

AN ENHANCED COLOR IMAGE
ENCRYPTION ALGORITHM USING LT-PRNG



SABA MOHAMMED ISMAEL

UMP

MASTER OF SCIENCE

UNIVERSITI MALAYSIA PAHANG

UNIVERSITI MALAYSIA PAHANG

DECLARATION OF THESIS AND COPYRIGHT

Author's Full Name : Saba Mohammed Ismael

Date of Birth : 03/10/1987

Title : An Enhanced Color Image Encryption Algorithm using
LT-PRNG

Academic Session : Semester 1 2018/2019

I declare that this thesis is classified as:

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

I acknowledge that Universiti Malaysia Pahang reserves the following rights:

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

Certified by:

(Student's Signature)

A12342556
New IC/Passport Number
Date: 08/10/2018

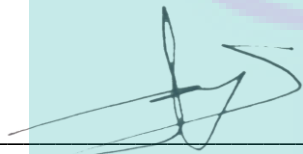
(Supervisor's Signature)

Dr. Mohamed Ariff Ameen
Name of Supervisor
Date: 08/10/2018

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

SUPERVISOR'S DECLARATION

I hereby declare that I have checked this thesis and in our opinion, this thesis is adequate in terms of scope and quality for the award of the degree of Master of Computer Science.



(Supervisor's Signature)

Full Name : DR. MOHAMED ARIFF AMEEDEN

Position : SENIOR LECTURER

Date : 08/10/2018



UMP

STUDENT'S DECLARATION

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

(Student's Signature)

Full Name : SABA MOHAMMED ISMAEL

ID Number : MCC16002

Date : 08/10/2018

UMP

AN ENHANCED COLOR IMAGE ENCRYPTION ALGORITHM USING
LT-PRNG

The logo of the University of Malaysia Pahang (UMP) is a shield-shaped emblem. It features a central white vertical band. The left side of the shield is light blue, and the right side is light purple. At the top, there is a yellow diamond shape. A stylized, swirling line in light blue and purple encircles the top part of the shield.

SABA MOHAMMED ISMAEL

Thesis submitted in fulfillment of the requirements
for the award of the
Master of Science

UMP

Faculty of Computer Systems and Software Engineering
UNIVERSITI MALAYSIA PAHANG

OCTOBER 2018

ACKNOWLEDGEMENTS

My greatest adoration and thanks to The Great Almighty God who enabled me to complete this act of faith. My sincere gratefulness and love to my husband (Sinan), my lovely son (Taym), and my daughter (Tara). For their endless love, prayers, sacrifice and support to pursue and successfully complete my master studies.

To my family, thank you for encouraging me in all of my pursuits and inspiring me to follow my dreams. I am especially grateful to my parents, who supported me emotionally. I always knew that you believed in me and wanted the best for me. Thank you for teaching me that my job in life was to learn, to be happy, and to know and understand myself; only then could I know and understand others.

Foremost, I would like to express my sincere gratitude to my supervisor Dr. Mohamed Ariff Ameen for taking out time to ensure qualitative supervision of this research. Thanks a lot for your support and frequent feedback.

A large, faint watermark of the UMP logo is centered on the page. It consists of a shield-like shape formed by four triangles meeting at the center. The top-left triangle is light blue, the top-right is light purple, the bottom-left is light purple, and the bottom-right is light blue. The letters 'UMP' are written in white, bold, sans-serif font across the center of the shield.

UMP

ABSTRAK

Dengan adanya komputer dan Internet, maklumat seringkali dihantar melalui Internet. Walau bagaimanapun, maklumat penting boleh digodam atau terganggu semasa penghantaran melalui Internet; oleh itu, keselamatan ke atas maklumat perlu diutamakan. Penyulitan imej adalah salah satu kaedah yang paling penting untuk melindungi maklumat berbentuk imej. Dengan bantuan algoritma penyulitan imej, 'plaintext' bagi imej disulitkan ke dalam bentuk 'ciphertext' sebelum dihantar. Hanya penerima yang dibenarkan boleh menyahsulit 'ciphertext' dengan kata kunci rahsia untuk mendapatkan 'plaintext'. Beberapa algoritma penyulitan imej berasaskan imej yang kacau bilau menggunakan tahap kekacauan yang rendah sebagai alat penyulitan. Walaupun algoritma ini mudah dan sesetengahnya berkesan, kebanyakannya tidak cekap kerana sebab-sebab berikut: pertama, terdapat keselamatan yang rendah disebabkan oleh degradasi dinamik pada sistem 'chaotic' ketika merealisasikan dengan komputer digital; kedua, beberapa penyulitan berasaskan tahap kekacauan yang rendah mempunyai kelajuan prestasi yang perlahan kerana pengiraan detik apungan analitikal yang menjadikan penyulitan tidak dapat dilaksanakan pada masa-nyata. Selain itu, jika sistem 'chaotic' dengan binaan yang mudah digunakan secara langsung untuk menyulitkan imej, maklumat berguna boleh diekstrak dari orbit 'chaotic'. Untuk mengatasi kekurangan ini, peta hibrid 'chaotic' telah dicadangkan. 'Chaotic' hibrid mempunyai beberapa ciri yang sangat bagus dan dapat mengatasi beberapa kekurangan 'chaotic' pada tahap yang rendah. Dalam kajian ini, peta hibrid 'chaotic' berdasarkan peta logistik dan peta tenda dicadangkan untuk menjana urutan rawak untuk meningkatkan prestasi kesulitan algoritma penyulitan imej. Algoritma penyulitan imej bergantung pada struktur aturan Fridrich, oleh itu, penambahbaikan struktur ini dicadangkan. Pada peringkat kekeliruan, piksel disusun berdasarkan urutan yang dijana melalui PRNG yang dicadangkan untuk setiap warna, sementara itu pada peringkat penyebaran, nilai piksel diubah menggunakan operator XOR antara semua warna untuk mencapai kadar gabungan yang tinggi. Skema yang dicadangkan telah diuji secara statistik menggunakan ujian NIST dan telah dianalisis untuk membuktikan bahawa ia mempunyai ruang utama yang besar, dan sensitif terhadap nilai awal. Kesimpulannya, skim yang dicadangkan adalah cekap dari segi kepekaan terhadap kekunci, kepekaan terhadap 'ciphertext', kekeliruan yang baik, penyebaran, dan kelajuan. Tidak ada kemungkinan penyerang memecahkan 'cipher' itu, kerana skema menunjukkan kekeliruan dan sifat penyebaran yang sempurna, dan boleh menahan serangan 'plaintext' yang diketahui / dipilih. Oleh itu, skema ini kukuh dan dilaksanakan dengan cekap, dan boleh digunakan dalam aplikasi masa-nyata.

ABSTRACT

With the advent of computer and Internet, information is commonly transmitted via the Internet. However, vital information can be hacked or interrupted during an active transmission over the Internet; therefore, the need for information security is paramount. Image encryption is one of the most important methods for protecting image information. With the aid of image encryption algorithms, the plaintext of the image is encrypted into the ciphertext before sending. Only the authorized receiver can decrypt the ciphertext with the secret key(s) to obtain the plaintext. Several chaos-based image encryption algorithms use low-dimension chaos as the encryption tools. Although these algorithms are simple and effective to some extent, most of them are inefficient due to the following reasons: firstly, there is a low security due to the dynamic degradation of chaotic systems in their realization with a digital computer; secondly, some low-dimension chaos-based encryptions have slow performance speeds because of analytical floating-point computations which makes encryption infeasible in real time. Moreover, if chaotic systems with simple constructions are directly used to encrypt an image, the useful information can be extracted from the chaotic orbits. To overcome these drawbacks, hybrid chaotic maps have been proposed. Hybrid chaos has several excellent characteristics and can overcome some drawbacks of low-dimension chaos. In this study, a hybrid chaotic map based on logistic map and tent map is proposed for generating a random sequence for enhancing the encryption performance of image encryption algorithms. The image encryption algorithm depends on the Fridrich encryption model; thus, an enhancement of this structure is proposed. The confusion stage sorts the pixel based on the generated sequence by the proposed PRNG for each color, while the diffusion stage changes in the values of the pixel by using XOR operator between all colors to attain a high rate of correlation, the proposed PRNG is called ‘Logistic Tent Map Pseudorandom Number Generator ‘LT-PRNG’. The proposed scheme has been tested statistically using NIST test suit and has been analyzed to prove that it has a big keyspace, and sensitive to initial values. In conclusion, the proposed scheme is efficient in terms of sensitivity to the key, sensitivity to the ciphertext, good confusion, diffusion. There is no possibility of an attacker breaking the cipher, as the scheme showed perfect confusion and diffusion properties, and can withstand known/chosen plaintext attacks. Thus, the scheme is robust and performed efficiently, and may be used in real-time applications. For future studies, the proposed encryption algorithm can be enhanced by combined compression encryption techniques, which would increase the encryption efficiency. Additionally, in future, the work can be extended, by applying the theoretical aspects of cipher design, to Integrated Circuit (IC) chip based implementation, and make an effort to better the performance of chaotic image encryption.

