chaotic point. These separated points are used to construct new initial values and control parameters, and so on.

Finally, the last three control parameter values and three chaotic initial value points are fed to the enhanced logistic Pseudo Random Number Generators (PRNGs) in the proposed dual-domain image cryptosystem.

The detailed steps of the KCVG are as follows:

- The KCVG asks the user to enter the Main encryption key $Main_key$, and the Block size $Block_size$. Assuming that the user follows our recommendation, $Main_key = 512$, and $Block_size = 201$.
- The $dec2bin()$ function converts the $Main_key$ to its binary representation and stores the value in the variable $Main_key_Binary$. The value of this variable will be assigned to $Main_key_Binary_temp$.
- The function $length()$ obtains the number of bits of the $Main_key_Binary$. The total number of blocks throughout the algorithm generally is calculated using the following mathematical equation:

$$Total\ number\ of\ blocks = secret\ key\ size - (block\ size - 1). \quad (5.1)$$

This equation enables the KCVG to work with different secret key sizes. So, for our example: $No_Blocks = 512 - (201 - 1) = 312$.

- The first two chaotic variables $x(1) = 0.25$, and $r(1) = 2.9586$ has been chosen randomly; taking into consideration that the value of x is between 0 and 1, and the r value is from 0 to infinity [1].
- The first loop will iterate 312 times. The first block equals the first 201 bits from the secret key. However, the consequence block is obtained after bit reversing the bits from 201 to 512. The bit reversal operation is done by the function *flipplr*(). The operation of obtaining the consequence blocks is continued until the end of the loop. The bit reversal method is shown in [44] to be a powerful, simple, and low computational burden operation to enhance the chaotic properties. Combing the bit reversal and overlapping processes on the blocks maximizes the sensitivity of the secret key on the generated chaotic variables.
- The nested loop inside the first one is used to count the number and location of zeros in each block to create perturbed chaotic points according to the following equation:

$$v_2(i) = \sum_{j=1}^{Block_size} (2 \times i)^{-j}, \quad (5.2)$$

where $i = 1, 2, 3, \dots, No_Blocks$ is the order of the block, j is the location of the zeros inside the block, and v_2 is the perturbed chaotic point generated from a block. A vector that contains all the perturbed chaotic points v_3 is created from the v_2 values.

- The final loop in the KCVG mission is to generate the chaotic variables x (initial value) and r (control parameter) using the perturbed chaotic vector v_3 and the

concept of the enhanced logistic map in [1]. These equations are expressed mathematically as follows:

$$r(a) = (r(a-1) \times x(a-1) \times v_3(a-1) \times 2^{32}) \bmod 10, \quad (5.3)$$

$$g = r(a) \times x(a-1), \quad (5.4)$$

$$f = r(a) \times g \times (1 - g), \quad (5.5)$$

$$x(a) = (f + (1/x(a-1))) \bmod 1, \quad (5.6)$$

where $a = 2, 3, 4, \dots No_Blocks$.

- Finally, the last three control parameter values and three chaotic initial value points are obtained to be the output of the KCVG. Later on, these values are passed to the dual-domain image cryptosystem as the chaotic variables for the enhanced logistic-based PRNGs.

It is noteworthy to mention that the generation of chaotic variables (initial variables and control parameters) from KCVG, and their corresponding random sequences (which will be explained in the upcoming section) are executed once per secret key. Consequently, this can also be computed before the execution of the main cryptosystem algorithm. As a result, this prevents additional computational overhead. Algorithm 1 outlines the precise steps required for the generation of the necessary chaotic variables for the enhanced logistic-based PRNGs.

Furthermore, the proposed dual-domain image cryptosystem is a symmetric-key cryptographic algorithm, necessitating the utilization of a shared secret key between the communicating entities: the sender and receiver. Thus, to ensure the utmost security, the secret key ought to be exchanged through established and reliable means, such as employing public-key encryption techniques.

Algorithm 1: Key Chaotic Variable Generator (KCVG)

Input: Main encryption key *Main_key*, Block size *Block_size*
Output: Initial values x_1 , x_2 & x_3 , Control paramters r_1 , r_2 , & r_3
Main_key_Binary $\leftarrow$ *dec2bin*(*Main_key*);
Main_key_Binary_temp $\leftarrow$ *Main_key_Binary*;
Binary_length_Main_key = *length*(*Main_key_Binary*);
No_Blocks = *Binary_length_Main_key* - (*Block_size* - 1);
 $x(1) \leftarrow 0.25$;
 $r(1) \leftarrow 2.9586$;
 $v_1, v_2, v_3 = []$;
for $i = 1 : \text{No_Blocks}$ **do**
 $v_1(1 : \text{Block_size}) = \text{Main_key_Binary_temp}(i : i + \text{Block_size} - 1)$;
 $\text{Main_key_Binary_temp}(i + 1 : \text{end}) = \text{fliplr}(\text{Main_key_Binary_temp}(i + 1 : \text{end}))$;
 $v_2(i) = 0$;
 for $j = 1 : \text{Block_size}$ **do**
 if $v_1(j) == "0"$ **then**
 $v_2(i) = v_2(i) + (2 \times i)^{-j}$;
 end
 end
 $v_3 = [v_3 \ v_2(i)]$;
end
for $a = 2 : \text{No_Blocks}$ **do**
 $r(a) = (r(a-1) \times x(a-1) \times v_3(a-1) \times 2^{32}) \bmod 10$;
 $g = r(a) \times x(a-1)$;
 $f = r(a) \times g \times (1 - g)$;
 $x(a) = (f + (1/x(a-1))) \bmod 1$;
end
 $x_1 = x(\text{end} - 2)$, $x_2 = x(\text{end} - 1)$, $x_3 = x(\text{end})$;
 $r_1 = r(\text{end} - 2)$, $r_2 = r(\text{end} - 1)$, $r_3 = r(\text{end})$;

5.2.2 Encryption Scheme for Proposed Dual-Domain Cryptosystem

This section provides a comprehensive exposition of the implementation of the encryption component within the proposed dual-domain image cryptosystem, shown in Fig.5.1a. The encryption scheme under consideration encompasses two primary pro-

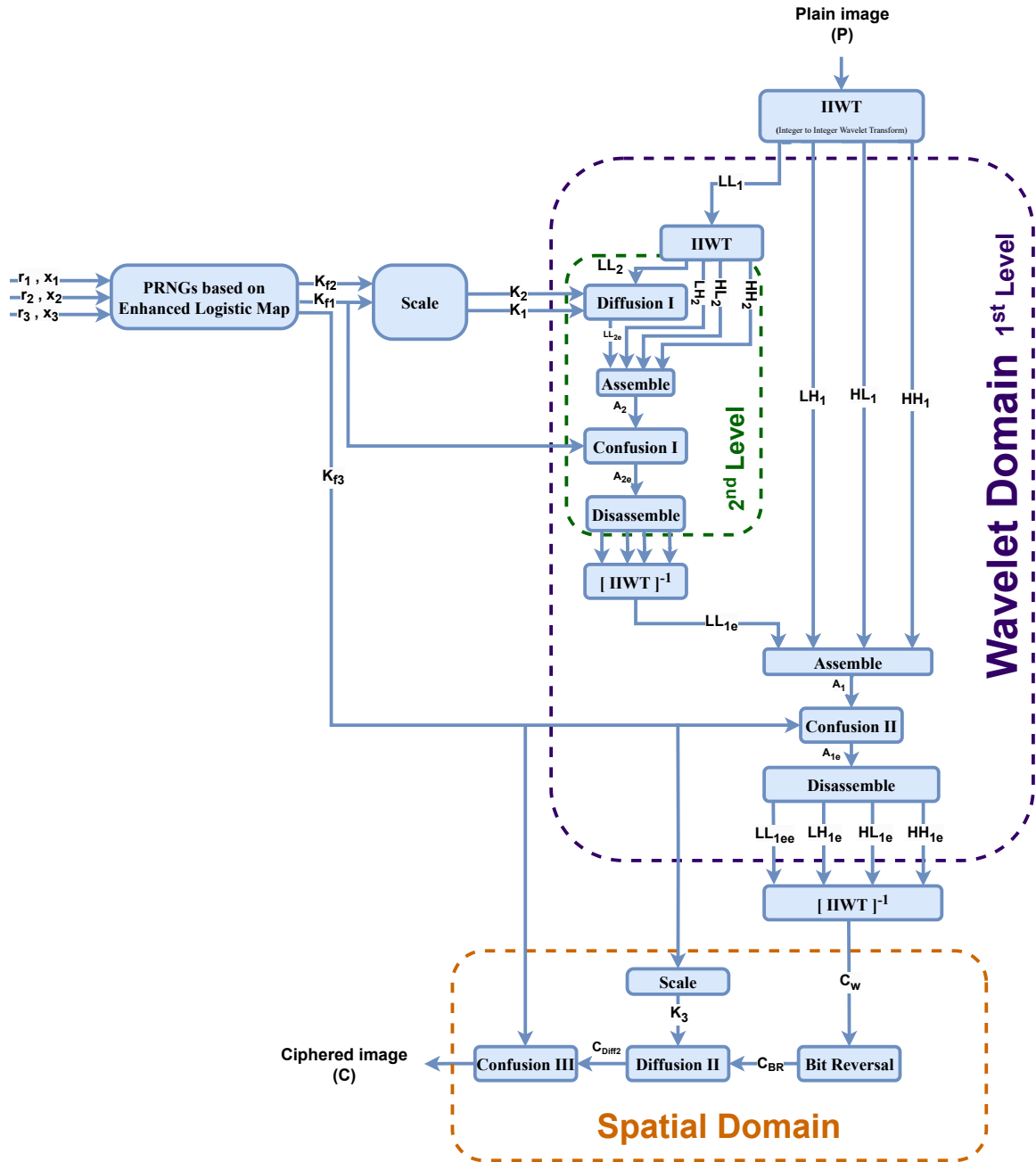
cesses: diffusion and confusion, which simultaneously are applied in both the wavelet and spatial domains.

The main reason behind the adaption of the wavelet transform for the proposed dual-domain cryptosystem came from its ability to provide an integer-to-integer version in contrast to other transforms, such as DFT that results in non-real complex numbers. This property effectively enables the implementation of customized diffusion processes across the wavelet domain. In addition, a bit reversal operation is employed as an intermediate mechanism to interconnect wavelet and spatial domains effectively.

The diffusion process consists of two principal blocks: Diffusion I and Diffusion II. These blocks are meticulously designed based on conditioned chaining processes, which are tailored to the specific implementation domain. This deliberate approach aims to bolster the resilience of the proposed dual-domain image cryptosystem against potential differential attacks.

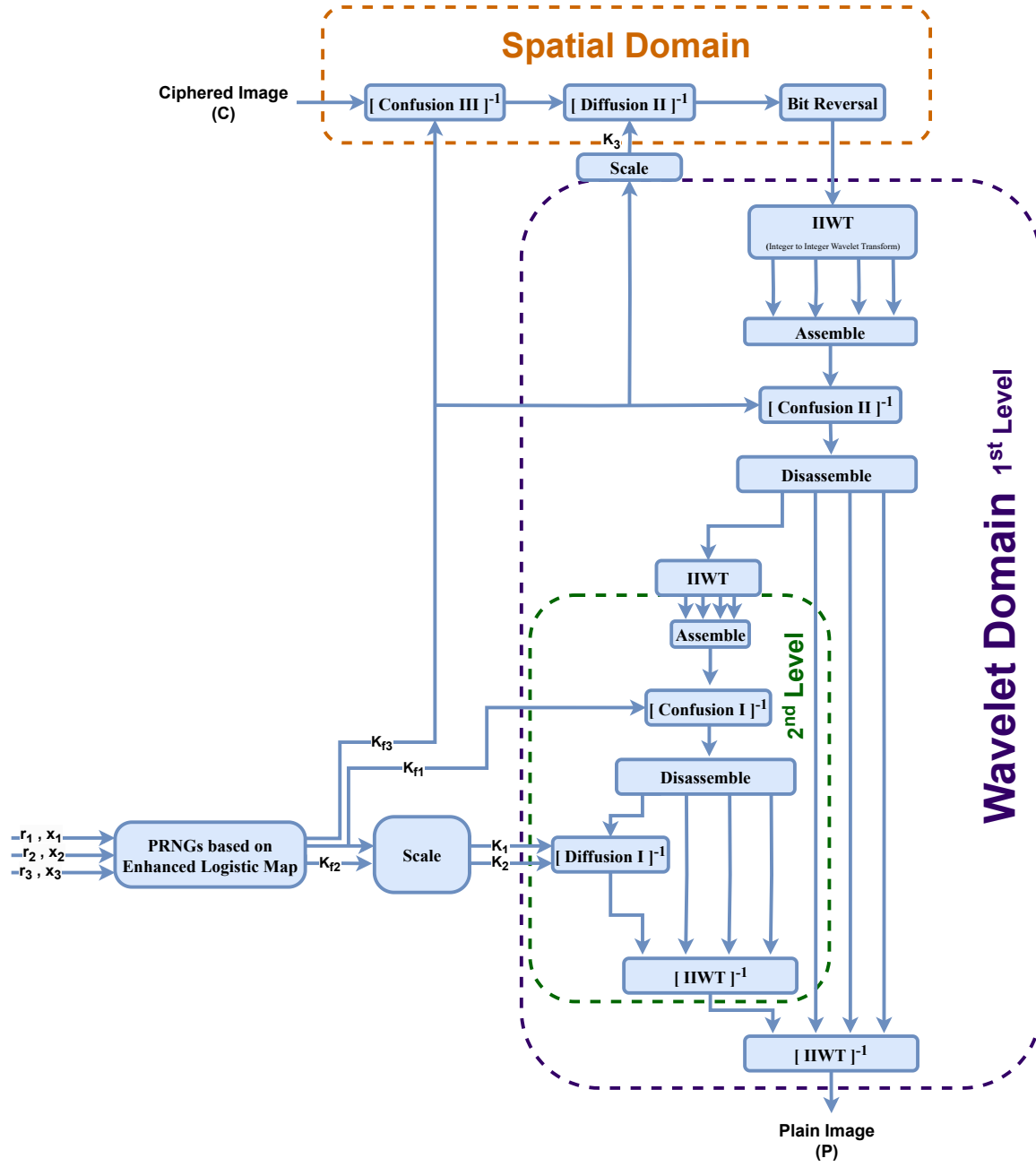
Furthermore, the confusion process contains three blocks: Confusion I, II, and III. The first two blocks are implemented in the wavelet domain to minimize the correlation between the different wavelet sub-bands, and to maximize the spreading of the diffused band over the non-diffused ones. The last block is implemented in the spatial domain to maximize the chaining effect of the previous confusion block.

It is noteworthy that, unlike other works in literature [45], [20], [21], [23], all the confusion and diffusion blocks are key-dependant, which increases the immunity of the proposed dual-domain image cryptosystem against different cryptanalytic attacks. As shown in Fig.5.1a, the detailed steps for the encryption process are as follows:



(a) Encryption scheme.

Figure 5.1: The proposed dual-domain image cryptosystem scheme.



(b) Decryption scheme.

Figure 5.1: The proposed dual-domain image cryptosystem scheme.

- Load the plain image P and set its dimensions to $M \times M$, with proper padding as needed.
- The Key Chaotic Variable Generator (KCVG), explained in section 5.2.1, is used to generate the chaotic variables r_i (control parameter) and x_i (initial value).
- These chaotic variables are used to generate random fractional vectors K_{fi} , using the enhanced logistic map in [1], where $i = 1, 2, 3$, with lengths $\frac{M}{2}$, $\frac{M}{4}$, and M respectively. The values of these vectors are in the range of $[0, 1]$.
- The random fractional vectors K_{fi} are used to obtain the encryption key vectors K_i , where each element in this vector is an 8-bit unsigned integer. This operation is expressed as follows:

$$K_i = uint8((K_{fi} \times 2^{32}) \bmod 256), \quad (5.7)$$

where *uint8* is an 8-bit unsigned integer data type operator, and *mod* is the modulo operator. The number 256 is chosen to ensure that the output will be always in the range of an 8-bit grayscale image.

- The plain image P is converted to the wavelet domain to obtain the first-level decomposition of four sub-bands LL_1, LH_1, HL_1 , and HH_1 , by the Integer to Integer Wavelet Transform block (*IWT*). Each band is a matrix with size $\frac{M}{2} \times \frac{M}{2}$.
- The *IWT* block is applied again on the first- level of the Low-Low band (LL_1)

to obtain the second-level decomposition of four sub-bands LL_2, LH_2, HL_2 , and HH_2 . Each band is a matrix with size $\frac{M}{4} \times \frac{M}{4}$.

- LL_2 matrix is applied to the *Diffusion I* block to obtain its ciphered version LL_{2e} . The main role of the *Diffusion I* block is to satisfy a good diffusion characteristic. This goal is achieved by applying a chaining XOR operation conditioned on the sign of the first $\frac{M}{4} \times \frac{M}{4}$ perspective elements in the HH_1 matrix. The diffusion equation is as follows:

$$LL_{2e}(i) = LL_2(i) \oplus K_j(i) \oplus B_e(i), \quad i = 1, 2, \dots, \frac{Q}{16}, \quad (5.8)$$

where $Q = M^2$, $\oplus$ indicates the XOR operation, and $B_e(i)$ is governed by the following rule:

$$B_e(i) = \begin{cases} 0, & \text{if } i = 1 \\ (LL_{2e}(i-1) \times i)^4 \bmod 256, & \text{if } i \neq 1 \end{cases} \quad (5.9)$$

and $K_j(i)$ is governed by:

$$K_j(i) = \begin{cases} K_1(i), & \text{if } HH_1(i) \leq 0 \\ K_2(i), & \text{otherwise} \end{cases} \quad (5.10)$$

A detailed pseudo-code illustrating the *Diffusion I* block is shown in Algorithm 2. The conditioned keys combined with the chaining process maximize the encryption randomness, leading to a higher diffusion effect.

Algorithm 2: Diffusion I algorithm

Input: encryption keys vectors K_1 & K_2 , LL_2 , HH_1
Output: Ciphered matrix LL_{2e}
 $LL_{2e} \leftarrow \text{zeros}(1, \text{numel}(LL_2));$
 $LL_2 \leftarrow LL_2(\cdot)^\top;$
for $i = 1 : \text{length}(LL_2)$ **do**
 if $i == 1$ **then**
 $B_e(i) \leftarrow 0;$ /* Condition for the chained XOR */
 else
 $B_e(i) \leftarrow ((LL_{2e}(i-1) \times i)^4) \bmod 256;$
 end
 if $HH_1(i) \leq 0$ **then**
 $LL_{2e}(i) = LL_2(i) \oplus K_1(i) \oplus B_e(i);$
 else
 $LL_{2e}(i) = LL_2(i) \oplus K_2(i) \oplus B_e(i);$
 end
end
 $LL_{2e} = \text{reshape}(LL_{2e}, \text{size}(LL_2));$

- The *Assemble* block combines the remaining second-level decomposition sub-bands with the resulted ciphered second-level low-low band as follows:

$$A_2 = \begin{bmatrix} LL_{2e} & LH_2 \\ HL_2 & HH_2 \end{bmatrix}, \quad (5.11)$$

where A_2 is the second-level combined sub-bands matrix with size $\frac{M}{2} \times \frac{M}{2}$.

- The *Confusion I* block takes matrix A_2 as its input to produce a shuffled version A_{2e} . The adapted shuffling process in this work is the well-known "Algorithm P" [46], which is seeded with the random fractional vector K_{f1} as its random indices. This algorithm has been chosen for its proven low-burden complexity, simplicity, and high performance in the literature [46], [47], [48], [49], [50], [51], [52], [53], [54], [55], [56], [57], [58], [59], [60], [61], [62]. However, the *Confusion I* block can be any efficient shuffling algorithm such as "Binary Sampling Tree", "Row-Column Rotation-Based", and "Successive Pair-wise Shuffling-Based" algorithms in [63], and "Block Generated Permutation" in [64]. A detailed illus-

tration of the confusion process is in Algorithm 3.

Algorithm 3: Confusion algorithm

Input: Random fractional vector K_f , P any data matrix
Output: Ciphered matrix C
 $P_1 \leftarrow P(\cdot)^\top$;
 $N \leftarrow \text{length}(P_1)$
for $i = 1 : N - 1$ **do**
 $j = \text{round}((N - i) \times K_f(i)) + 1$;
 $\text{temp} \leftarrow P_1(N - i + 1)$;
 $P_1(N - i + 1) \leftarrow P_1(j)$;
 $P_1(j) \leftarrow \text{temp}$;
end
 $C = \text{reshape}(P_1, \text{size}(P))$;

- The A_{2e} is applied to the *Disassemble* block to get the new encrypted second-level decomposition sub-bands. These sub-bands are passed to the inverse Integer to Integer Wavelet Transform block $[\text{IIWT}]^{-1}$ to get the first encrypted version of the first low-low subband LL_{1e} .
- The ciphered first-level low-low band LL_{1e} , along with the remaining first-level decomposition sub-bands, are assembled as follows:

$$A_1 = \begin{bmatrix} LL_{1e} & LH_1 \\ HL_1 & HH_1 \end{bmatrix}, \quad (5.12)$$

where A_1 is the first-level combined sub-bands matrix with size $M \times M$.

- The A_2 is passed to the second shuffling block *Confusion II* to get its ciphered version A_{2e} . The same Algorithm 3 is used for shuffling but with the random fractional vector K_{f3} as its random indices.
- The *Disassemble* block divides the A_{2e} matrix into four ciphered first-level decomposition sub-bands LL_{1ee} , LH_{1e} , HL_{1e} , and HH_{1e} . These ciphered sub-bands are

devolved to the $[\text{IIWT}]^{-1}$. The output of the $[\text{IIWT}]^{-1}$ block is the spatial-domain ciphered matrix C_w .

- The C_w matrix is applied to the *Bit Reversal* block; to get the C_{BR} matrix. This is expressed mathematically as:

$$C_{BR} = R_B[C_w], \quad (5.13)$$

where R_B is the bit reversal operator, i.e. for a 8-bit pixel, $R_B[b_0, b_1, b_2, b_3, b_4, b_5, b_6, b_7] = [b_7, b_6, b_5, b_4, b_3, b_2, b_1, b_0]$, and C_{BR} is the bit reversed matrix.

The proposed insertion of the simple low computational burden bit reversal operation has been proven in the literature [65], [66], [44], [67] and experimentally that it leads to significantly improved randomness and statistical characteristics of the overall ciphering process.

- The *Diffusion II* block is the second diffusion block in the proposed cryptosystem. In particular, it ensures that the proposed cryptosystem is robust against differential attacks. A simple chaining XOR operation is employed to achieve this objective. The diffusion process is defined as follows:

$$C_{Diff2}(i) = C_{BR}(i) \oplus K_3(i) \oplus b_e(i), \quad i = 1, 2, 3, \dots, Q, \quad (5.14)$$

where C_{Diff2} is the output matrix of the *Diffusion II* block, C_{BR} is the bit

reversed version of C_w matrix, and $b_e(i)$ is governed by the following rule:

$$b_e(i) = \begin{cases} 0, & \text{if } i = 1 \\ C_{Diff2}(i-1), & \text{if } i \neq 1, \end{cases} \quad (5.15)$$

A detailed illustration for all operations inside the *Diffusion II* block is shown in Algorithm 4

Algorithm 4: Diffusion II algorithm

Input: encryption key vector K_3 , C_{BR}

Output: Ciphered matrix C_{Diff2}

$C_{Diff2} \leftarrow \text{zeros}(1, \text{numel}(C_{BR}))$;

$C_{BR} \leftarrow C_{BR}(\cdot)^\top$;

for $i = 1 : \text{length}(C_{BR})$ **do**

if $i == 1$ **then**

$b_e(i) \leftarrow 0$

else

$b_e(i) \leftarrow C_{Diff2}(i-1)$;

end

$C_{Diff2}(i) = C_{BR}(i) \oplus K_3(i) \oplus b_e(i)$;

end

$C_{Diff2} = \text{reshape}(C_{Diff2}, \text{size}(C_{BR}))$;

- The last step to obtain the ciphered image C is to apply the third shuffling block: *Confusion III*. Also, this operation follows Algorithm 3, with K_{f3} as its random fractional vector for the random indices.

5.2.3 Decryption Scheme for Proposed Dual-Domain Cryptosystem

The process of decryption involves almost the same operations as encryption but in reverse order. As shown in Fig.5.1b, the deciphering process of the ciphered image C implicates two stages; one in the spatial domain and another in the wavelet domain, respectively. Moreover, the inverse version of the following blocks: *Confusion I*, *II*,

and *III*, and *Diffusion I*, and *II* have been used throughout the scheme to extract the plain image P . The operator $[]^{-1}$ indicates the reverse operation of a block. Furthermore, to successfully recover the plain image P , all the keys that have been used for the encryption process must be reused for the process of decryption to ensure a successful recovery of the ciphered image C .

5.2.4 Discussion

As shown in the abovementioned sections, the proposed dual-domain image cryptosystem has the ability to perform the encryption process on different plain images with diverse sizes using enhanced chaotic maps. Furthermore, the development of the proposed dual-domain image cryptosystem is to guarantee a successful achievement of both crucial cryptography properties: diffusion and confusion. As a result of that, the proposed dual-domain image cryptosystem is advantageous in the following manner:

- Conventional frequency domain-based cryptosystems apply the diffusion process on the whole image pixels [3], [25], [68], [24], which is considered as an added complexity overhead. However, the proposed diffusion process in the wavelet domain includes an XOR chaining process applied only to 1/16 of the pixels of the plain image. As a result, this compensates for the complexity and time consumption of going in and out of the wavelet domain. In addition, it allows the cryptosystem to benefit from the high confusion property associated with frequency domain-based cryptosystems [20], [24].
- The abovementioned property does not decrease the diffusion quality. On the

contrary, the condition that controls the chaining process combined with the fast-applied confusion process maximizes the effect of other bands on the diffusion process. Thus, this causes the statistics of the plain image to spread throughout the entire ciphered image.