TABLE OF CONTENT

DECLARATION

TITLE PAGE

ACKNOWLEDGEMENTS **ii**

ABSTRAK **iii**

ABSTRACT **iv**

TABLE OF CONTENT **v**

LIST OF TABLES **viii**

LIST OF FIGURES **ix**

LIST OF SYMBOLS **x**

LIST OF ABBREVIATIONS **xi**

CHAPTER 1 INTRODUCTION **1**

1.1 Background 1

1.2 Problem Statement 5

1.3 Research Questions 6

1.4 Objectives 6

1.5 Scope 7

1.6 Limitations 7

1.7 Thesis Organization 7

CHAPTER 2 LITERATURE REVIEW **9**

2.1 Introduction 9

2.2 Cryptography 9

2.3	Chaos Based Cryptography	11
2.4	Chaos-Based Random Number Generator	13
2.5	Chaotic-Map Based Image Encryption	18
2.6	The Problems with Permutation Algorithms	22
2.7	Related Works	24
	Mixed linear-nonlinear coupled map lattices	32
2.8	Standard Chaotic Maps	35
2.8.1	Logistic Map	35
2.8.2	The Tent Map	37
2.9	The NIST Statistical Test Suite	39
2.9.1	The NIST Test Suit	39
2.10	Summary	42
	CHAPTER 3 METHODOLOGY	44
3.1	Introduction	44
3.2	Proposed Image Encryption System	45
3.3	The proposed PRNG Algorithm	47
3.4	Image Encryption algorithm	52
3.5	Summary	55
	CHAPTER 4 RESULTS AND DISCUSSION	57
4.1	Introduction	57
4.2	Security Analysis	57
4.2.1	Key Space Analysis	58
4.2.2	Key Sensitivity	59
4.2.3	Histogram Analysis	62

4.2.4	Correlation of Two Adjacent Pixels	66
4.2.5	Correlations between Plain and Cipher Images	70
4.2.6	Information Entropy Analysis	72
4.2.7	NPCR and UACI Analysis	73
4.2.8	The NIST Testing Strategy	74
CHAPTER 5 CONCLUSION AND FUTURE WORKS		76
5.1	Introduction	76
5.2	Conclusion	77
5.3	Future Works	78
REFERENCES		80
PUBLICATIONS		91

LIST OF TABLES

Table 2.1	A comparison of the different permutation algorithms	23
Table 2.2	Advantages and disadvantages of the most related works	31
Table 3.1	First phase of XOR process	50
Table 3.2	Second phase of XOR process	50
Table 3.3	Third phase of XOR process	50
Table 4.1	Parameters values for the experiments	58
Table 4.2	The key space results	59
Table 4.3	Correlation coefficients of two adjacent pixels in vertical direction	67
Table 4.4	Correlation coefficients of two adjacent pixels in horizontal direction	67
Table 4.5	Correlation coefficients of two adjacent pixels in diagonal direction	67
Table 4.6	Correlation coefficients of two adjacent pixels for Lena	69
Table 4.7	Correlations between Plain and Cipher image for all colors	70
Table 4.8	Correlation coefficient between the image and cipher image	71
Table 4.9	Correlation coefficient comparison to other related work on Lena	71
Table 4.10	Information entropy of the proposed algorithm	72
Table 4.11	Comparison of information entropy	73
Table 4.12	NPCR and UACI of ciphered image with one bit different	74
Table 4.13	Results of NIST	75

LIST OF FIGURES

Figure 2.1	The process of a simple image encryption	10
Figure 2.2	A classic image encryption architecture	20
Figure 2.3	Classification of Image Encryption	21
Figure 2.4	Bifurcation of the logistic map	36
Figure 2.5	The logistic map Lyapunov exponent	36
Figure 2.6	The tent map Lyapunov exponent	37
Figure 2.7	Bifurcation of Tent map	38
Figure 3.1	The block diagram of the proposed system	46
Figure 3.2	Block diagram of LT-PRNG	47
Figure 3.3	Chaotic numbers generator	48
Figure 3.4	XOR Processes	49
Figure 3.5	Pseudocode for LT-PRNG	52
Figure 3.6	Pseudocode for confusion algorithm	54
Figure 3.7	Pseudocode of diffusion algorithm	54
Figure 3.8	Example of Confusion and Diffusion stages	56
Figure 4.1	Key sensitivity analysis	60
Figure 4.2	Sensitivity analysis for encryption algorithm	61
Figure 4.3	Histogram analysis for Lena image	63
Figure 4.4	Histogram analysis for Baboon image	64
Figure 4.5	Histogram analysis for Peppers image	66
Figure 4.6	Horizontal correlation of the original and cipher Baboon image	68
Figure 4.7	Horizontal correlation of the original and cipher Lena image	68
Figure 4.8	Horizontal correlation of the original and cipher Peppers image	69

LIST OF SYMBOLS

μ	Mutation of Logistic Map
λ	Lyapunov exponent
Lim	Limit
ω	Mutation of Tent Map
X_0	Initial Value for Logistic Map
Y_0	Initial Value for Tent Map
t	Number of Iterations for the Initial Stage of PRNG
X_t	Input Value to the LTM Map
Y_t	Input Value to the TLM Map
R	Output for one Iteration
β	Number of Bits
N	Hight or Width of Plain Image
C	Color
CP	Color permutation Generated By PRNG
CC	Confused Color
X_R	Initial Value for Red LM
X_G	Initial Value for Green LM
X_B	Initial Value for Blue LM
Y_R	Initial Value for Red TM
Y_G	Initial Value for Green TM
Y_B	Initial Value for Blue TM

LIST OF ABBREVIATIONS

DES	Data Encryption Standard
AES	Advance Encryption Standard
RSA	Rivest-Shamir-Adleman
DNA	Deoxyribonucleic Acid
PRNG	Pseudo Random Number Generator
CM	Chaotic Map
1D	One Dimension
2D	Two Dimension
MD	Multi Dimension
LM	Logistic Map
TM	Tent Map
LTM	Logistic Tent Map
TLM	Tent Logistic Map
LT-PRNG	Logistic Tent- Pseudo Random Number Generator
BLP	Bit Level Permutation
IDEA	International Data Encryption Algorithm
XTEA	Extended Tiny Encryption Algorithm
BFA	Brute Force Attack
DMLM-PRNG	Digitalized Modified Logistic Map-based Pseudo Random Number Generator
CML	Coupled Map Lattice
CMLDCI	Coupled Map Lattice based on Discrete Chaotic Iteration
CCCBG	Cross Couple Chaotic Random Bit Generator
SNS	Social Network Service
CNCM	Couple Nonlinear Chaotic Map
PWLCM	Piecewise Linear Chaotic Map
ANN	Artificial Neural Network
MLP	Multi-Layer Perceptron
RGB	Red-Green-Blue
NIST	National Institute of Standard and Technology
NPCR	Number of Pixels Change Rate
UACI	Unified Average Changing Intensity
CC	Correlation Coefficient

CHAPTER 1

INTRODUCTION

1.1 Background

The realities of the modern ways of life have necessitated the need to monitor all aspects of our daily activities. The information generated is considered an asset and it people tend to want to keep it safe from attacks of various types (Solms and Niekerk, 2013a). This means that only those authorized should have access to the information. To keep information safe, it must be hidden from unauthorized people. Computers have become an essential part of information storage as well as its transfer from one part of the world to other. Most of the information transferred is through computer networks. Information could consist of for example text, audio, image or videos. A basic requirement of any information transfer is to keep it confidential and integral. Information can be hacked at any point of transfer between the source and the destination. Computer networks face different types of information thefts (Radwan et al., 2016).

Currently, many different types of information are transmitted over computer networks. It is not only text files, but also audio, digital images and video (Mohit Kumar et al., 2014a). With the rapid development of mobile phones, internet and other digital communication technologies, it has become very important for information to reach its destination securely. The technical way to secure this information is by cryptography (Oğraş and Türk, 2016) or steganography (Cheddad et al., 2010; Kaur and Behal, 2014). The science of consuming the calculation and math behind the procedure to encrypt and decrypt data is called cryptography. Cryptography involves the protection of sensitive information as it pass through an insecure networks in order to keep it safe from the public except the intended receiver. Encryption provides the ways and means to safeguard the data from unauthorized access (Solms and Niekerk, 2013b; Stallings, 2011).

Several multimedia applications have recently emerged, such as digital TV broadcast, on-line video conferencing, and distance education networks. Highly advanced multimedia processing technologies and ubiquitous network access are the two most important factors driving this trend. On one hand, new technologies facilitate the creation, transmission, exchange, and storage of large volumes of digitized multimedia data. On the other hand, the need for digital rights protection becomes more urgent. In particular, the internet provides a public network that allows illegal distribution of multimedia data much more easily. Thus, multimedia data security, which is the core of Digital Rights Management (DRM) systems, has gained a lot of attention in academia as well as industry.