- The adapted enhanced logistic map [1], in the proposed dual-domain image cryptosystem; has high Lyapunov Exponent (LE) and Largest Lyapunov Spectrum (LSE) values, indicating increased chaotic dynamics and ergodicity. As a result, these traits have a visible impact on the performance of the confusion process.
- The proposed dual-domain image cryptosystem requires only two rounds of operation (one in the wavelet and another in the spatial domains) to reach robust diffusion and confusion characteristics. On the other hand, traditional block ciphers require a significant number of rounds to achieve the same level of robustness. For example, work in [69] requires a minimum of 5 rounds for practical security.
- The performance of the proposed dual-domain image cryptosystem is affected by the selection of the secret key, particularly in terms of the confusion and diffusion processes. This property distinguishes it from conventional cryptosystems wherein these operations remain static and independent of the cryptographic key.
- The derived initial values and control parameters from the confidential key have a high sensitivity to any minor fluctuation in it. The property in question can be attributed to the KCVG design, which effectively employs bit reversal and

chaotic perturbation techniques to generate these values. For the adapted secret key length of 512-bit, the proposed dual-domain image cryptosystem uses three initial values and three control parameters. Each chaotic variable is a 201-bit fixed-point number. As a result, the proposed dual-domain image cryptosystem relies on 1206 bits for the generation of the random sequences. Besides that, as mentioned before, the secret key length is adaptable to suit the user application.

5.3 Simulation Results

In this section, we proceed with a comprehensive assessment of the obtained results by employing a variety of encryption quality metrics. Our experimental environment consists of an Intel(R) Core(TM) i7-11800H CPU processor with a clock speed of 2.3 GHz, 16 GB of RAM, and a Microsoft Windows 11 operating system. To run our encryption and decryption programs, we rely on Matlab 2022a.

The proposed dual-domain chaotic image cryptosystem has been tested with multiple test images with diverse frequency spectrum characteristics, ranging from images with high-frequency emphasis (such as the Mandrill image) to images with low-frequency emphasis (such as the Cameraman image).

Moreover, to ensure the reliability of the obtained results, 10^3 ciphered images are obtained for each plain image with completely random 10^3 secret keys. Then, each quality metric is computed for each 10^3 ciphered image and averaged over them to obtain the final value. As a result of this approach, the calculated quality metrics are more immune against any bias in the performance.

5.3.1 Visual Test

One of the most straightforward evaluation methodologies is the visual examination, whereby imperfections are discerned through direct observation with the human eye. Although it is less reliant on advanced techniques compared to alternative approaches, it remains a highly dependable and efficacious method for identifying all manifestations [70].

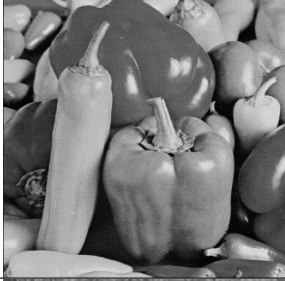
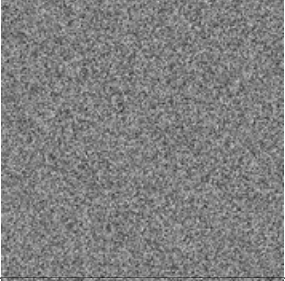
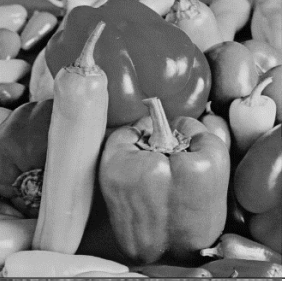
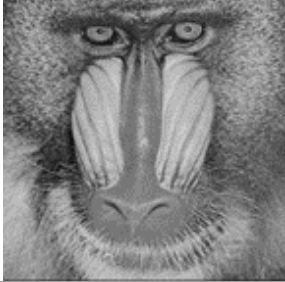
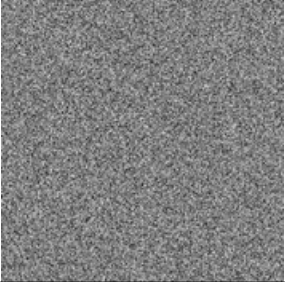
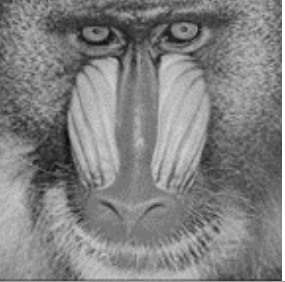
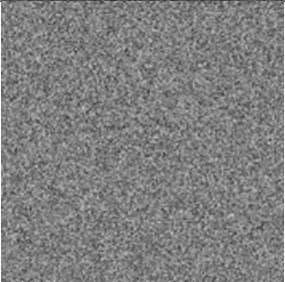
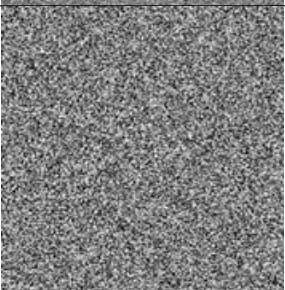
Table 5.1 shows the ciphered and deciphered results of multiple plain images: Peppers, Mandrill, Boat, and Cemeraman with sizes 512×512 , 512×512 , 512×512 , and 256×256 , respectively. The proposed methodology facilitates the encryption process by modifying the characteristics of encrypted images in such a manner that they lost their complementary plain images' features, ensuring their encryption efficiency.

5.3.2 General Correlation Coefficient Test

The correlation coefficient test serves as a quantitative metric for evaluating the relationship between two variables [71]. In the context of image processing, it is observed that pixels exhibit a strong correlation with one another [72]. Consequently, image encryption algorithms are primarily oriented toward mitigating the pixel associations within an encrypted image [73]. Moreover, The correlation coefficient test has multiple versions: general correlation coefficient test, correlation coefficient of adjacent pixels, and correlation coefficient between plain and ciphered image test. A detailed description of each test is provided in the upcoming sections.

The general correlation coefficient between plain and encrypted image's pixels is

Table 5.1: Visual test for the encryption and decryption process for multiple images

Image Name & Dimension	Plain Image	Ciphered Image	Deciphered Image
Peppers 512x512			
Mandrill 512x512			
Boat 512x512			
Cameraman 256x256			

estimated in the subsequent way [74]:

$$r_g(p, c) = \frac{\text{cov}(p, c)}{\sqrt{G(p)}\sqrt{G(c)}} \quad (5.16)$$

$$E(p) = \frac{1}{M \times N} \sum_{i=1}^{M \times N} p_i \quad (5.17)$$

$$G(p) = \frac{1}{M \times N} \sum_{i=1}^{M \times N} (p_i - E(p))^2 \quad (5.18)$$

$$\text{cov}(p, c) = \frac{1}{M \times N} \sum_{i=1}^{M \times N} (p_i - E(p)) (c_i - E(c)) \quad (5.19)$$

where p is the plain image, c is the ciphered image, and $M \times N$ is the total number of pixels. $r_g(p, c)$ has a value between -1 and 1. The value of +1 represents a full positive correlation, while -1 indicates a full negative correlation between the plain and ciphered image. As a result, a correlation coefficient of 0 indicates that the images are not related.

As evidenced by the data presented in Table 5.2, the general correlation coefficient outcomes between the pixel values of plain images and their respective encrypted counterparts exhibit notably favorable values. Table 5.3, illustrates the general correlation coefficient results between plain and ciphered image pixels for the "Lena" image compared with the literature. The results demonstrate the superiority of the proposed dual-domain image cryptosystem over other work in the literature.

5.3.3 Correlation Coefficient of Adjacent Pixels

The general correlation coefficient is a practical mathematical tool for calculating the overall dependency between the tested pixels. However, in some cases, it fails to determine a good insight into the local dependency [76]. Thus, the author in [77] proposed a solution for this problem by introducing horizontal, and vertical correlation coeffi-

Table 5.2: General correlation coefficient results between plain images with different sizes and their corresponding ciphered ones.

Image	Proposed Scheme
Peppers 512×512	1.7876×10^{-05}
Mandrill 512×512	8.4977×10^{-05}
Boat 512×512	1.0791×10^{-04}
Lena 256×256	-2.8612×10^{-04}
Cameraman 256×256	1.4863×10^{-04}

Table 5.3: General correlation coefficient results between plain and ciphered image pixels for the” Lena” image compared with the literature.

General Correlation Coefficients	Proposed Scheme (Lena 256×256)	[75]	[21]	[20]
	-2.8612×10^{-04}	3×10^{-4}	1.5×10^{-3}	1.7×10^{-3}

cients as more efficacious approaches. Therefore, this paper adapts this approach to compute the horizontal, vertical, and diagonal correlation coefficients between adjacent pixels within the ciphered image. Mathematically, the vertical, horizontal, and diagonal correlation coefficients between adjacent pixels can be expressed respectively, as follows [77]:

$$r_V(c, c) = \frac{\sum_{i=1}^{M-1} \sum_{j=1}^N (c_{(i,j)} - E(c)) (c_{(i+1,j)} - E(c))}{\sqrt{\sum_{i=1}^{M-1} \sum_{j=1}^N (c_{(i,j)} - E(c))^2 \sum_{i=1}^{M-1} \sum_{j=1}^N (c_{(i+1,j)} - E(c))^2}}, \quad (5.20)$$

$$r_H(c, c) = \frac{\sum_{i=1}^M \sum_{j=1}^{N-1} (c_{(i,j)} - E(c))(c_{(i,j+1)} - E(c))}{\sqrt{\sum_{i=1}^M \sum_{j=1}^{N-1} (c_{(i,j)} - E(c))^2 \sum_{i=1}^M \sum_{j=1}^{N-1} (c_{(i,j+1)} - E(c))^2}}, \quad (5.21)$$

$$r_D(c, c) = \frac{\sum_{i=1}^{M-1} \sum_{j=1}^{N-1} (c_{(i,j)} - E(c))(c_{(i+1,j+1)} - E(c))}{\sqrt{\sum_{i=1}^{M-1} \sum_{j=1}^{N-1} (c_{(i,j)} - E(c))^2 \sum_{i=1}^{M-1} \sum_{j=1}^{N-1} (c_{(i+1,j+1)} - E(c))^2}}, \quad (5.22)$$

where M is the height of the ciphered image, N is the width of the ciphered image, i and j are the pixel indices of the ciphered image. $E(c)$ is the expectation of ciphered image pixels' values.

As shown in Table 5.4, the correlation coefficients of the adjacent pixels exhibit advantageous values. Furthermore, Table 5.5 shows a comparison between the proposed dual-domain image cryptosystem and literature in terms of the correlation coefficients of adjacent pixels. The comparison is done using the Ciphered version of the "Cameraman" image. Accordingly, the proposed cryptosystem demonstrates better results than other work in terms of vertical, horizontal correlation coefficients. But, the cryptosystem in [22] is better in the diagonal correlation coefficient. Despite that, the performance of the proposed cryptosystem is very close to the cryptosystem in [22].

Table 5.4: Results for correlation coefficients of adjacent pixels for multiple ciphered images.

Image	Plain Image			Ciphered Image		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Peppers 512 × 512	0.9791	0.9767	0.9638	3.5055×10^{-05}	3.8669×10^{-07}	-5.294×10^{-05}
Mandrill 512 × 512	0.7586	0.8665	0.7261	1.2469×10^{-04}	2.0493×10^{-05}	1.7773×10^{-05}
Boat 512 × 512	0.9787	0.9630	0.9458	-4.6101×10^{-06}	-4.6162×10^{-05}	-6.9288×10^{-06}
Lena 256 × 256	0.9695	0.9401	0.9180	-2.4894×10^{-04}	2.4062×10^{-05}	-2.4323×10^{-04}
Cameraman 256 × 256	0.9592	0.9335	0.9087	-1.2941×10^{-04}	-1.5704×10^{-05}	1.3730×10^{-04}

Table 5.5: Results for correlation coefficients of adjacent pixels for the ciphered version of "Cameraman" image compared with the literature .

Encryption Scheme	Ciphered Image (Cameraman 256×256)		
	Horizontal	Vertical	Diagonal
Proposed	-1.2941×10^{-04}	-1.5704×10^{-05}	1.3730×10^{-04}
[23]	-0.0003	-0.0039	0.0037
[22]	-0.01041	-0.00337	-0.00011
[45]	-0.001211	-0.006940	-0.0004557
[26]	0.0018	-0.0014	-0.0181
[78]	0.0010	-0.0016	-0.0123
[79]	3.361×10^{-1}	3.802×10^{-1}	-2.711×10^{-1}

5.3.4 Correlation Coefficient between Plain and Ciphered Images

One of the essential metrics for evaluating the effectiveness of encryption schemes is the correlation coefficient between plain and ciphered images [5]. This metric serves as an indicator of the degree of association between both of them. However, as we discussed before, the reliability of the general correlation coefficient alone may not yield sufficient insights into the encryption local's association quality. Hence, the conduction of the correlation coefficient between plain images and encrypted images vertically, horizontally, and diagonally is introduced, which is expressed by the following equations, respectively [23]:

$$r_V(p, c) = \frac{\sum_{i=1}^{M-1} \sum_{j=1}^N (p_{(i,j)} - E(p))(c_{(i+1,j)} - E(c))}{\sqrt{\sum_{i=1}^{M-1} \sum_{j=1}^N (p_{(i,j)} - E(p))^2 \sum_{i=1}^{M-1} \sum_{j=1}^N (c_{(i+1,j)} - E(c))^2}}, \quad (5.23)$$

$$r_H(p, c) = \frac{\sum_{i=1}^M \sum_{j=1}^{N-1} (p_{(i,j)} - E(p))(c_{(i,j+1)} - E(c))}{\sqrt{\sum_{i=1}^M \sum_{j=1}^{N-1} (p_{(i,j)} - E(p))^2 \sum_{i=1}^M \sum_{j=1}^{N-1} (c_{(i,j+1)} - E(c))^2}}, \quad (5.24)$$

$$r_D(p, c) = \frac{\sum_{i=1}^{M-1} \sum_{j=1}^{N-1} (p_{(i,j)} - E(p))(c_{(i+1,j+1)} - E(c))}{\sqrt{\sum_{i=1}^{M-1} \sum_{j=1}^{N-1} (p_{(i,j)} - E(p))^2 \sum_{i=1}^{M-1} \sum_{j=1}^{N-1} (c_{(i+1,j+1)} - E(c))^2}}, \quad (5.25)$$

where p is the plain image, c is the ciphered image, M is the height of the image, N is the width of the image, i and j are the pixel indices. $E(c)$ is the expectation of ciphered image pixels' values. $E(p)$ is the expectation of plain image pixels' values.

Table 5.6 presents the correlation coefficients between plain images' pixels and their corresponding ciphered ones. Results show very small values in all three types of correlation, which indicates favorable behavior. Finally, Table 5.7 demonstrates the superiority of the proposed dual-domain image cryptosystem over the cryptosystems in [23], [22] in all three types of correlation: vertically, horizontally, and diagonally.

Table 5.6: Results for correlation coefficients between plain images and their corresponding ciphered images pixels .

Image	Correlation Coefficients of Plain and Cipher Images		
	Horizontal	Vertical	Diagonal
Peppers 512 × 512	3.8290×10^{-05}	2.0993×10^{-05}	3.6141×10^{-05}
Mandrill 512 × 512	1.5174×10^{-04}	6.7722×10^{-05}	1.2088×10^{-04}
Boat 512 × 512	-1.0554×10^{-04}	-4.9991×10^{-05}	-7.1404×10^{-05}
Lena 256 × 256	-9.7588×10^{-05}	-9.9300×10^{-05}	-1.4385×10^{-04}
Cameraman 256 × 256	9.8938×10^{-05}	1.1843×10^{-04}	1.2306×10^{-04}

Table 5.7: Results for the coefficients of correlation between plain and ciphered pixels for the "Peppers" image compared with the literature.

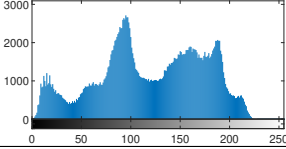
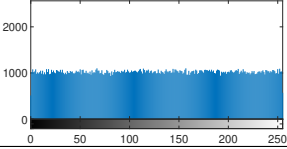
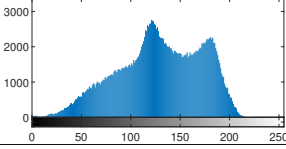
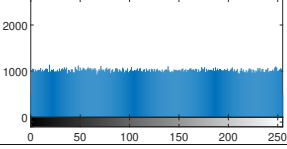
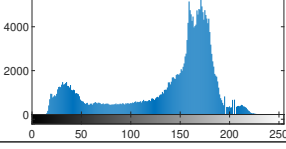
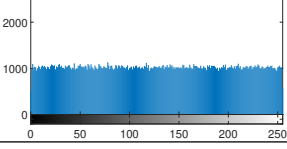
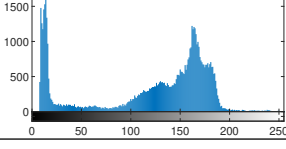
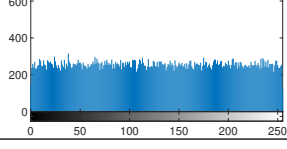
Encryption Scheme	Ciphered Image (Peppers 512×512)		
	Horizontal	Vertical	Diagonal
Proposed	3.8290×10^{-05}	2.0993×10^{-05}	3.6141×10^{-05}
[23]	0.0023	-0.0025	0.0002
[22]	-0.00395	-0.00341	-0.00392

5.3.5 Histogram Visualization

One of the most effective tests to mitigate statistical attacks is the study of the distribution of pixels over grayscale values (in the case of grayscale images) [80]. The histogram distribution provides an overall view of this matter. The horizontal axis of the histogram defines the value of the grayscale. In addition, the vertical axis specifies the frequency of grayscale values [81]. If a ciphered image appears to have a histogram distribution that its behavior could be considered approximately uniform, we can regard it to demonstrate favorable characteristics [82].

Table 5.8 demonstrates the histogram distribution for various plain images: Peppers, Mandrill, Boat, and Cameraman and their perspective ciphered version. The results show a uniform behavior from all the encrypted images, which demonstrates the capability of the proposed dual-domain image cryptosystem to mitigate histogram distribution-based statistical attacks.

Table 5.8: Histogram distribution results for multiple plain images, and their corresponding ciphered ones

Image Name & Dimension	Plain Image Histogram	Ciphered Image Histogram
Peppers 512x512		
Mandrill 512x512		
Boat 512x512		
Cameraman 256x256		

5.3.6 Chi-Square Test

The uniformity of the histogram distribution of the ciphered image is an important encryption quality metric. One way to quantify it is the chi-square metric which mathematically can be expressed as follows:

$$\chi^2 = \frac{I_{max} + 1}{M \times N} \times \sum_{i=0}^{I_{max}} \left(h_i - \frac{M \times N}{I_{max} + 1} \right)^2, \quad (5.26)$$

where, I_{max} is the maximum value of the color intensity; in which for the grayscale case $I_{max} = 255$, $M \times N$ is the total number of pixels in the ciphered image, and h_i is the histogram value at the color intensity level i .

Furthermore, for the case of grayscale images and using the chi-square table and choosing the level of significance at $\alpha = 0.05$, the threshold value will be $\chi^2_{0.05} = 293.2478$. Following the work in [83], a ciphered image with $\chi^2 < \chi^2_{0.05}$ is considered to exhibit an approximate uniform histogram distribution.

As shown in Table 5.9, all the tested ciphered images by the proposed dual-domain cryptosystem pass the conditional chi-square test. Table 5.10 shows a comparison between the proposed cryptosystem and literature in terms of the Chi-square test performed on the ciphered version of the "Peppers" image. The presented results demonstrate the superiority of the proposed cryptosystem over its corresponding in the literature.

Table 5.9: Chi-square test results.

Image	χ^2	Passed ($\chi^2_{0.05} < 293.2478$)
Peppers 512 × 512	262.8710	✓
Mandrill 512 × 512	260.1077	✓
Boat 512 × 512	262.5383	✓
Lena 256x256	259.8783	✓
Cameraman 256x256	257.5842	✓
Average	260.5959	✓

5.3.7 Uniformity Deviation Test

Another metric that provides insight into the uniformity of the histogram distribution is the uniformity deviation D_U . This metric quantifies the amount of deviation

Table 5.10: Chi-square test results of the ciphered version of the "Peppers" image comparing the proposed cryptosystem with existing literature.

Encryption Scheme	χ^2 (Peppers 512×512)
Proposed	262.8710
[23]	286.742
[78]	271.2109
[84]	267.78

presented from each color intensity level from its ideal value. Mathematically, it can be expressed as follows [85]:

$$D_U = \frac{1}{M \times N} \times \sum_{i=0}^{255} \Delta_i, \quad (5.27)$$

where Δ_i is the amplitude of the absolute difference between the actual histogram value of the i_{th} color intensity level of the ciphered image and its corresponding ideal value, and $M \times N$ is the total number of pixels.

For an 8-bit grayscale ciphered image, the ideal histogram value of i_{th} color intensity level can be calculated as follows:

$$H_{ideal} = \begin{cases} 0 & \text{if } 0 > i > I_{max} \\ \frac{M \times N}{I_{max} + 1} & \text{if } 0 \leq i \leq I_{max} \end{cases} \quad (5.28)$$

where I_{max} is the maximum value of the color scale intensity; in which for the grayscale case $I_{max} = 255$.

Table 5.11 shows the uniformity deviation results for different grayscale test im-

ages. The results illustrate that the ciphered images' distributions slightly deviate from the ideal uniform distribution, which is considered a favorable behavior.

A comparison between the proposed cryptosystem and literature based on the uniformity deviation test performed on the ciphered version of the "Peppers" image is presented in Table 5.12. Results show the superiority of the proposed dual-domain cryptosystem over other cryptosystems in [23], [86], [85].

Table 5.11: Uniformity deviation results for different grayscale test images.

Image	D_{UH}
Peppers 512×512	0.0304
Mandrill 512×512	0.0293
Boat 512×512	0.0292
Lena 256×256	0.0535
Cameraman 256×256	0.0554
Average	0.0396

5.3.8 Histogram Deviation Test

The histogram deviation test is a metric that determines the amount of deviation between the histogram distribution of the plain image and its corresponding ciphered one. Large values for this metric are more favorable. This metric can be calculated

Table 5.12: Uniformity deviation test results of the ciphered version of the "Peppers" image comparing the proposed cryptosystem with existing literature.

Encryption Scheme	D_{UH} (Peppers 512×512)
Proposed	0.0304
[23]	0.0315
[86]	0.0917
[85]	0.0502

by summing the absolute differences between the histogram values of the plain and ciphered images at each pixel value and normalizing it by the total number of pixels.

The histogram deviation test is expressed mathematically as [87]:

$$H_D = \frac{\left(\frac{\delta_0 + \delta_{255}}{2} + \sum_{i=1}^{254} \delta_i\right)}{M \times N}, \quad (5.29)$$

where $M \times N$ indicates the total number of pixels and δ_i represents the amplitude of the absolute difference between the histogram values of the plain and ciphered images at the i_{th} color intensity level.

As shown in Table 5.13, the proposed dual-domain image cryptosystem outperforms the other encryption schemes in [20], [23], [22] in all the tested ciphered images indicating the superiority of the proposed cryptosystem in this metric.

5.3.9 Irregular Deviation Test

The irregular deviation metric quantifies the level of irregularity appearing in the encrypted image. Hence, achieving a minimal value for this metric is preferable [20].

Table 5.13: Histogram deviation results for different test images

Image	Proposed Scheme	Literature		
		[20]	[23]	[22]
Peppers 512×512	0.5591	0.4517	0.2665	0.558
Mandrill 512×512	0.7690	-	0.461	0.759
Boat 512×512	0.8594	0.4591	-	-
Lena 256×256	0.5838	-	-	0.285
Cameraman 256×256	0.9829	0.0681	0.2456	0.248

This metric is calculated as follows[20]:

$$I_D = \frac{\sum_0^{255} D(i)}{M \times N}, \quad (5.30)$$

where $D(i) = |H(i) - E(H)|$, H is the histogram for the absolute value difference between the ciphered image and its corresponding plain one, $E(H)$ is the expectation of H , and $M \times N$ indicates the total number of pixels.

As shown in Table 5.14, the proposed dual-domain image cryptosystem outperforms the other encryption schemes in [20], [23], [22] for the Boat and Lena images. However, the encryption scheme in [22] surpasses the proposed cryptosystem for the Peppers image. In addition, the encryption scheme in [23] outperforms the proposed system for the Mandrill and Cameraman images.

Table 5.14: Irregular deviation results for different test images

Image	Proposed Scheme	Literature		
		[20]	[23]	[22]
Peppers 512×512	0.6379	0.7623	0.3488	0.3222
Mandrill 512×512	0.7261	-	0.2285	0.3105
Boat 512×512	0.6378	0.711	-	-
Lena 256×256	0.6141	-	-	1.4719
Cameraman 256×256	0.6037	0.7299	0.1226	0.4990

5.3.10 Mean Square Error Test

One major goal for any image cryptosystem is to maximize the ambiguity between the plain image and its corresponding ciphered one. Hence, one metric to measure the degree of this ambiguity is the Mean Square Error (MSE). This metric calculates the square of the difference of the pixels' values between the plain and ciphered image averaged on their number. MSE can be defined as follows:

$$MSE = \frac{\sum_{j=1}^M \sum_{i=1}^N (P(j, i) - C(j, i))^2}{M \times N} \quad (5.31)$$

where $M \times N$ is the image's total number of pixels, P is the plain image, C is the ciphered image, and (j, i) is the indices of a pixel in the tested image. Generally, an image cryptosystem exhibits an advantageous behavior if its MSE value is greater than or equals 30dB [88].