Digital media is facing multiple kinds of attacks, such as intercepting, altering, changing or removing data from the source. The field of multimedia security has recently developed to provide protection to digital media. In this scenario, the security of multimedia digital packets have become important and cryptography is a way to secure digital multimedia packets. The size of an image file is larger than other digital data like text and audio. This means that encryption of digital images requires large amounts of computation, hence the need to devise special algorithms to handle this type of data. Some standards cryptographic algorithms are used to provide secure transmission of digital images like DES, AES and RSA. But chaotic maps and DNA technology are the two most popular topics currently used in image encryption, combined or separately. These two technologies have good security features and can be used in digital image security(Aljawarneh et al., 2017; Pande and Zambreno, 2013).

During transmission over the global network, digital images are subject to security attacks. Therefore, information security of the digital image has become a burning research issue. Image cryptography is usually achieved by the user through traditional encryption algorithms. In theory, the traditional encryption techniques are good, but most traditional encryption is developed for text data without considering the unique characteristics of image data. Compared to the encryption of traditional alphanumeric data files, the encryption of multimedia data has encountered several new challenges due to their unique characteristics. First, the size of the multimedia content is often substantially larger than that of the text data. A total encryption approach that encrypts the entire multimedia content demands a very large amount of computation. This

means that the above techniques are not only inefficient but also less secure (Singh, 2013; Xuancai Zhang et al., 2017) .

All systems can be broadly classified as deterministic, stochastic (probabilistic) or chaotic systems of which chaotic systems are most unpredictable. Chaotic maps are often used in the study of dynamical systems which exhibit behaviors that are highly sensitive to initial conditions and even small perturbations can yield widely diverging outcomes. Still these systems are deterministic because based on the initial condition future behavior can be predicted, hence, their behavior could be called deterministic chaos. There is a close relationship between chaotic systems and cryptography which makes chaos-based algorithms a natural candidate for image encryption.

The two basic properties of a good cipher are confusion and diffusion and both are important features of chaotic systems too. For real-time applications encryption schemes which take lesser computational time but wouldn't compromise with the desired security are suitable. Chaos-based encryption technique is a good amalgamation of high speed, security, complexity and less power consumption(Dăscălescu et al., 2013; Xuancai Zhang et al., 2017).

The basic principle of chaos-based encryption is to use the dynamical systems to generate a sequence of numbers that are pseudo-random in nature and these sequences could be used as a key to encrypt input image. For given parameters two initial conditions can deviate exponentially into two different trajectories. These parameters can be used for encryption and decryption and keys can be chosen from these conditions. Due, to these chaotic parameters and initial condition we could generate a large key space which further enhances the security. Because of the random behavior, the output seems random to the attacker whereas only the sender and receiver know that the system is well defined. Also, these algorithms are easier and cheaper to be embedded onto small chips, which make them a good fit for encryption systems.

There is a need to develop reliable encryption schemes to fulfil the ever-increasing security need of the increasing data of communication system. The study of chaos proved a better encryption technology for providing security to sensitive data that uses non-periodic signals generated by chaotic system, which has features such as randomness, extreme sensitivity to initial conditions for encryption. Thus, the use of

discrete chaotic maps not only helps to build a good encryption system but also makes it a good candidate for efficiency. To ensure the security of digital image information, the effective protective measure is image encryption(Kanso and Ghebleh, 2017; W. Zhang et al., 2016).

The security of a digital image has attracted much attention recently. A combination of the chaotic theory and cryptography improves security. Chaos is the study of nonlinear systems, which are highly sensitive to initial conditions and parameter values. Chaotic schemes deal with designing encryption schemes using chaotic systems(Mohit Kumar et al., 2014b; Radwan et al., 2016).

Chaotic cryptosystems are nonlinear and deterministic. Chaotic maps are used to generate a series of pseudorandom values for image encryption schemes. Some maps fail to generate a larger sequence of pseudorandom values and fail to have random-like behavior. The logistic map is a simple, widely used classical map. It is used in many schemes, especially in designing image encryption schemes. Though it is suitable for image encryption, it has some common problems, such as a stable window, blank window, uneven distribution and weak key(Murillo-Escobar et al., 2017).

The motivation behind this research is the ever-increasing need for harder to break encryption algorithm as the computer and network technologies evolve. By proposing chaos base image encryption algorithm, it will help to reduce the relationship among image elements by increasing the entropy value of the encrypted images as well as lowering the correlation.

Most of the schemes in the literature are linear in nature, have less sensitivity to the plaintext, fail to withstand attacks and have a lower speed. Besides, the key is relatively small, the key sequence is equivalent, the sensitivity to the key is less, the computation cost is high, and security is less. Cryptanalysis techniques are considered in the design of new encryption schemes. The main motivation of the study is to increase the key length using a new set of chaotic maps, and to design a simple and fast image encryption system using new chaotic maps with high security that can withstand known attacks.

1.2 Problem Statement

There are several beneficial properties of the chaotic systems, including but not limited to ergodicity, pseudo-randomness, periodicity, control parameters, and high sensitivity to initial conditions. These properties have endeared the chaotic systems to several researchers for application in image encryption (Xu et al., 2016).

There are two major categories of the chaotic systems/maps in image encryption algorithms, which are one dimensional chaotic systems (1D) and multi-dimensional (MD) chaotic systems. Majority of the applications of the MD chaotic maps are in image security (W. Liu et al., 2016; Zhou, Bao, et al., 2014) owing to their multiple parameters and complex structures. Meanwhile, hardware/software implementation and computational complexity usually increase in the presence of multiple parameters (Lingfeng Liu and Miao, 2016; Ye, 2010). Contrarily, the 1D chaotic systems are simple structured and easy to implement (Li, Chunhu and Luo, Guangchun and Qin, Ke and Li, 2017; Zhou, Bao, et al., 2014), though they are notorious to four problems which include:

- A limited or/and discontinuous range of chaotic behaviours.
- Vulnerable to low computation cost analysis when using correlation and iteration functions.
- A non-uniform data distribution of output chaotic sequences (Arroyo et al., 2013; Chai, 2017; Li et al., 2009; Yuan et al., 2017).
- The key space is usually small when using them for generation of a pseudo-random number, and leads to the development of weak encryption algorithms (Leyuan Wang et al., 2016).

With these in mind, there is a need to enhance the chaotic maps to overcome the above-mentioned issues.

There are two categories of the current chaos-based image cryptosystems (Permutation); the first category has a pixel considered as the least element while a digital image is regarded as a collection of several pixels; but in the second category, a pixel can be subdivided to bit level where operations are carried out. A pixel in a grey-scale image, for instance, is usually comprised of 8 bits which carry different levels of information (Zhu et al., 2011). The permutation of the pixels can be done on one of two strategies

which are sorting based or 2D chaotic map-based. The first strategy has a long execution time which is not acceptable, while the second strategy may produce some repeated patterns.

Conclusively, these strategies have certain drawbacks (Zhang et al., 2016) and to overcome these challenges, a hybrid of two chaotic maps (Logistic map and Tent map) based colored image encryption algorithm is set forth. The proposed algorithm has the ability to protect the contents of images by generating big enough key spaces and stand against the well-known attacks.

1.3 Research Questions

In the context of finding a good algorithm that is able to enhance the performance of image encryption algorithms by using chaotic maps, this thesis seeks to answer the following research questions:

- i. What are the available algorithms used currently for generating pseudorandom number generator (PRNG) sequences?
- ii. What is the proposed PRNG algorithm that would be able to generate random key sequences with big enough key space (i.e. more than 2^{128})?
- iii. What is the proposed encryption algorithm that would be able to protect the contents of the digital coloured images as compared to the existing algorithms?

1.4 Objectives

The main aim of this thesis is to provide an efficient encryption algorithm for colored images cryptography. The proposed algorithm uses a unique design of pseudorandom random number generator PRNG. In detail, the following tasks are to be undertaken:

- i. To investigate image encryption algorithms based on chaotic maps and highlight their weaknesses.
- ii. To enhance the image encryption algorithm by designing a hybrid chaotic PRNG based on logistic map and tent map.
- iii. To validate and analyse the results of the proposed PRNG method and encryption algorithm.

1.5 Scope

The main focus of this project is the design of an efficient encryption algorithm for filed colored images cryptography (RGB color to be precise). The system will use a unique design, based on two chaotic maps logistic map and tent map. These chaotic maps with two new hybrid chaotic maps called Logistic-Tent Map (LTM) and Tent-Logistic Map (TLM), generate a pseudo random number sequence. The generated sequence is used twice as permutation key, first time, for the confusion stage, when the pixels are sorted totally (columns and rows), and second time, for the diffusion stage, when the values of all the pixels are change based on this key. Both stages, work in a novel way, and together with the PRNG, they form the new encryption algorithm.