Table 5.15 shows MSE values for different test images indicating a favorable behavior. A comparison between the presented cryptosystem and literature in terms of

the Mean Square Error (MSE) test performed on the plain and ciphered version of the "Mandrill" image is shown in Table 5.16. Results show that the dual-domain proposed cryptosystem exhibits the best behavior compared to cryptosystems in [23], [22], [45].

Table 5.15: Mean Square Error (MSE).

Image	MSE _{dB}
Peppers 512 × 512	78.4284
Mandrill 512 × 512	77.1403
Boat 512 × 512	78.2977
Lena 256 × 256	79.0453
Cameraman 256 × 256	79.4422

Table 5.16: Mean Square Error (MSE) test results of the ciphered version of the "Mandrill" image comparing the proposed cryptosystem with existing literature.

Encryption Scheme	MSE _{dB} (Mandrill 512 × 512)
Proposed	77.1403
[23]	46.0304
[22]	39.67941
[45]	76.8145

5.3.11 Global Entropy Test

Global entropy is a statistical examination aimed at assessing the level of unpredictability and randomness characterizing the pixel data through an entire image.

Claude Shannon initially introduced this fundamental concept in 1948 [89]. It was introduced in the domain of communication systems to serve as a quantitative measure of uncertainty. A ciphered image exhibiting a higher entropy value tends to provide a more effective hiddenness of the underlying plain image compared to others with lower entropy. Mathematically, entropy is expressed as follows [19]:

$$GE(y) = \sum_{i=0}^{2^S-1} P(y_i) \log_2 \frac{1}{P(y_i)}, \quad (5.32)$$

where, $GE(y)$ is the value of global entropy in bits, $P(y_i)$ is the probability that y_i occurs, and N is number of bits required to represent one pixel. For an ideal scenario where each grayscale level is equiprobable, represented with 8 bits for each, the benchmark value for the global entropy is calculated from the abovementioned equation as follows:

$$GE_{(benchmark)} = \sum_{i=0}^{255} (\log_2 256) \times \frac{1}{256} = 8 \quad (5.33)$$

As a result, the global entropy for a ciphered image is considered favorable as it approaches 8. On the other hand, a ciphered image that exhibits a low global entropy value is regarded as vulnerable to brute-force attacks.

Table 5.17 demonstrates the results for the global entropy test implemented on the ciphered versions of multiple plain images. As illustrated in Table 5.18, the proposed dual-domain image cryptosystem exhibits the most favorable value compared to encryption schemes in [75], [21], [20], [45], [13], [78], [26] for the ciphered version of

” Lena” image.

Table 5.17: Global entropy results for different test images

Image	Plain Image	Proposed Scheme
Peppers 512×512	7.5925	7.9976
Mandrill 512×512	7.3579	7.9976
Boat 512×512	7.1238	7.9980
Lena 256×256	7.5683	7.9985
Cameraman 256×256	7.0097	7.9966

Table 5.18: The Global Entropy results for the ciphered version of ” Lena” image compared with the literature

Encryption Scheme	Global Entropy (Lena 256x256)
Proposed	7.9985
[75]	7.9977
[21]	7.7190
[20]	7.7771
[45]	7.9976
[13]	7.9826
[26]	7.9920
[78]	7.9975

5.3.12 Differential Analysis

Differential attacks examine how the difference between two pairs of inputs, which are applied to an exclusive OR operation, results in a difference between the corresponding

outputs. Such attacks could be a helpful tool for an attacker to extract confidential data such as the secret key and plain image from its corresponding ciphered one. Therefore, to test the immunity of cryptosystems against such attacks, two proposed metrics have been suggested in the literature: the Unified Averaged Changed Intensity (UACI) and the Number of Changing Pixel Rate (NPCR) [90].

Consider P_1 and P_2 , as two plain images. Each one has a total number of pixels $M \times N$. The only difference between both of them is the value of one pixel. Let C_1 and C_2 be the corresponding ciphered versions of P_1 and P_2 , respectively. The UACI and NPCR are mathematically expressed as follows:

$$UACI = \frac{1}{M \times N} \left[\sum_{i,j} \frac{C_1(i,j) - C_2(i,j)}{I_{max}} \right] \times 100\%, \quad (5.34)$$

$$NPCR = \frac{\sum_{i,j} f(i,j)}{M \times N} \times 100\%, \quad (5.35)$$

$$f(i,j) = \begin{cases} 1 & \text{if } C_1(i,j) \neq C_2(i,j) \\ 0 & \text{if } C_1(i,j) = C_2(i,j) \end{cases} \quad (5.36)$$

where I_{max} is the maximum value of the color scale intensity; in which for the grayscale case $I_{max} = 255$.

Moreover, the calculation of the UACI and NPCR tests' values necessitates the exploitation of benchmark values or ranges to evaluate their effectiveness. This issue has been investigated in [91], where the authors introduced the threshold value $NPCR|_{\alpha}^*$ for ciphered images with different sizes. This threshold value is expressed

as follows:

$$NPCR|_{\alpha}^* = \frac{-[T \times \Phi^{-1}(\alpha)] + I_{max}}{1 + I_{max}}, \quad (5.37)$$

$$T = \left[\frac{I_{max}}{N \times M} \right]^{0.5}, \quad (5.38)$$

where $\Phi^{-1}(\alpha)$ is the inverse cumulative density function of the normal distribution $\mathcal{N}(0, 1)$, and α is the level of significance. Hence, a ciphered image exhibits a favorable NPCR if its value is greater than or equals $NPCR|_{\alpha}^*$.

As for the UACI test, the authors in [91] presented two threshold values $UACI|_{\alpha}^{*-}$ and $UACI|_{\alpha}^{*+}$ to define the critical interval. These thresholds are expressed as follows:

$$\begin{cases} UACI|_{\alpha}^{*-} = \mu_{uaci} - \Phi^{-1}(0.5\alpha) \times \sigma_{uaci} \\ UACI|_{\alpha}^{*+} = \mu_{uaci} + \Phi^{-1}(0.5\alpha) \times \sigma_{uaci}, \end{cases} \quad (5.39)$$

$$\mu_{uaci} = \frac{2 + I_{max}}{3 \times (1 + I_{max})} \quad (5.40)$$

$$\sigma_{uaci}^2 = \frac{(I_{max}^2 + 2I_{max} + 3)(I_{max} + 2)}{N \times M \times 18(I_{max} + 1)^2 \times I_{max}} \quad (5.41)$$

A selection of $\alpha = 5 \times 10^{-2}$ is made for the calculations of the threshold values. Table 5.19 demonstrates the values of the UACI and NPCR tests applied over several test images with different sizes. The results show that all the values are within the favorable ranges indicating the capability of the proposed dual-domain image cryptosystem to mitigate differential attacks successfully.

Table 5.20 provides a comparison among the proposed dual-domain image cryptosystem and multiple cryptosystems in [23], [22], [20], [26], [78]. The illustrated results show the superiority of the proposed cryptosystem over other compared work.

Table 5.19: UACI and NPCR results for different ciphered images

Image	Proposed Scheme		$NPCR \geq NPCR _{\alpha}^*$	$UACI _{\alpha}^{*-} \leq UACI \leq UACI _{\alpha}^{*+}$
	NPCR	UACI	$NPCR_{0.05}^* = 99.5893\%$	$UACI _{0.05}^{*-}, UACI _{0.05}^{*+} = (33.3730\%, 33.5541\%)$
Peppers 512 × 512	99.656	33.53	✓	✓
Mandrill 512 × 512	99.623	33.554	✓	✓
Boat 512 × 512	99.622	33.491	✓	✓
Image	Proposed Scheme		$NPCR \geq NPCR _{\alpha}^*$	$UACI _{\alpha}^{*-} \leq UACI \leq UACI _{\alpha}^{*+}$
	NPCR	UACI	$NPCR_{0.05}^* = 99.5693\%$	$UACI _{0.05}^{*-}, UACI _{0.05}^{*+} = (33.2824\%, 33.6447\%)$
Lena 256 × 256	99.624	33.492	✓	✓
Cameraman 256 × 256	99.639	33.54	✓	✓

Table 5.20: Comparison between proposed dual-domain cryptosystem and its corresponding in literature in terms of UACI and NPCR results

Image	Proposed Scheme		Literature									
			[20]		[23]		[22]		[26]		[78]	
	NPCR	UACI	NPCR	UACI	NPCR	UACI	NPCR	UACI	NPCR	UACI	NPCR	UACI
Peppers 512x512	99.656	33.53	99.526	24.204	99.621	33.486	99.641	33.453	-	-	99.608	33.475
Mandrill 512x512	99.623	33.554	-	-	99.612	33.553	99.605	33.437	99.609	33.326	99.589	33.548
Boat 512x512	99.622	33.491	99.173	22.37	99.617	33.491	-	-	99.519	33.365	99.579	33.487
Lena 256x256	99.624	33.492	99.76	26.48	-	-	99.619	33.485	99.626	33.462	99.617	33.451
Cameraman 256x256	99.639	33.54	98.942	25.937	99.636	33.391	99.604	33.485	99.616	33.054	99.600	33.386

5.3.13 Analysis of Ciphared Image Randomness

NIST SP800 is a set of policies that measures the secrecy of data released by the National Institute of Standards and Technology (NIST) that is currently an authoritative reference utilized by a broad number of information security experts [92], [93].

For the purpose of evaluating the randomness and unpredictability of a given sequence, this work utilizes the NIST SP 800-22 test suite [94]. The adapted suite execute 15 different test in which a $p_{value} \in [0, 1]$ is obtained from each test. Moreover, a sequence passes a test successfully, if its $p_{value} > 0.01$.

To generate the tested sequence, we utilized 10^3 secret keys to produce their corresponding ciphared image. Each consequence key is different from the previous one by one bit. Hence, we have 10^3 sequences, each is $(512 \times 512 \times 8)$ bit in length. This approach has been adapted to produce large enough sequences to be used by the test suit and to test the key sensitivity.

Table 5.21 demonstrates the results of the 15 tests for the ciphared version of the "Mandrill" image. Results demonstrate that the "Mandrill" image passed successfully all the 15 tests. Results also indicate that the proposed dual-domain image cryptosystem exhibits sensitive behavior to any small variations in the secret key, even in the range of one bit.

5.3.14 Immunity Analysis Against Cryptanalytic Attacks

In a general context, a cryptosystem must retain the ability of not restoring the plain image from its corresponding ciphared one in the case of using any other key than the

Table 5.21: Tests' results of randomness for the ciphered 512×512 "Mandrill" image.

Sub-test	p_{value}	Passed ($p_{value} > 0.01$)
Frequency	0.350485	✓
Block Frequency	0.739918	✓
Cumulative Sums	0.350485	✓
Runs	0.122325	✓
Longest Run of Ones	0.017912	✓
Rank	0.534146	✓
FFT	0.350485	✓
Non-Overlapping Template	0.911413	✓
Overlapping Template	0.739918	✓
Universal	0.911413	✓
Approximate Entropy	0.213309	✓
Random Excursions	0.739918	✓
Random Excursions Variant	0.911413	✓
Serial	0.534146	✓
Linear Complexity	0.739918	✓

secret one. Nevertheless, in the realm of cryptography, it is likely for some kinds of attacks (without the knowledge of the right key) to perform specialized approaches via iterative experimentation to acquire the plain image. In order to achieve these kinds of attacks, it's essential to have efficacious information about the cryptosystem and its related components. As a result, referring to the information type used to perform the attack, a division into a number of categories is obtained. An illustration of some of these attacks is held throughout this section [95], [96], [97]:

- **Ciphertext-only attack (COA):** This attack occurs when an attacker seeks

to estimate the plain image or the used secret key, just by examining the ciphered image. However, in this type of attack, the attacker's attempts to extract the abovementioned information will eventually fail if the cryptosystem provides strong enough statistical randomness outcomes free from any patterns or biases. As shown in Section 5.3.13, the proposed dual-domain image cryptosystem managed to pass the statistical tests of NIST, indicating its resilience against such an attack.

- **Chosen-plaintext attack (CPA) and Known-plaintext attack (KPA):**

The attacker can perform the KPA if he successfully possesses a large number of plaintexts and their corresponding ciphered ones without holding the capability of choosing. The CPA holds the same procedure as KPA but with the flexibility of choice. Thus it is more practical. In general, showing the susceptibility of a cryptosystem against KPA implies its vulnerability to CPA [98]. The proposed dual-domain image cryptosystem has the advantage of performing keyed confusion and diffusion operations. Therefore, the proposed dual-domain chaotic image cryptosystem holds the ability to mitigate any type of attack that tries to mimic the corresponding cryptosystem's processes.

For instance, when the attacker wants to use algebraic attacks to attack a system based on S-boxes, they can illustrate the nonlinear process using a set of equations algebraically [99]. However, in the case of the proposed dual-domain image cryptosystem, it substitutes each pixel in the plain image diligently based on a secret key, which ensures that the same pixels' values are assigned to dif-

ferent indices. Herby, this prevents the adversary from formulating the set of equations. Moreover, the attacker will need to deduce the equations for different plain images that differ in size. As a result of the dynamicity and randomness of the procedure of substitution in the proposed dual-domain image cryptosystem [100], we conclude by stating the resilience of the proposed cryptosystem to such algebraic attacks. In the case of differential attacks, results in Section 5.3.12 shows the proposed dual-domain image cryptosystem's ability to resist such an attack.

Moreover, the proposed dual-domain image cryptosystem is tested using "All Black" and "All White" images against KPA and CPA. As shown in Fig.5.2, the ciphered versions of "All White" and "All Black" images exhibit a very noisy behavior, indicating the capability of the proposed cryptosystem to mitigate CPA and KPA.

5.3.15 Time Consumption Analysis

In Cryptography, cryptosystems' algorithms should be efficient in terms of time consumption. However, this should not be at the cost of either the security or quality of the obtained ciphered image [101], [102]. Hence, this section introduces a time consumption analysis for the proposed dual-domain image cryptosystem.

Table 5.22 demonstrates the time consumption results for multiple test images with various sizes. Simulation results illustrate that the proposed dual-domain image cryptosystem exhibits satisfactory consumption in processing time. thus, this indicates

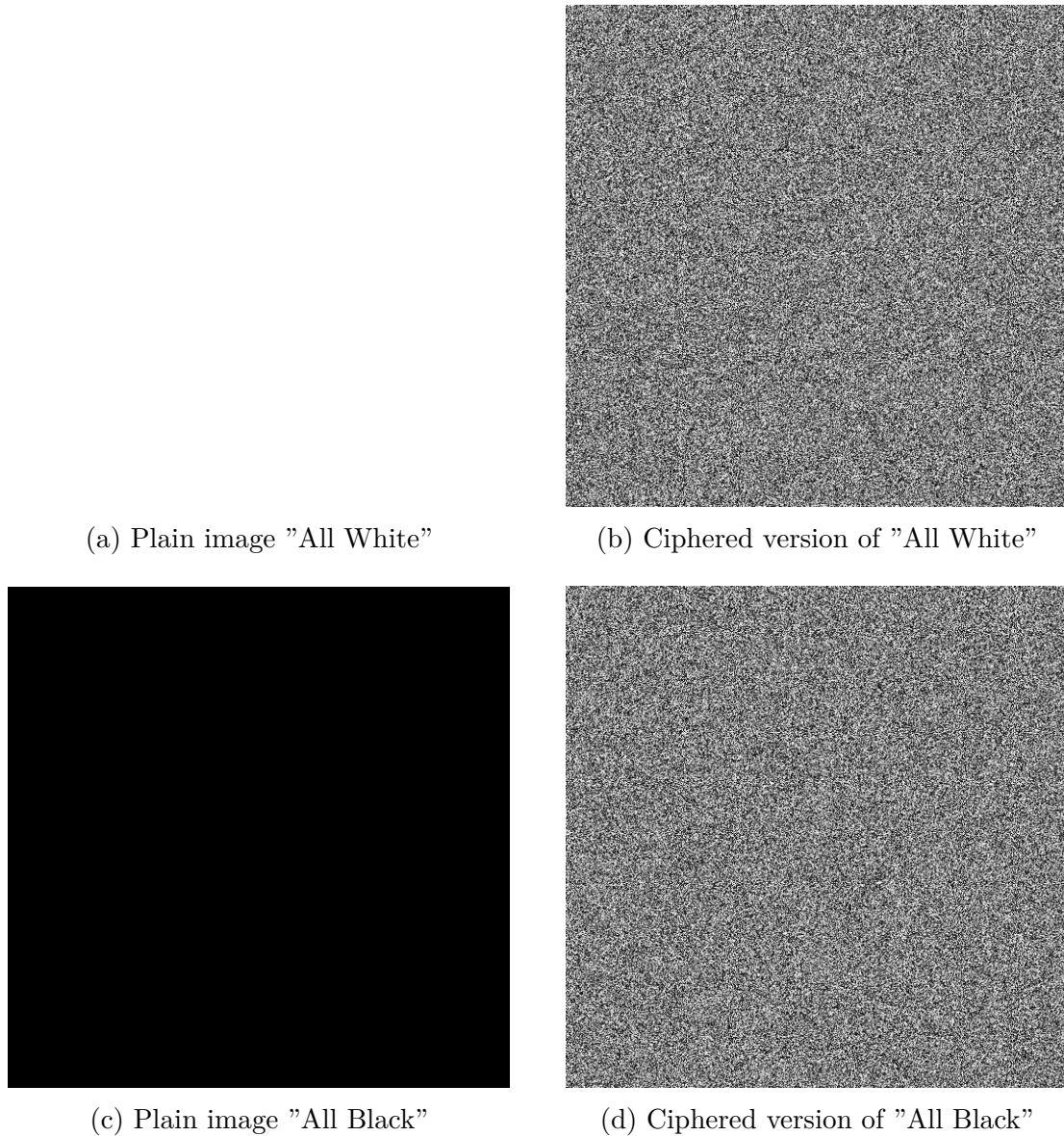


Figure 5.2: Results for the "All White" and "All Black" images and their ciphered version.

its time consumption efficiency.

The comparison in Table 5.23 displays the processing time required to execute the proposed encryption scheme along with other schemes mentioned in the literature. The evaluation is conducted on a "Lena" image with dimensions of 256×256 . The proposed cryptosystem is compared with cryptosystems presented in [22], [45], [103],

implemented using machines with the following specifications respectively, Core i5 with 8GB RAM, Core(TM) i5-7200U CPU at 2.5 GHz with 8GB RAM, and Core i5 CPU at 3.6 GHz, with 8GB RAM. The results indicate that the proposed encryption scheme consumes less time compared to other schemes.

Table 5.22: Time consumption results for multiple test images.

Image	Time (sec)
Peppers 512×512	0.6314
Mandrill 512×512	0.6490
Boat 512×512	0.6144
Lena 512×512	0.6412
Lena 256×256	0.1638
Cameraman 256×256	0.1654

Table 5.23: Time consumption test results performed on 256×256 "Lena" image comparing the proposed cryptosystem with existing literature.

Time (s)	Proposed Scheme (Lena 256x256)	[22]	[45]	[103]
	0.1638	0.3234	2.1743	1.9134

5.3.16 Comparative Analysis of Dual-Domain Chaotic Image

Cryptosystem with Different Wavelets

Table 5.24, shows the results of the dual-domain chaotic image cryptosystem using two different wavelet transforms, namely Bior3.7 and Haar wavelets. Various encryption performance metrics have been calculated for the resulting ciphered images using

repetitively pseudorandomly choosing different keys following the procedure presented at the beginning of this section. As shown in Table 5.24, on average, the cryptosystem that adapted the Bior3.7 wavelet outperformed the one that adapted the Haar wavelet for all metrics except the UACI.

Table 5.24: Comparative Analysis of Dual-Domain Chaotic Image Cryptosystem with Different Wavelets

Image	Wavelet	Correlation Coefficient	H_D	Entropy	χ^2	NPCR	UCAI
Peppers 512×512	Bior3.7	1.7876×10^{-05}	0.5591	7.9976	262.8710	99.656	33.53
	Haar	1.8553×10^{-04}	0.5507	7.9978	308.9420	99.366	32.955
Mandrill 512×512	Bior3.7	8.4977×10^{-05}	0.7690	7.9976	260.1077	99.623	33.554
	Haar	2.8188×10^{-04}	0.7515	7.9979	267.2330	99.510	31.873
Boat 512×512	Bior3.7	1.0791×10^{-04}	0.8594	7.9980	262.5383	99.622	33.491
	Haar	3.5300×10^{-04}	0.8589	7.9978	303.1819	99.346	34.800
Lena 256×256	Bior3.7	-2.8612×10^{-04}	0.6838	7.9985	259.8783	99.624	33.492
	Haar	2.9971×10^{-04}	0.6449	7.9978	315.7140	99.604	33.416
Cameraman 256×256	Bior3.7	1.4863×10^{-04}	0.9829	7.9966	257.5842	99.639	33.54
	Haar	8.2273×10^{-04}	0.9808	7.9963	291.9606	99.442	36.583
Average	Bior3.7	1.613×10^{-04}	0.7708	7.9977	260.5959	99.6328	33.5214
	Haar	3.886×10^{-04}	0.7574	7.9975	297.4063	99.4536	33.9254

5.4 Chapter Summary

In conclusion, the confidentiality of multimedia data is a major concern in the realm of cybersecurity. This chapter has delved into the chaotic image ciphers as a potential solution to this issue. While previous research has explored chaotic image encryption in various transformation domains, such as spatial, discrete Fourier transform, and wavelet transform, it has been observed that frequency-based cryptosystems, while exhibiting favorable confusion properties, fall short in terms of diffusion properties and succumb to certain statistical vulnerabilities, rendering them susceptible to a

range of attacks.

In response to these challenges, this work has introduced a dual-domain image cryptosystem, combining the wavelet and spatial domains, and proposed an innovative diffusion process within the wavelet domain. This new approach addresses the issue of weak resilience against statistical, analytical, and differential attacks. Notably, the proposed diffusion process in the wavelet domain is computationally more efficient than existing wavelet domain-based methods, as it operates on only 1/16 of the plain image pixels. Furthermore, this cryptosystem effectively resolves the bell-shaped histogram problem associated with frequency-based cryptosystems, as verified through visual and objective examinations using various performance metrics in simulation results. Additionally, this research introduced a novel key-dependent chaotic variable generator for generating the necessary chaotic variables for an enhanced chaotic map.

The results used for the evaluation of the proposed cryptosystem, compared to state-of-the-art methods, demonstrate its superiority across a spectrum of performance metrics, including visual tests, various correlation coefficients, histogram visualization, histogram deviation, irregular deviation, mean square error, chi-square test, global entropy, as well as analyses related to differential attacks, standard randomness test, cryptanalysis, and time consumption. These findings collectively underscore the efficacy and robustness of the proposed approach in enhancing the security and secrecy of multimedia data.

CHAPTER 6

CONCLUSIONS & RECOMMENDATIONS

6.1 Conclusions

In conclusion, protecting the confidentiality of multimedia data remains a noteworthy focal point within the cybersecurity domain. As the development of new multimedia applications continues, so does the imperative for enhanced security measures.

This thesis has investigated the realm of chaotic image ciphers as a potential remedy for this ongoing concern. While earlier research has explored chaotic image encryption across various transformation domains, including spatial, DFT, and wavelet transform, it has been evident that frequency-based cryptosystems while demonstrating favorable confusion properties, exhibit deficiencies in diffusion properties. They also fail to specific statistical vulnerabilities, leaving them open to various types of attacks. Additionally, some of these systems manifest non-uniform histograms.

In response to these challenges, this thesis has introduced two potential solutions.

The first work presented an enhanced block cipher image cryptosystem, featuring multiple operational modes founded on the bit reversal concept, incorporating a 2D chaotic baker map and DFT. The experimental results have demonstrated the superiority of the proposed enhancement across various quality metrics. Notably, it has successfully achieved uniform histograms in the MCFB and OFB modes, along with a substantial enhancement in resistance against differential attacks.

The second work presented a dual-domain image cryptosystem, combining the wavelet and spatial domains, and introduced a novel diffusion process within the wavelet domain. This novel approach addresses the issue of weak resilience against statistical, analytical, and differential attacks. Remarkably, the proposed diffusion process in the wavelet domain stands out for its computational efficiency, operating on only 1/16 of the plain image pixels. Furthermore, this cryptosystem effectively resolves the bell-shaped histogram problem associated with frequency-based cryptosystems, as validated through visual and objective examinations utilizing diverse performance metrics within simulation results. Furthermore, this research has introduced a novel key-dependent chaotic variable generator, which facilitates the generation of essential initial conditions and control parameters for an enhanced chaotic map.

The results of this work are used to evaluate the proposed cryptosystem, compared to state-of-the-art methods. These results have showcased its superiority across a wide spectrum of performance metrics, encompassing visual examinations, numerous correlation coefficients, histogram analysis, deviation assessments, mean square error, chi-square tests, global entropy, and examinations related to differential attacks, standard randomness tests, cryptanalysis, and time efficiency. Collectively, these findings

emphasize the effectiveness and resilience of the proposed approach in strengthening the security and confidentiality of multimedia data.

The proposed approaches are not without limitations, however. One potential limitation is that the tested images for the proposed cryptosystems were only grayscale images. Another limitation of this research is the use of pre-known confusion processes. These limitations can be addressed, for example, by the use of different types of images, such as colored images. In addition, a study can be conducted to design novel customized confusion processes for various transformation domains. This could be done, for instance, by the aid of machine learning.