1.6 Limitations

The study will not cover the other cryptography fields, such as texts, audios, and videos encryption. Also, it will not cover the block cipher algorithm such as DES, AES, or 3DES.

1.7 Thesis Organization

Chapter 1 provides an introduction to cryptography and chaos-based image encryption. In this chapter, problem statement for this research work is explained. This chapter describes the objectives of this research and the organization of the thesis.

The related works in this area are discussed in chapter 2. The literature survey includes the chaos based random number generator, and different image encryption schemes, for both gray scale and color images. In this chapter various existing schemes, chaotic maps, the cryptanalysis of chaotic schemes and their drawbacks are also discussed.

Chapter 3 first presents a detailed description of the preliminary study phase followed by the modeling phase for the proposed pseudorandom number generation (PRNG). An encryption algorithm that included the proposed PRNG is created in the

development phase. Finally, the evaluation phase discusses the method to evaluate the performance of the proposed algorithms.

Chapter 4 discussed the testing and evaluation of the proposed algorithms. The proposed algorithm had been tested and evaluated in two parts. The first part shows the results of the proposed PRNG, consisting of two tests, (Security analysis tests (key space analysis and key sensitivity analysis), and Statistical analysis (NIST test suit)). The second part shows the results of the proposed encryption algorithm, in three sets of tests (histogram, correlation coefficient, and NPCR, UACI).

Chapter 5 summarized this research work and present the suggested future work.



UMP

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

A review of the most prominent related studies conducted on chaos-based cryptography in general, and image encryption in particular, is going to be presented. The first part explains the cryptography, and the chaos-based cryptography. While the second part explains pseudorandom number generator based on chaotic maps, with the most important related works. Finally, image encryption based on chaotic map is explained with the identification of the problems of encryption algorithms which have proposed in the literature.

2.2 Cryptography

Cryptology as a science mainly deals with the provision of information security in the digital space(Hamza, 2017). A handbook of applied cryptography (Menezes et al., 1997) provided a thorough overview of cryptology. There are many aspects of information security, of which the most important are authenticity and confidentiality. Confidentiality refers to the keeping sensitive information away from unauthorized access, while authenticity involves both the preservation of data integrity (not to be tampered by an unauthorized person) and ascertaining the source of the data (authentication of data origin). The field of cryptology is generally divided into two related fields which are cryptography and cryptanalysis (Solms and Niekerk, 2013b)

The design of protocols and algorithms for information security has been studied by (Delfs and Knebl, 2015; Stallings, 2011). It would be ideal to develop secure

algorithms but this could only be achieved in limited cases. Therefore, the best approach towards assessing the security of cryptographic algorithms is by subjecting it to all known attacks. Cryptanalysis deals with the study of mathematical techniques that attempt to break cryptographic primitives.

There are two families of cryptographic algorithms - symmetric and asymmetric algorithms (Katz and Lindell, 2008; Ostrovsky, 2010; Radwan et al., 2016). The symmetric algorithms which are also known as secret key algorithms require the sharing of a secret key among the communicating parties, but in asymmetric algorithms (which are also known as public key algorithms), a public key is kept in the public domain while its corresponding private key is secretly kept by a single entity.

The conversion of a plaintext into a ciphertext involves a process known as encryption, while decryption involves plaintext recovery from the ciphertext. Figure 2-1 shows these two processes in a cryptographic system.

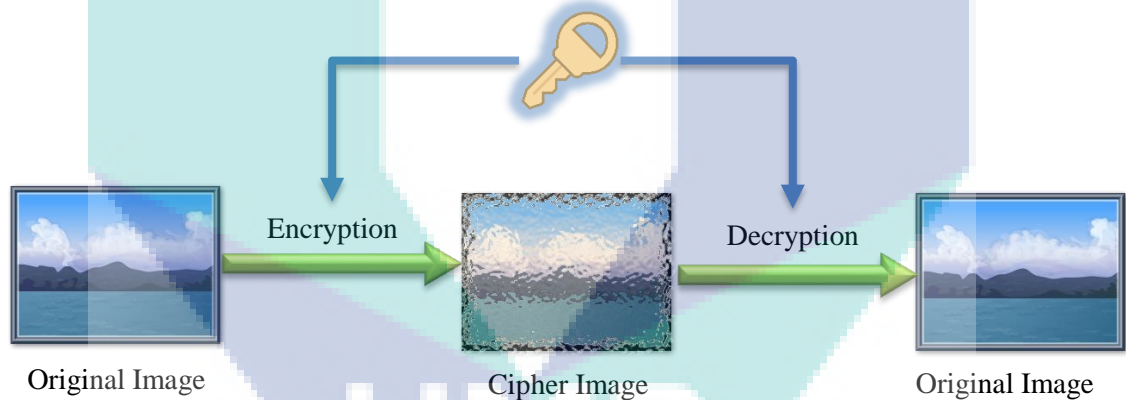


Figure 2.1 The process of a simple image encryption

Some of the conventional cryptographic algorithms include Blowfish, Triple Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), RC6, MRC6, Extended Tiny Encryption Algorithm (XTEA), Advanced Encryption Standard (AES), ARIA and so on. These text-based encryption schemes are unreliable in protecting image data due to some special image data features such as having a strong redundancy, strong correlation among pixels and the bulk storage size of the uncompressed data.

2.3 Chaos Based Cryptography

Chaos is naturally multidisciplinary as it has a wide range of coverage, including physics, communications, mathematics, and engineering. A proposal for a chaos-based cryptography based on the logistic map for message encryption has been made by (Baptista, 1998). Chaotic maps have a wide area of application in cryptography. (Matthews, 1989) formulated a one-dimensional chaotic map and recommended its use for the generation of pseudo-random sequences that can be utilized for message encryption. There are several good features of chaotic sequences, such as the ease of generating the keys and the dependency on the parameter values and initial conditions. The security of data can be enhanced by applying chaos to cryptography due to the excellent features of chaotic sequences. The properties of chaotic systems are:

- **Deterministic:** Their behaviour can be determined using certain mathematical equations.
- **Unpredictable and nonlinear:** They are too sensitive to initial conditions to an extent that even a slight variation in the starting point can result in a significantly different result.
- **Randomness:** They present to be disorderly and random, but in the actual sense, they are not random. There is a sense of order and pattern concealed under their random nature.

Due to the lack of the confusion property, most of the suggested cryptosystems based on chaos can be broken easily. Security-wise, (Fridrich, 1998a) suggested that a good cryptosystem should possess the following desirable features:

- **Must be key sensitive:** A totally different cipher text can be created by changing a bit in a key even when it is used on the same plaintext.
- **Must be plaintext sensitive:** A totally different cipher text could be created by changing one bit in the plaintext.
- **Must map the plaintext to the random cipher text:** The cipher text should not have any recognized pattern.

From the listed features, the first two features relate to the diffusion property while the last feature relates to the confusion property. A good cipher should strongly withstand all forms of cryptanalytic attacks. Attack resistance is to an extent, a good performance measure of a cryptosystem. Based on the method of the attacker's access to additional information, crypto-attacks may be divided into 5 classes:

1. Cipher text only attack

The attacker can access the communication medium and eavesdrop some segments of the cipher text which have been encrypted using a certain key. The attacker aims to reveal the plaintext as much as possible, and also to extract the cipher key.

2. Known-plaintext attack

In this form of attack, the attacker is in possession of the plaintext and its corresponding cipher text samples and tries to use both to extract the hidden information such as the secret keys.

3. Chosen-plaintext attack

This is an attack where the intruder can arbitrarily select some plaintexts to be encrypted in order to observe the corresponding cipher texts.

4. Chosen-cipher text attack

Here, the attacker can select different ciphertext segments and aim to get their corresponding plaintext. Beside these afore-mentioned attacks, there is also exhaustive key search attack, where the attacker tries to get the key in the key space in order to completely decrypt the plain image. This exhaustive searching works quite well only if the cipher has a small key space, given the availability of the supercomputing power today.

5. Brute-force attack (BFA)

A method of attack in which the intruder breaks a cipher by searching exhaustively for all possible keys is known as brute-force attack. A BFA is quicker when the cipher is weak. The size of the cipher key space K and the available computational power to the intruder determines the possibility of a BFA on a cipher. A key space of

about $K < 2^{128}$ has been generally accepted as not sufficiently secure. To sufficiently secure against brute-force attacks, the size of the key space must be more than 2^{128} .

2.4 Chaos-Based Random Number Generator

Having rigorously reviewed the related works, many researchers were observed to have applied various techniques for the design of random number generators. They have taken different processes, systems, and phenomena towards designing and analyzing RNG content, and have tried to find the unknown parameters. Any scheme for the generation of a number sequence which approximates the features of random numbers is a pseudorandom number generator (PRNG). These sequences are truly not random; although sequences hardware random number generators can be used to generate sequences of closer proximity to the truly random, pseudorandom numbers are practically important for simulation studies and are necessary for cryptography.