6.2 Recommendations

In light of the findings presented in this thesis, it is advisable to explore further research in the following points:

- Customized confusion processes: More detailed research can be conducted on designing customized confusion processes for different transformation methods. This can be achieved with the help of machine learning.
- Designing asymmetric transform-based chaotic cryptosystems: this is an interesting research direction, which has the potential to extend the transform-based chaotic cryptosystems to wider applications in the realm of cybersecurity.
- Various data types: More effort can be spent to generalize these transform-based image cryptosystems, so they can be able to cipher other data types, such as

audio files.

In conclusion, transform-based image cryptosystems show great potential in securing multimedia, yet there remains room for improvement in their design. These suggestions lay the foundation for further exploration in this field of research.

REFERENCES

- [1] M. Alawida, A. Samsudin, and J. S. Teh, “Enhancing unimodal digital chaotic maps through hybridisation,” *Nonlinear Dynamics*, vol. 96, pp. 601–613, 2019.
- [2] W. Stallings, *Cryptography and Network Security: Principles and Practice*. Pearson, 2023. [Online]. Available: <https://books.google.com.sa/books?id=zjbZzgEACAAJ>
- [3] H. S. El-Sayed, A. Afifi, M. A. AlZain, and O. S. Faragallah, “An image cryptosystem using chaotic baker map in dft,” in *2021 International Conference of Women in Data Science at Taif University (WiDSTaif)*. IEEE, 2021, pp. 1–7.
- [4] B. Zolfaghari and T. Koshiba, “Chaotic image encryption: State-of-the-art, ecosystem, and future roadmap,” *Applied System Innovation*, vol. 5, no. 3, p. 57, 2022.
- [5] F. E. Abd El-Samie, H. E. H. Ahmed, I. F. Elashry, M. H. Shahieen, O. S. Faragallah, E.-S. M. El-Rabaie, and S. A. Alshebeili, *Image encryption: a communication perspective*. CRC Press, 2013.

- [6] Z. Galias and L. Kocarev, *Intelligent Computing Based on Chaos*. Springer, 2009.
- [7] C. E. Shannon, “Communication theory of secrecy systems,” *The Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.
- [8] C.-S. Park, “2d discrete fourier transform on sliding windows,” *IEEE Transactions on Image Processing*, vol. 24, no. 3, pp. 901–907, 2015.
- [9] V. Solachidis and L. Pitas, “Circularly symmetric watermark embedding in 2-d dft domain,” *IEEE transactions on image processing*, vol. 10, no. 11, pp. 1741–1753, 2001.
- [10] X. Wu, D. Wang, J. Kurths, and H. Kan, “A novel lossless color image encryption scheme using 2d dwt and 6d hyperchaotic system,” *Information Sciences*, vol. 349, pp. 137–153, 2016.
- [11] T. Yan, P. Wu, Y. Qian, Z. Hu, and F. Liu, “Multiscale fusion and aggregation pcnn for 3d shape recovery,” *Information Sciences*, vol. 536, pp. 277–297, 2020.
- [12] W. Sweldens, “The lifting scheme: A construction of second generation wavelets,” *SIAM journal on mathematical analysis*, vol. 29, no. 2, pp. 511–546, 1998.
- [13] Y. Luo, M. Du, and J. Liu, “A symmetrical image encryption scheme in wavelet and time domain,” *Communications in Nonlinear Science and Numerical Simulation*, vol. 20, no. 2, pp. 447–460, 2015.

- [14] I. Daubechies and W. Sweldens, “Factoring wavelet transforms into lifting steps,” *Journal of Fourier analysis and applications*, vol. 4, pp. 247–269, 1998.
- [15] S. H. Strogatz, *Nonlinear dynamics and chaos with student solutions manual: With applications to physics, biology, chemistry, and engineering*. CRC press, 2018.
- [16] C. Li, B. Feng, S. Li, J. Kurths, and G. Chen, “Dynamic analysis of digital chaotic maps via state-mapping networks,” *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 66, no. 6, pp. 2322–2335, 2019.
- [17] C. Li, D. Lin, J. Lü, and F. Hao, “Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography,” *IEEE multimedia*, vol. 25, no. 4, pp. 46–56, 2018.
- [18] R. Küsters and M. Tuengerthal, “Universally composable symmetric encryption,” in *2009 22nd IEEE Computer Security Foundations Symposium*, 2009, pp. 293–307.
- [19] M. Alawida, J. S. Teh, and W. Alshoura, “A new image encryption algorithm based on dna state machine for uav data encryption,” *Drones*, vol. 7, no. 1, p. 38, 2023.
- [20] O. S. Faragallah, A. Afifi, W. El-Shafai, H. S. El-Sayed, E. A. Naeem, M. A. Alzain, J. F. Al-Amri, B. Soh, and F. E. Abd El-Samie, “Investigation of chaotic image encryption in spatial and frft domains for cybersecurity applications,” *IEEE Access*, vol. 8, pp. 42 491–42 503, 2020.

- [21] I. F. Elashry, W. El-Shafai, E. S. Hasan, S. El-Rabaie, A. M. Abbas, F. E. Abd El-Samie, H. S. El-sayed, and O. S. Faragallah, “Efficient chaotic-based image cryptosystem with different modes of operation,” *Multimedia Tools and Applications*, vol. 79, pp. 20 665–20 687, 2020.
- [22] J. Arif, M. A. Khan, B. Ghaleb, J. Ahmad, A. Munir, U. Rashid, and A. Y. Al-Dubai, “A novel chaotic permutation-substitution image encryption scheme based on logistic map and random substitution,” *IEEE Access*, vol. 10, pp. 12 966–12 982, 2022.
- [23] Y. Alghamdi, A. Munir, and J. Ahmad, “A lightweight image encryption algorithm based on chaotic map and random substitution,” *Entropy*, vol. 24, no. 10, p. 1344, 2022.
- [24] O. S. Faragallah, M. A. AlZain, H. S. El-Sayed, J. F. Al-Amri, W. El-Shafai, A. Afifi, E. A. Naeem, and B. Soh, “Secure color image cryptosystem based on chaotic logistic in the frft domain,” *Multimedia Tools and Applications*, vol. 79, pp. 2495–2519, 2020.
- [25] M. Guan, X. Yang, and W. Hu, “Chaotic image encryption algorithm using frequency-domain dna encoding,” *IET image processing*, vol. 13, no. 9, pp. 1535–1539, 2019.
- [26] J. Karmakar and M. K. Mandal, “Chaos-based image encryption using integer wavelet transform,” in *2020 7th International Conference on Signal Processing and Integrated Networks (SPIN)*. IEEE, 2020, pp. 756–760.

- [27] Q. Wang, Q. Ding, Z. Zhang, and L. Ding, “Digital image encryption research based on dwt and chaos,” in *2008 Fourth International Conference on Natural Computation*, vol. 5. IEEE, 2008, pp. 494–498.
- [28] J. Wang, “Image encryption algorithm based on 2-d wavelet transform and chaos sequences,” in *2009 International Conference on Computational Intelligence and Software Engineering*. IEEE, 2009, pp. 1–3.
- [29] Q. Zhang, M. Shen, B. Li, and R. Fang, “Chaos-based color image encryption scheme in the wavelet domain,” in *2014 7th International Congress on Image and Signal Processing*. IEEE, 2014, pp. 330–334.
- [30] X. Li and Y. Zhang, “Digital image encryption and decryption algorithm based on wavelet transform and chaos system,” in *2016 IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC)*. IEEE, 2016, pp. 253–257.
- [31] C. Macovei, M. Răducanu, and O. Datcu, “Image encryption algorithm using wavelet packets and multiple chaotic maps,” in *2020 International Symposium on Electronics and Telecommunications (ISETC)*. IEEE, 2020, pp. 1–4.
- [32] Q. Qin, Z. Liang, S. Liu, X. Wang, and C. Zhou, “A dual-domain image encryption algorithm based on hyperchaos and dynamic wavelet decomposition,” *IEEE Access*, vol. 10, pp. 122 726–122 744, 2022.

- [33] G. Ye and X. Huang, “A secure image encryption algorithm based on chaotic maps and sha-3,” *Security and Communication Networks*, vol. 9, no. 13, pp. 2015–2023, 2016.
- [34] J. Chen, Z.-l. Zhu, L.-b. Zhang, Y. Zhang, and B.-q. Yang, “Exploiting self-adaptive permutation–diffusion and dna random encoding for secure and efficient image encryption,” *Signal Processing*, vol. 142, pp. 340–353, 2018.
- [35] H. Liu, X. Wang *et al.*, “Image encryption using dna complementary rule and chaotic maps,” *Applied Soft Computing*, vol. 12, no. 5, pp. 1457–1466, 2012.
- [36] M. Gupta, V. P. Singh, K. K. Gupta, and P. K. Shukla, “An efficient image encryption technique based on two-level security for internet of things,” *Multi-media Tools and Applications*, vol. 82, no. 4, pp. 5091–5111, 2023.
- [37] J. I. M. Bezerra, G. Machado, A. Molter, R. I. Soares, and V. Camargo, “A novel simultaneous permutation–diffusion image encryption scheme based on a discrete space map,” *Chaos, Solitons & Fractals*, vol. 168, p. 113160, 2023.
- [38] X. Gao, J. Mou, S. Banerjee, and Y. Zhang, “Color-gray multi-image hybrid compression–encryption scheme based on bp neural network and knight tour,” *IEEE Transactions on Cybernetics*, 2023.
- [39] P. Liu, X. Wang, Y. Su, H. Liu, and S. Unar, “Globally coupled private image encryption algorithm based on infinite interval spatiotemporal chaotic system,” *IEEE Transactions on Circuits and Systems I: Regular Papers*, 2023.

- [40] S. Zhou, X. Wang, and Y. Zhang, “Novel image encryption scheme based on chaotic signals with finite-precision error,” *Information Sciences*, vol. 621, pp. 782–798, 2023.
- [41] S. Sharma, S. Sharma, and T. Choudhury, “A study of post quantum cryptographic security model using symmetric key algorithm,” *International Journal of Intelligent Systems and Applications in Engineering*, vol. 11, no. 5s, pp. 181–198, 2023.
- [42] C. U. Sak, S. Z. M. Naziri, R. C. Ismail, M. N. M. Isa, and R. Hussin, “Hardware design of combinational 128-bit camellia symmetric cipher using 0.18 μ m technology,” in *2022 IEEE International Conference on Semiconductor Electronics (ICSE)*, 2022, pp. 101–104.
- [43] R. Anusha, M. D. Kumar, V. S. Shetty, and N. P. Hegde, “Symmetric key algorithm in computer security: A review,” in *2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*. IEEE, 2020, pp. 765–769.
- [44] M. Alawida, A. Samsudin, and J. S. Teh, “Enhanced digital chaotic maps based on bit reversal with applications in random bit generators,” *Information Sciences*, vol. 512, pp. 1155–1169, 2020.
- [45] H. Mahalingam, T. Veeramalai, A. R. Menon, and R. Amirtharajan, “Dual-domain image encryption in unsecure medium—a secure communication perspective,” *Mathematics*, vol. 11, no. 2, p. 457, 2023.

- [46] D. E. Knuth, *The Art of Computer Programming, Volume 2, Seminumerical Algorithms*. Addison-Wesley Professional, 2005.
- [47] S. Noshadian, A. Ebrahimzade, and S. J. Kazemitabar, “Optimizing chaos based image encryption,” *Multimedia Tools and Applications*, vol. 77, pp. 25 569–25 590, 2018.
- [48] —, “Breaking a chaotic image encryption algorithm,” *Multimedia Tools and Applications*, vol. 79, pp. 25 635–25 655, 2020.
- [49] S. Q. Ren, B. H. M. Tan, S. Sundaram, T. Wang, Y. Ng, V. Chang, and K. M. M. Aung, “Secure searching on cloud storage enhanced by homomorphic indexing,” *Future Generation Computer Systems*, vol. 65, pp. 102–110, 2016.
- [50] M. Á. Prada-Delgado, I. Baturone, G. Dittmann, J. Jelitto, and A. Kind, “Puf-derived iot identities in a zero-knowledge protocol for blockchain,” *Internet of Things*, vol. 9, p. 100057, 2020.
- [51] S. S. Roy, O. Reparaz, F. Vercauteren, and I. Verbauwhede, “Compact and side channel secure discrete gaussian sampling,” *Cryptology ePrint Archive*, 2014.
- [52] J. W. Yoon and H. Kim, “An image encryption scheme with a pseudorandom permutation based on chaotic maps,” *Communications in Nonlinear Science and Numerical Simulation*, vol. 15, no. 12, pp. 3998–4006, 2010.
- [53] H. Zhong and G. Li, “Multi-image encryption algorithm based on wavelet transform and 3d shuffling scrambling,” *Multimedia Tools and Applications*, vol. 81, no. 17, pp. 24 757–24 776, 2022.