In a real random generator, the output has an equal number of ones and zeros. Several statistical characteristics which describe the keystream generated by a random source can be easily formulated. There are various test suites available in the literature which are designed for the evaluation of the randomness properties of finite sequences. The chaotic orbits which are generated by nonlinear systems are aperiodic, irregular, sensitive to initial conditions, and unpredictable. These features tally with the diffusion and confusion features in cryptography. In recent years, therefore, there have been studies on the chaotic system for security application in both analog and digital formats.

The PRNG in stream cipher is one of the vital components. Some chaotic system based-PRNGs have recently been suggested (Akhshani et al., 2014; François et al., 2014; Nian-sheng, 2011; Wang et al., 2012). Simple chaotic maps, such as logistic or tent map can be iterated to generate pseudorandom numbers with high speed. Although the one-dimensional chaotic systems have the advantages of being simple and highly efficient, they are still laden with some fundamental problems such as having weak security and small key space (Li et al., 2014). Most of the chaos based-PRNGs are directly obtained through a sampling of the chaotic map trajectory. In this way, there is an exposure of some of the chaotic map information which can lead to some loopholes (Murillo-Escobar et al., 2017).

Moreover, several methods for the prediction of chaotic time series have been proposed (Li et al., 2012; Maguire et al., 1998; Short, 1994, 1996; Lei Wang et al., 2014). The complex chaotic system should be considered ought to be considered to prevent attackers from predicting the series in an attempt to break the PRNG. The high-dimensional and spatiotemporal chaos has been used for the designing of PRNG (Hu et al., 2013; Li et al., 2006). This algorithm met the requirements of PRNG owing to its fully utilizing the traits of a complex system. However, there is a need for more computational studies on these schemes when generating pseudorandom numbers. Further studies on the difference between efficiency and security in PRNG are necessary.

For the enhancement of randomness, a nonlinear Digitalized Modified Logistic Map-based Pseudo Random Number Generator (DMLM-PRNG) has been suggested by (Chen et al., 2010). The computation cost was reduced using constant parameter selection and output sequence scrambling without altering the complexity of the output sequence. (Addabbo et al., 2007) and (Callegari et al., 2005) proposed the chaotic map-based PRNGs. (Savi., 2007) investigated the influence of randomness on the nonlinear dynamic behavior of coupled logistic maps having considered it as fluctuations and uncertainties due to noise. The noise effect was incorporated by the addition of the random variation to either the state variables or to the parameters.

A simultaneous encryption and compression algorithm of binary sequences has been proposed by (Wong and Yuen, 2008). This algorithm was formulated on a chaotic cryptosystem which depends on ID logistic map and initially designed for encryption. The proposed cryptosystem has a keyspace of about 130 bits equivalence. From the simulation result, the whole standard test files were shown to be reduced to a desired level, and the ciphertext was highly sensitive to minute alterations in the plaintext or the key. Compression capability was, therefore, achieved while security was ensured. Their scheme further ensured that the ciphertext and the plaintext are equal.

A robust chaotic map which is a modified logistic map that showed both a uniform distribution in 0, 1 and no chaotic window has been proposed by (Chang et al., 2009). They developed a multi-system hyper-chaotic synchronization system based on this map which is an asymptotic synchronization of the modified logistic hyper-chaotic system for secure communication. This system can asymptotically synchronize the transmitter and receiver in simplex partial coupling transmission after finite times. Furthermore, the

implicit driving technique ensured the asymptotical synchronization between the drive and response systems during the transmission of plaintext.

(Rani and Agarwal, 2009) suggested the enhancement of logistic map capabilities via superior iterations. There is a wide application of the logistic transformations $x_{n+1} = rx_n (1 - x_n)$ for choosing X_0 between 0 and 1 and $0 < r \leq 4$ in chaos, discrete dynamics and fractals. Logistic map stability can be investigated through computation. The logistic map is stable for $0 < r \leq 3.2$ in Picard orbit, but in higher orbits, there is a drastic increase in the range of logistic map stability; in some cases, the logistic map behavior even fades.

(Patidar et al., 2009) proposed a novel pseudorandom number bit generator (PRBG) which is based on two standards and 2 standard chaotic maps. The maps start from independent random initial conditions and are running side-by-side. They studied their schemes on the NIST and DIEHARD tests suite which are regarded as the most complex tests suites for testing randomness.

(Narendra K Pareek et al., 2010) presented a cross-coupled chaotic random bit generator (CCCBG) which generates random bits by comparing 2 cross-coupled linear chaotic map produced-orbits which are made up of two skew tent maps. The generator successfully satisfied the tested statistical packages like the poker test, frequency test, NIST, serial test, and autocorrelation.

(Wang et al., 2012) proposed a novel PRNG algorithm is known as couple map lattice based on discrete chaotic iteration (CMLDCI)). This algorithm combined the chaotic iteration and coupled map lattice (CML). They did several experiments such as NIST 800-22 statistical test suit, drew the auto-correlation and histogram figures, and used their proposed algorithm in the image encryption. They obtained pretty good results and demonstrate that this new PRNG is suitable for practice. The authors did not prove their algorithm can work in the form of Li-York chaotic map and use it in a parallel condition.

Pseudorandom numbers can be generated by implementing chaotic maps in circuits. Chaotic maps have been used in a circuit and the value of the initial seed comes from a random source (Nejati et al., 2012). The generator is, therefore, a real random number generator.

A trigonometric function-based chaotic dynamical system has been proposed by (Dăscălescu et al., 2013) which was intended to be used in cryptographic applications. With the aid of specific chaos theory tools such as a Lyapunov exponent, Kolmogorov-Smirnov test, and attractor's fractal dimension) and statistics (such as NIST suite of tests), they were able to prove the proposed scheme to have a chaotic behavior for large values of parameter space, and with acceptable statistical features. The proposed system was further used in together with the binary operation for the design of a new PRBG which was subjected to various statistical assessments in turns. Theoretical and practical arguments confirmed the viability of the proposed chaotic dynamical system and the novel PRBG. They were further recommended for cryptographic applications.

(Hu et al., 2013) proposed a binary sequence generator using a high-dimensional Chen chaotic system. They based their pseudorandom bit generator on a combination of 3 coordinates of the chaotic orbit. From the security and statistical analysis, it was verified that the system has good pseudorandom features and can reasonably withstand attacks.

A new PRNG which is based on the quantum chaotic map was proposed by (Akhshani et al., 2014). The system presented some good statistical outcomes such as ENT, NIST, TestU01 and DIEHARD. Meanwhile, the chaotic map was controlled by 3 difference equations with several arithmetic operations; it also requires a high computation power which usually results in low-speed PRNG generation. In the case of (Cicek et al., 2014), they employed generated pseudorandom numbers using the chaotic map but the input of the map was determined from a random source.

(François et al., 2014) proposed a PRNG algorithm which is based on the combination of 3 chaotic maps which were generated from an initial input vector. They tested the algorithm based on statistical and security analysis using such platforms as NIST, correlation, differential attack and key sensitivity. From their study, (Michael François et al., 2014) suggested a novel PRNG algorithm through a combination of 3 chaotic logistic maps using XOR and binary-64 floating-point arithmetic operation which at every iteration, generates a block of 32 random bits to increase the generator's throughput. The system satisfied the criteria of some statistical packages like NIST and correlation tests.

(García-Martínez and Campos-Cantón 2015) proposed a cryptographically secure PRNG known as CSPRNG which is based on k -modal maps, (a multimodal discrete systems) and a combination of its k -time series through XOR operation. These maps (multimodal) aided the generation of pseudorandom sequences which has longer periods of avoiding the issue of periodicity often presented in the logistic map. Statistical tests of the CSPRNG using NIST presented satisfactory outcomes; maps with $k \geq 2$ were cryptographically secure and lie within the confidence interval as according to the test suite. However, both correlation and speed analysis were hidden in the CSPRNG sequence.

Similarly, (Stoyanov and Kordov, 2015) presented a PRNG which is based on 2 Tinkerbell maps. The system was subjected to some security tests like keyspace, speed, key sensitivity, and correlation. Despite the successful outcome of the tests, the Tinkerbell map is a 2D system, and if the PRNG scheme employs 2 maps, each iteration will have 26 arithmetic operations which may reduce the processing speed in digital systems with limited hardware.

(Wang et al., 2016) suggested a piecewise logistic map (PLM)-based PRNG. The PLM is an improved logistic map. The authors subjected the system to efficiency and security tests using 15 tests of NIST suite to portray the performance criteria of a PRNG. However, about 18 arithmetic operations are needed to achieve an 8-bit number in the scheme.

(Abutaha et al., 2016) proposed a novel RNG which is based on a pseudo-chaotic number generator. The novel system employs 2 nonlinear recursive filters and operates on Linux random number generator. The outcome of the analysis on the bit rate, software security, and statistical properties showed that the new generator can confidently be employed for applications where random numbers are required.

A novel PRNG algorithm for secure and fast encryption has been proposed by (Murillo-Escobar et al., 2017). From their study, the pseudorandom features of the logistic map were improved by adding one multiplication and performing modular arithmetic (mod 1). They portrayed the benefits of their system by comparing its results to that of the classic logistic map at the histogram and Lyapunov exponents' level. The statistical tests using NIST 800-22 and TestU01 presented satisfactory results. From the

results of the security analysis, the system required few arithmetic operations and a high rate of output. The suggested PRNG–PELM scheme was stated to be suitable for implementation in secure encryption and embedded systems where there are limited hardware resources.

A novel way of obtaining pseudorandom numbers which are based on the discrete-space chaotic map has been proposed by (Lambic' and Nikolic', 2017). This method utilized a discrete chaotic map which is based on permutation composition. Statistical tests such as NIST 800-22 test was used to certify the randomness of the pseudo-random sequences which were generated by the proposed method. The method was insensitive to dynamical degradation and there was no effect of approximations on the process of the pseudo-random numbers generation. The ability of the proposed method to have an unlimited keyspace and being able to generate the same number of different pseudo-random sequences with a significantly lower memory space are the advantages of the system. the system can also achieve great cycle lengths and higher levels of security. Being able to utilize small memory endeared the proposed PRNG for application in devices with small memory space.

(Riaz et al., 2017) presented a new algorithm for the generation of pseudorandom numbers which was based on Duffing map. The focused on finding its potential application in engineering and science fields. For an effective practical application of this algorithm, the algorithm was tested on various statistical tests such as the initial seed value, CPU performance test, key sensitivity test, and pseudorandom orbit to test its strength. The proposed generator was subjected to further analysis and evaluation using NIST statistical test suite and the outcome of the tests proved that the new generator can be used successfully in applied physics, mathematical sciences, electrical engineering, and computer science.

2.5 Chaotic-Map Based Image Encryption

There are several applications of PRNGs such as in numerical analysis, secure communications, probabilistic algorithms, integrated circuit testing, cryptography, and computer games. The major criterion for distinguishing different PRNGs is the quality of randomness, but beside this criterion, other criteria are similarly important, such as the

cost of implementation and throughput. These factors are necessary for the evaluation of the effectiveness of the PRNGs for application in modern communications, video encryption, image encryption, and sensor networks.

In recent times, Chaos has been widely employed in cryptography, where chaotic maps are employed for image encryption. Image diffusion and confusion are expanded through the application of chaos. Owing to the benefits of nonlinear dynamical systems such as their pseudorandom behavior, unpredictability, sensitivity to initial conditions, and ergodicity, encryption based on chaos has been suggested as an efficient approach towards dealing with the issues of fast and highly secure image encryption. In this chapter, chaotic-based pseudo-random value generation and its comparisons were discussed. In image encryption schemes, a one-dimensional logistic map is usually employed due to low hardware complexities, easiness, and better pseudo-random number generation, and low computation cost.

Besides, the high implementation cost renders it an unsuitable pseudo-random number generator. Although it is preferred to use the logistic map for image encryption, there are still some issues with it such as blank windows, stable windows, uneven sequence distribution, and weak key. This research is suggesting hybrid chaotic maps for alleviating the earlier mentioned issues of chaotic maps. The maps were combined together for random values improvement.

The sharing of videos and digital images online has increased over the years due to the advancements in the field of internet technology and social networking services (SNS). However, unauthorized access and tampering with personal information have been a source of worry in recent times. Though these types of problems can be solved through information encryption, it is more appropriate to use the conventional encryption schemes like DES and AES for the encryption of multimedia information owing to the inherent characteristics of this form of information such as a high data correlation in the neighboring pixels, and the need for real-time transformation (Zhu et al., 2011). There is, therefore, a need for a novel encryption technique which can specifically address the demands of multimedia information. There have been significant developments in recent times in the area of image encryption technology which uses the chaos theory in conjunction with permutation–diffusion architecture.

Shannon was the first to introduce the idea of employing the permutation and diffusion theory for digital information protection (Shannon, 1949). Fridrich (1998) suggested a similar framework which employs 2D dynamic systems for image encryption, thereby, striking a balance between efficiency and security (Fridrich, 1998b). Figure 2.2 showed a typical framework that uses chaotic maps for image encryption. From the figure, all the pixels were permuted in the confusion stage. An exchange of the pixels at different locations was equivalent to the encryption of the (x_i, y_i) coordinate pair. These $N \times N$ pixels in the diffusion phase were regarded as a 1D sequence, and each pixel value was modified based on the chaotic sequence. A continuous repeat of these two operations results in changing the pixel vector set $\{\vec{p}\}$ substantially, and a completion of the encryption process.

Several algorithms for image encryption have been proposed; these algorithms are classified into two based on their means of generating pseudorandom numbers. These groups are chaos theory-based and non-chaos theory-based algorithms. The chaos-based encryption utilizes the similarity between cryptosystems and chaos dynamic systems such as their ergodicity, sensitivity to the initial conditions, and pseudorandom behavior. In this category, pseudorandom number sequences are generated using 1D high-dimensional or hybrid-chaotic systems to enable the construction of symmetric cryptosystems. On the other hand, non-chaos-based encryption the utilization of non-chaotic dynamic systems for the generation of pseudorandom number sequences for image encryption.

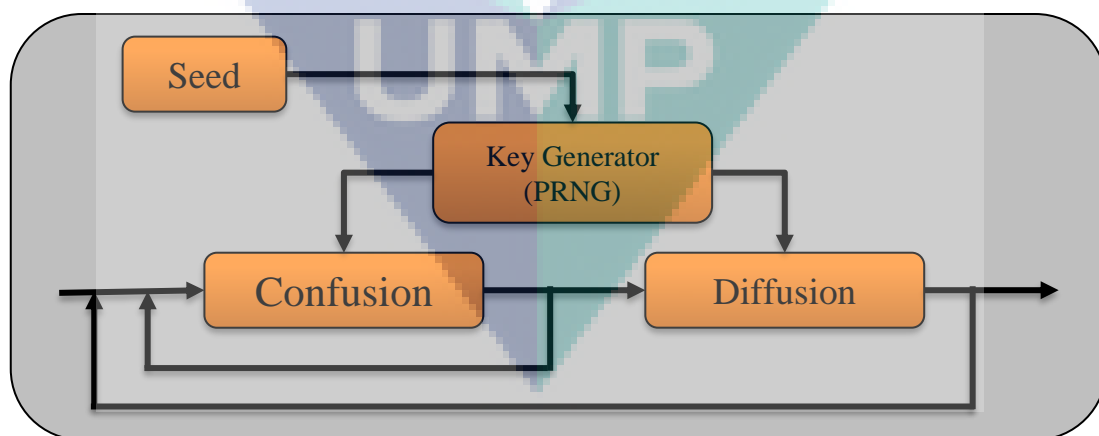


Figure 2.2 A classic image encryption architecture

There are two categories of the current chaos-based image encryption systems. A pixel is regarded in the first category as the least element while a digital image is considered as a collection of pixels. But the second category divided a pixel into several bits on which operations at bit level are performed. Figure 2.2 showed the classification of image encryption.

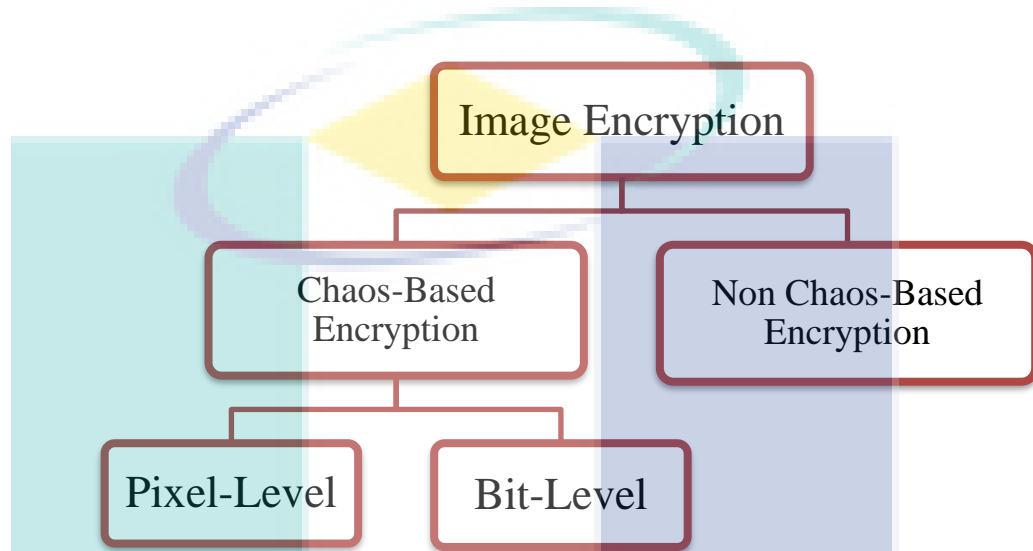


Figure 2.3 Classification of Image Encryption

Permutation algorithms can further be classified based on the algorithm itself. This is the method used for the calculation of the new location of each pixel after permutation. The two categories are the sorting-based permutation algorithms and those that base on 2D chaotic maps permutation. The sorting based permutation algorithms used a random number sequence to define the new position of each pixel post permutation (Murillo-Escobar et al., 2015; Wang, Teng, and Qin, 2012; Zhou et al., 2014). A calculation of one or more random sequences is generally made based on the pseudorandom systems and after that, the sequence is sorted. Based on this, a mapping rule is obtained pre and post sorting, and used on the permuting units which may be columns, rows, or pixels.