- [54] Z. Chen, Y. Yang, and X. Jiang, “An image-encryption algorithm based on stage-merging bit scrambling,” *Applied Sciences*, vol. 12, no. 14, p. 6972, 2022.
- [55] U. Saokani, M. Irfan, D. S. Maylawati, R. J. Abidin, I. Taufik *et al.*, “Comparison of the fisher-yates shuffle and the linear congruent algorithm for randomizing questions in nahwu learning multimedia,” *Khazanah Journal of Religion and Technology*, vol. 1, no. 1, pp. 10–14, 2023.
- [56] T. K. Hazra and S. Bhattacharyya, “Image encryption by blockwise pixel shuffling using modified fisher yates shuffle and pseudorandom permutations,” in *2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*. IEEE, 2016, pp. 1–6.
- [57] T. K. Hazra, R. Ghosh, S. Kumar, S. Dutta, and A. K. Chakraborty, “File encryption using fisher-yates shuffle,” in *2015 International Conference and Workshop on Computing and Communication (IEMCON)*. IEEE, 2015, pp. 1–7.
- [58] D. Adhar, U. Indriani, E. Panggabean, A. Sabir, H. Kurniawan *et al.*, “Application of the fisher-yates shuffle algorithm in the game matching the world monument picture,” in *2020 2nd International Conference on Cybernetics and Intelligent System (ICORIS)*. IEEE, 2020, pp. 1–6.
- [59] S. Saeed, M. S. Umar, M. A. Ali, and M. Ahmad, “A gray-scale image encryption using fisher-yates chaotic shuffling in wavelet domain,” in *International Con-*

- ference on Recent Advances and Innovations in Engineering (ICRAIE-2014)*.
IEEE, 2014, pp. 1–5.
- [60] M. Irfan, D. R. Ramdhania, I. S. Nita, T. Priatna, and A. R. Atmadja, “Design and build an early childhood puzzle educational game using the fisher-yates shuffle algorithm as an android-based scrambler for snippets,” in *2020 6th International Conference On Wireless And Telematics (Icwt)*. IEEE, 2020, pp. 1–6.
- [61] M. Tayel, G. Dawood, and H. Shawky, “Block cipher s-box modification based on fisher-yates shuffle and ikeda map,” in *2018 IEEE 18th International Conference on Communication Technology (ICCT)*. IEEE, 2018, pp. 59–64.
- [62] K. Tong, J. Wu, J. Yang, J. Li, J. Zhang, and L. Wang, “Random placement algorithm of military game based on fisher-yates,” in *2021 33rd Chinese Control and Decision Conference (CCDC)*. IEEE, 2021, pp. 2192–2196.
- [63] Y. M. Hasan, “Key-joined block ciphers with input-output pseudorandom shuffling applied to remotely keyed authenticated encryption,” in *2007 IEEE International Symposium on Signal Processing and Information Technology*. IEEE, 2007, pp. 74–79.
- [64] M. Alawida, “A novel chaos-based permutation for image encryption,” *Journal of King Saud University-Computer and Information Sciences*, vol. 35, no. 6, p. 101595, 2023.

- [65] S. Dey, "Sd-aei: An advanced encryption technique for images," in *2012 Second International Conference on Digital Information Processing and Communications (ICDIPC)*. IEEE, 2012, pp. 68–73.
- [66] M. Sharma and V. Bharti, "Image encryption using a new 2d bit reversed logistic map," in *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*. IEEE, 2020, pp. 1–6.
- [67] A. U. Zanzaney, C. K. Sharma, L. Jain, and C. Gururaj, "Proficient evaluation of visual cryptography using transposition cipher and bit reversal techniques," in *2022 Second International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT)*. IEEE, 2022, pp. 1–5.
- [68] M. A. S. Hassan and I. S. I. Abuhaiba, "Image encryption using differential evolution approach in frequency domain," *arXiv preprint arXiv:1103.5783*, 2011.
- [69] G. Leander, T. Moos, A. Moradi, and S. Rasoolzadeh, "The speedy family of block ciphers - engineering an ultra low-latency cipher from gate level for secure processor architectures," *Cryptology ePrint Archive*, Paper 2021/960, 2021, <https://eprint.iacr.org/2021/960>. [Online]. Available: <https://eprint.iacr.org/2021/960>
- [70] J. Ahmad, M. A. Khan, F. Ahmed, and J. S. Khan, "A novel image encryption scheme based on orthogonal matrix, skew tent map, and xor operation," *Neural Computing and Applications*, vol. 30, pp. 3847–3857, 2018.

- [71] A. I. Sallam, O. S. Faragallah, and E.-S. M. El-Rabaie, "Hvc selective encryption using rc6 block cipher technique," *IEEE Transactions on Multimedia*, vol. 20, no. 7, pp. 1636–1644, 2017.
- [72] S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish, and M. M. Fouda, "A new image encryption algorithm for grey and color medical images," *IEEE Access*, vol. 9, pp. 37 855–37 865, 2021.
- [73] T. Chuman, W. Sirichotedumrong, and H. Kiya, "Encryption-then-compression systems using grayscale-based image encryption for jpeg images," *IEEE Transactions on Information Forensics and security*, vol. 14, no. 6, pp. 1515–1525, 2018.
- [74] A. Shahverdi, M. Taha, and T. Eisenbarth, "Lightweight side channel resistance: threshold implementations of s imon," *IEEE Transactions on Computers*, vol. 66, no. 4, pp. 661–671, 2016.
- [75] M. Alawida, J. S. Teh, A. Mehmood, A. Shoufan *et al.*, "A chaos-based block cipher based on an enhanced logistic map and simultaneous confusion-diffusion operations," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 10, pp. 8136–8151, 2022.
- [76] J. Ahmad and F. Ahmed, "Efficiency analysis and security evaluation of image encryption schemes," *computing*, vol. 23, no. 04, p. 25, 2010.

- [77] F. Dikbaş, “A novel two-dimensional correlation coefficient for assessing associations in time series data,” *International Journal of Climatology*, vol. 37, no. 11, pp. 4065–4076, 2017.
- [78] Y. Chen, S. Xie, and J. Zhang, “A hybrid domain image encryption algorithm based on improved henon map,” *Entropy*, vol. 24, no. 2, p. 287, 2022.
- [79] I. Yasser, M. A. Mohamed, A. S. Samra, and F. Khalifa, “A chaotic-based encryption/decryption framework for secure multimedia communications,” *Entropy*, vol. 22, no. 11, p. 1253, 2020.
- [80] B. Ma and Y. Q. Shi, “A reversible data hiding scheme based on code division multiplexing,” *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 9, pp. 1914–1927, 2016.
- [81] Y. Zhao and L. Liu, “A bit shift image encryption algorithm based on double chaotic systems,” *Entropy*, vol. 23, no. 9, p. 1127, 2021.
- [82] I. F. Elashry, O. S. Farag Allah, A. M. Abbas, S. El-Rabaie, and F. E. Abd El-Samie, “Homomorphic image encryption,” *Journal of Electronic Imaging*, vol. 18, no. 3, pp. 033 002–033 002, 2009.
- [83] Y. Yang, L. Wang, S. Duan, and L. Luo, “Dynamical analysis and image encryption application of a novel memristive hyperchaotic system,” *Optics & Laser Technology*, vol. 133, p. 106553, 2021.

- [84] W. S. Sayed, A. G. Radwan, H. A. Fahmy, and A. Elsedek, "Trajectory control and image encryption using affine transformation of lorenz system," *Egyptian Informatics Journal*, vol. 22, no. 2, pp. 155–166, 2021.
- [85] C. Lakshmi, K. Thenmozhi, J. B. B. Rayappan, and R. Amirtharajan, "Hopfield attractor-trusted neural network: an attack-resistant image encryption," *Neural Computing and Applications*, vol. 32, no. 15, pp. 11 477–11 489, 2020.
- [86] A. Belazi, A. A. Abd El-Latif, and S. Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos," *Signal Processing*, vol. 128, pp. 155–170, 2016.
- [87] A. H. M. Ragab, O. S. F. Alla, and A. Y. Noaman, "Encryption quality analysis of the rc6 block cipher compared with rc5 algorithms," *Cryptology ePrint Archive*, 2014.
- [88] A. B. Mohamed, G. Zaibi, and A. Kachouri, "Implementation of rc5 and rc6 block ciphers on digital images," in *Eighth International Multi-Conference on Systems, Signals & Devices*. IEEE, 2011, pp. 1–6.
- [89] C. E. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, 1948.
- [90] H.-H. Nien, S. Changchien, S. Wu, and C. Huang, "A new pixel-chaotic-shuffle method for image encryption," in *2008 10th International Conference on Control, Automation, Robotics and Vision*. IEEE, 2008, pp. 883–887.

- [91] Y. Wu, J. P. Noonan, S. Agaian *et al.*, “Npcr and uaci randomness tests for image encryption,” *Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT)*, vol. 1, no. 2, pp. 31–38, 2011.
- [92] Z. Man, J. Li, X. Di, Y. Sheng, and Z. Liu, “Double image encryption algorithm based on neural network and chaos,” *Chaos, solitons & fractals*, vol. 152, p. 111318, 2021.
- [93] H. R. Shakir, “An image encryption method based on selective aes coding of wavelet transform and chaotic pixel shuffling,” *Multimedia Tools and Applications*, vol. 78, no. 18, pp. 26 073–26 087, 2019.
- [94] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert *et al.*, *A statistical test suite for random and pseudorandom number generators for cryptographic applications*. US Department of Commerce, Technology Administration, National Institute of ..., 2001, vol. 22.
- [95] Z. Liang, Q. Qin, C. Zhou, N. Wang, Y. Xu, and W. Zhou, “Medical image encryption algorithm based on a new five-dimensional three-leaf chaotic system and genetic operation,” *PloS one*, vol. 16, no. 11, p. e0260014, 2021.
- [96] Q. Li, X. Wang, B. Ma, X. Wang, C. Wang, S. Gao, and Y. Shi, “Concealed attack for robust watermarking based on generative model and perceptual loss,”

- IEEE Transactions on Circuits and Systems for Video Technology*, vol. 32, no. 8, pp. 5695–5706, 2021.
- [97] Z. Hua, K. Zhang, Y. Li, and Y. Zhou, “Visually secure image encryption using adaptive-thresholding sparsification and parallel compressive sensing,” *Signal Processing*, vol. 183, p. 107998, 2021.
- [98] H. C. Van Tilborg and S. Jajodia, *Encyclopedia of cryptography and security*. Springer Science & Business Media, 2014.
- [99] N. T. Courtois and G. V. Bard, “Algebraic cryptanalysis of the data encryption standard,” in *Cryptography and Coding: 11th IMA International Conference, Cirencester, UK, December 18-20, 2007. Proceedings 11*. Springer, 2007, pp. 152–169.
- [100] N. T. Courtois, “General principles of algebraic attacks and new design criteria for cipher components,” in *International Conference on Advanced Encryption Standard*. Springer, 2004, pp. 67–83.
- [101] V. Manikandan and R. Amirtharajan, “On dual encryption with rc6 and combined logistic tent map for grayscale and dicom,” *Multimedia Tools and Applications*, vol. 80, no. 15, pp. 23 511–23 540, 2021.
- [102] N. Tsafack, J. Kengne, B. Abd-El-Atty, A. M. Iliyasu, K. Hirota, and A. A. Abd EL-Latif, “Design and implementation of a simple dynamical 4-d chaotic circuit with applications in image encryption,” *Information Sciences*, vol. 515, pp. 191–217, 2020.

- [103] L. Reyes-López, J. Murguía, H. González-Aguilar, M. T. Ramírez-Torres, M. Mejía-Carlos, and J. Armijo-Correa, “Scaling analysis of an image encryption scheme based on chaotic dynamical systems,” *Entropy*, vol. 23, no. 6, p. 672, 2021.

VITAE

- Name: Mahmoud Yassin Mahmoud Yassin.
- Nationality: Egyptian.
- Date of Birth: 05/02/1996.
- Email: *mahmoud.yassin2211@gmail.com*
- Permanent Address: 9, Beshir Bek Street, Altabia, Aswan, Egypt.
- Education: Bachelor of science in Electronics & Communications Engineering, Arab Academy for Science, Technology & Maritime Transport (AAST), Egypt: (GPA:3.91/4), "Distinction with Honor", 2019.
- Work Experience:
 - Graduate Teaching Assistant, Electrical Engineering Department, College of Engineering & Physics, King Fahd University of Petroleum & Minerals, Saudi Arabia: Spring 2022- Present.
 - Graduate Teaching Assistant, Electronics & Communications Engineering Department, College of Engineering & Technology, Arab Academy for Sci-

ence, Technology & Maritime Transport, Egypt: Spring 2021 & Summer 2021.

- Soldier Engineer, Unmanned Integrated Systems Technology, and Innovation Center (UMISTIC), Military Technical College, Cairo, Egypt: 12/2019 - 12/2020.
- Site Engineer, GLEXTEL Company, Aswan Office, Egypt: 07/2019 - 09/2019.