2.6 The Problems with Permutation Algorithms

In image encryption, the permutation algorithms play an important role which usually forms the basic framework of cryptosystems. There are two levels of permutation algorithms based on the movement of the pixels or bits after encryption. The algorithms for permutations at bit level redefine the fundamental bit composition of individual pixels and therefore, gives statistical information which is totally different on the pixel level. (Zhu et al., 2011) initiated the method of employing Bits Level Permutation (BLP) for encryption, in which the establishment of a relationship between the position of small particle bits and the pixel value is demonstrated. In this new method of permutation, pixel values are simultaneously encrypted with bit locations. (Zhu et al., 2011) independently permuted each of the plain image's eight-bit planes with 256 gray levels before recombining them to generate the cipher image. Meanwhile, the differences between the bit planes were neglected. For an algorithm for bit level permutation, two factors must be considered, which are the bit values and their weights. (Zhu et al., 2011) adopted an approach of restricting the scope for permutation at bit level to the same bit plane, indicating a modification of the bit location alone, instead of the weight. This suggests that irrespective of the difference in the macroscopic level after confusion, the statistical features for each bit plane was maintained.

(Zhang et al., 2013) compared a plain image with its consequent cipher image and revealed almost a similar distribution pattern of bits in the two images, with just about 3% difference in the bit values. The major thing is placing the right bit in the right position. Based on this, permutation at bit level is more important than the diffusion algorithm believed to have contributed significantly during image encryption. Bit-level permutation algorithms are designed to focus mainly on the elimination of all restriction during permutations at bit level by permitting a random movement of each bit in the plain-image within the same plain or any other bit plain of any color channel in the cipher image.

The sorting-based and 2D chaotic map-based permutation algorithms differ in their characteristics. The permuted image in the schemes for 2D chaotic map permutation may contain repeat patterns which are a result of the chaotic map-controlled mapping rule which may cause almost the whole pixels to move a similar distance in the same plane. These repeat patterns indicate the movement of the pixels in a regular pattern. These kind

of permutation algorithms are beneficial because they are time efficient in terms of implementation, but their disadvantage is that the cryptosystem offers security by relying on diffusion operation to an extent, while the permutation algorithm is a supplementary step for diffusion operation.

However, the sorting-based permutation algorithms present a different situation. They may follow one of two permutation methods; the first method is employing the basic permutation element as one column or row of pixels, where only a few numbers need to be sorted. For instance, an image of size $M \times N$ and two random sequences of size M and N respectively would require sorting; thus, the time needed to carry out this operation will be less. However, there will be an increase in the time needed for the sorting of the specific sequences when there is an increase in the numbers in the sequence. The disadvantage of the other method of permutation is that the basic permutation element is the bit or pixel which has the same length of the random sequence. The sorting of such a large sequence is not time-efficient. Table 2.1 presented a comparison of the different permutation algorithms.

Table 2.1 A comparison of the different permutation algorithms

Permutation Strategy	Permuted element	Advantages	Disadvantages
Sorting-Based	It sorts rows and column	It is a rapid method	The patterns are repeated
	The bits and pixel are sorted	There is a good permutation effect	There is a long execution time which is not acceptable
2D Chaotic Map Based	Pixel or Bit	It is a fast approach	The patterns are repeated

2.7 Related Works

The basis of stream encryption is the generation of an infinite cryptographic key stream which is used for the encryption of one or two bits or bytes at a time. The stream ciphers require a relatively low memory. Numerous algorithms for image permutations have been proposed. Many studies on colored image encryption algorithms based on chaotic maps can be found in the literature. This section presents the important related works in image encryption.

A chaotic logistic map-based image encryption approach for the purpose of meeting the demands for a secure image transfer has been presented by (Pareek et al., 2006). The proposed scheme adopts 2 chaotic logistic maps and a secret key (external) of 80-bit. The initial condition of the chaotic maps was generated by the provision of different weightage to all its bits using the external secret key. Furthermore, the scheme uses eight different operations for image pixel encryption and the particular operation for a particular pixel is selected based on the logistic map result. To increase the resistance of the cipher to attacks, there is an encryption of the secret key after the encryption of each block of 16 pixels of the image. The experimental, key sensitivity and statistical analyses presented the proposed to offer a secure and efficient image encryption for real-time transmission.

(Kwok and Tang, 2007) suggested a system for image encryption which has a stream cipher structure and is based on chaos. The system assumed a 32-bit precision representation with fixed-point arithmetic to facilitate hardware realization and achieve a fast throughput. The core of the image encryption system was a pseudo-random keystream generator which was based on a chaotic map cascade and served in the generation of sequences and random mixing. Contrary to the other current chaos-based PRNGs, the system did not just achieve a fast throughput, it equally satisfied the statistical tests of up-to-date test suite even under quantization. It was concluded from the experimental studies that the system performed better than the existing schemes in both security and speed. Due to the high throughput of the system, it was certified for application in fast and real-time encryption.

A new approach suggested for a secure and fast encryption of images has been suggested by (Sun et al., 2008). The system deployed high-dimensional chaos as the main

cryptographic structure. Some of the advantages of the system include the output the ciphered image having a high complexity, an effective byte confusion and diffusion in many directions in the variable space, and a long period of chaos realization. These advantages were attributed to the high-dimensionality and chaoticity of the system. These are beneficial features towards achieving high practical security. This report was the first attempt towards exploring the spatial chaos in a cryptosystem for direct digital image encryption and decryption.

(Mazloom and Eftekhari-Moghadam, 2009) proposed CNCM, a new chaos-based algorithm for image encryption which utilizes a Coupled Nonlinear Chaotic Map for color image encryption. To address the issues of weak security and small key space in the commonly used 1D logistic systems, this system uses a new nonlinear chaotic algorithm. The initial conditions and parameters of the map were generated using a 240 bit-long secret key through key algebraic transformation. The security of the cryptosystem was enhanced by these transformations and the CNCM coupling structure. The system was subjected to security analysis to prove that its key space was reasonably large to resist BFA. Experimental results with detailed numerical analysis have demonstrated the efficiency and high security of the scheme. From the presented findings, the scheme was concluded to perform better than the other encryption schemes and can be deployed for real-time transmission. Although this paper presented an algorithm which focused on image encryption, the study was not limited to this area as it can be widely deployed in other fields of information security.

(Lian, 2009) proposed an efficient scheme for image and video encryption which was constructed based on spatiotemporal chaos system. The scheme used the chaotic lattices to generate pseudorandom sequences for the individual encryption of the image blocks. An iteration of the chaotic maps for certain times resulted in sequences with a high initial sensitivity and good randomness. The direct current coefficient (DC) and the signs of the alternating current coefficients (ACs) were encrypted using the pseudorandom-bits in each lattice. The experimental results and theoretical analysis showed the scheme to have a good cryptographic and perceptual security which does not apparently influence the compression efficiency. These characteristics endeared the scheme for application in practical applications.

A novel chaos-based hybrid image encryption technique was presented by (Nien et al., 2009). The key space of images was increased by the proposed scheme; it also blurred the distribution features of RGB-level matrices, completely eradicated the outlines of the encrypted images, and effectively protects against decryption exhaustive attacks. Correlation coefficient studies were performed on the scheme to test the distribution of specialized variables for the encrypted image. A keyspace value of more than 10^{180} was achieved. The adopted examples showed the highly confidential encrypted images and demonstrated a potential application in the encryption of digital colored images.

(Zhu et al., 2010) presented an enhanced scheme for encryption that was based on logistic maps. This scheme presented a new method for the permutation of image pixel positions. A secret key is first used for the generation of 9 real chaos sequences by the logistic map; followed by the sorting of six chaotic sequences by the ordinal numbers that corresponds to the original sequences to generate new sequences. These new sequences are deployed for row and column position scrambling. At last, the remaining 3 chaotic sequences were employed for the value diffusion transformation of the image pixel. The simulation results and the performance analysis showed the scheme to have a large secret-key space, fast encryption speed, high security, and strong robustness. The scheme achieved a multi-chaos encryption effect using only a logistic map.

(Yu et al., 2010) presented a chaos-based image encryption system. As a whole image is encrypted, the efficiency of the process is difficult to be improved. The proposed scheme uses wavelet decomposition to concentrate the main image information to the areas with a low frequency before applying a high-strength chaotic encryption. After the high-speed encryption, diffusion will be performed through wavelet reconstruction and Arnold scrambling. Finally, the encryption process will be completed through another set of wavelet decomposition. Experimental findings and theoretical analysis showed the proposed scheme to have a high efficiency, satisfied security, large key-space, and suits for image data transmission.

(Liu et al., 2011) proposed a scheme for color image encryption based on bit-level permutation and high-dimension chaotic map. The plain color images of size $(M \times N)$ are first converted to a grayscale image of size $(M \times 3N)$ before its transformation into a binary matrix and permuted at bit-level using the scrambling map generated by piecewise

linear chaotic map (PWLCM). Furthermore, the red, green and blue components are simultaneously confused and diffused using a Chen system. The scheme was confirmed through experimental reports and security analysis to have a good encryption performance, and also had a key space which was reasonably large to resist common attacks.

(Lili Liu et al., 2012) presented an RGB image encryption scheme based on DNA encoding and chaotic map. The scheme first performs DNA encoding for the R, G, B components of the RGB image; then, realizes the addition of R, G, B by DNA addition and carries out complement operation by using the DNA sequence matrix controlled by logistic. After the decoding, three gray images are obtained; finally, the encrypted RGB images is achieved by reconstructing the R, G, B components which use image pixels disturbed by logistic chaotic sequence. From the simulation result, it was shown that the proposed scheme achieved a large secret keyspace as well as a strong secret key sensitivity. The system can also resist exhaustive and statistical attacks, and thus, was suitable for the encryption of RGB images.

(Zhou, Bao, et al., 2014) proposed an algorithm with a 4-round encryption structure, and each round comprises of five steps which are the insertion of the random pixel, separation of the rows, 1D substitution, combination of the rows, and rotation of the image. First, a random pixel is inserted at the beginning of each row of the original image; then, each row is separated into 1D data matrix before applying a substitution process to alter the data values in each 1D matrix. All the 1D matrices are combined back into a 2D data matrix based on their row positions in the original image before being rotated 90 degrees in an anticlockwise direction. The final encrypted image is achieved by repeating the process 4 times. The algorithm was certified through experimental and security analysis to have excellent image encryption performance and can resist various attacks.

A novel hybrid system which consists of a permutation-substitution network that is based on chaotic systems and Latin square encryption strategies has been proposed by (Machkour et al., 2015). This scheme has good confusion and diffusion properties and robustness to noise integration in decryption due to the homogeneity between the two systems. Security analysis presented the scheme as secure enough to withstand brute-

force attack, chosen plaintext attack, differential attack, statistical attack, and known-plaintext attack.

A proficient method for image encryption was presented by (Rathore and Suryavanshi, 2016) who used the logistic map for the generation of the pseudo-random sequence used in the cryptosystem. They scrambled the image pixel positions using Arnold cat map before using the chaotic map to generate the pseudorandom key. Similarly, (Li et al., 2016) presented a novel scheme for image encryption which is based on hybrid cellular automata (CA) and depth-conversion integral imaging. This scheme has better performances in trying to meet the criteria for secure image transmission.

(Sharif et al., 2016) a novel approach for image encryption based on mixing chaotic maps is proposed. Two secret keys which are entitled “CK”, “AK”, used to make their scheme highly dependent on the image. Indeed, if these values changed slightly, the result will be changed completely. In diffusion phase, a combination of two high-level chaotic maps that are “Logistic-sinus” and “Power-Logistic” used to build a chaotic matrix, which is possessed better chaotic behavior. Finally, in permutation phase, produced an index of two newfound high-level chaotic maps are used to modify pixel positions. The proposed diffusion phase provides desirable uniform distribution in color histogram of the encrypted image and increases the robustness of the scheme against statistical attacks. Furthermore, an acceptable result in the average of NPCR (99.68), UACI (33.50), and brute force attack resistance was achieved by creating secret with high sensitivity to the original image. The scheme was confirmed by experimental results to have the features of a secure encryption scheme such as high security, large keyspace, and high sensitivity.

(Huang and Yang, 2017a) proposed a new color image encryption method based on the Logistic mapping and double random-phase encoding. At first, the scheme uses Logistic mapping for color image diffusion, then, the red, green and blue aspects of the result are scrambled through the replacement matrices that are generated using Logistic mapping. Secondly, the scheme encrypts the three scrambled images into one encrypted image using a double random-phase encoding. Experiment results showed the scheme to not only achieve good results but also had a key space which was reasonably large to resist common attacks.

A scheme for image encryption based on chaotic system and DNA sequence operations were proposed by (Chai et al., 2017). At first, the plain image is encoded into a DNA matrix, and then, a new wave-based permutation scheme is performed on it. The chaotic sequences produced by 2D Logistic chaotic map are employed for row circular permutation (RCP) and column circular permutation (CCP). The SHA 256 hash of the plain image and the obtained values are used to calculate the initial values and parameters of the chaotic system. Then, a row-by-row image diffusion method at DNA level was applied. A key matrix generated from the chaotic map is used to fuse the confused DNA matrix; also the initial values and system parameters of the chaotic system were renewed by the hamming distance of the plain image. Finally, after decoding the diffused DNA matrix, the cipher image obtained. The DNA encoding/decoding rules of the plain image and the key matrix were determined by the plain image. Experimental results and security analyses both confirmed that the proposed algorithm has not only an excellent encryption result but also resists various typical attacks.

A hyper chaos-based algorithm for image encryption which uses pixel-level and bit-level permutation has been proposed by (Li et al., 2017). The scheme first resists general methods that can decipher low dimensional chaotic maps using a hyper-chaotic system. The chaotic sequence which has been generated by the chaotic system is important to the features of the plain-image. Different plain-images could, therefore, have completely different chaotic sequences. The selected plaintext and ciphertext attacks are void. Then, a pixel-level permutation is employed. Next, a bit-level permutation was used to scramble the image. A combination of pixel-level and bit-level permutation can strengthen the system security. Finally, pixels were added after pixel-level permutation in diffusion operation. Compared to the most related hyper-chaos based image encryption algorithms, the proposed algorithm was safer because of using a pixel-level permutation, bit-level permutation, and more complex chaotic system. The scheme was confirmed through experimental results and simulation studies to have not only performed well but also resisted different attacks.

Multiple-image encryption (MIE) algorithm based on the mixed image element and permutation proposed has been proposed by (Zhang et al., 2017). The contributions of the proposed algorithm were to improve the encryption efficiency. To achieve this aim, this work presents a new MIE algorithm based on the mixed image element and

permutation. In this study, the conceptions of pure and mixed image elements were defined. Furthermore, a method for the generation of a permutation and chaotic image with the chaotic system was offered in this study. This work also introduced two similar algorithms and makes comparative analyses of the two algorithms. To verify the feasibility of the new algorithm, several experiments were performed in this study. The experimental results showed that the proposed algorithm was efficient and secure.

The most related works have been reviewed but for convenience, most of relevant methods or techniques which have been reviewed, their levels, category, and weaknesses are highlighted in Table 2.2.

The logo of UMP (Universitas Muhammadiyah Palembang) is a large, stylized shield-like shape. It is composed of several geometric sections in shades of teal, light blue, and yellow. The letters 'UMP' are prominently displayed in white, bold, sans-serif font across the lower-middle part of the shield.

UMP

Table 2.2 Advantages and disadvantages of the most related works

No.	Ref	Algorithm	Chaotic Maps	Category	Level	Comments
1	(Z. Zhu et al., 2011)	8-bit planes are independently permuted and controlled by 8 Cat maps. A combination of the eight permuted bit planes gives the cipher image.	Logistic Map, Arnold Cat Map	2D chaotic map	Bit	It is not possible to change the bit weight and the position of the target bit is restricted to the original bit plane
2	(W. Zhang et al., 2013b)	The permuting plane is expanded with each 2-bit pixel; it is controlled by a Cat map	Cat Map	2D chaotic map	Bit	Some of the issues of bit permutation were resolved. Bits can select from either even or odd bit plane as its target.
3	(X. Wang et al., 2012)	The permutation of the image rows and column require sorting of two random sequences.	Logistic Map	Sorting based	Pixel	There is a simultaneous permutation of 3 color channels; after each permutation, the statistical information remains the same.
4	(Zhou, Cao, et al., 2014)	All the image bits are arranged into a one-bit sequence; to govern the process, a random sequence of similar size is sorted.	Logistic Map	Sorting based	Bit	The sequence size and the number of bits in the plain-image are the same. The searching and sorting operations are time-wasting.
5	(Murillo-Escobar et al., 2015)	Two parts of one random sequence are sorted to govern the row and column permutations	Logistic Map	Sorting based	Pixel	The algorithm for the modification of the pixel value is executed in a float point domain and this is not time efficient.

Table 2.2 Advantages and disadvantages of the most related works

No.	Ref	Algorithm	Chaotic Maps	Category	Level	Comments
6	(Hua et al., 2015)	The random sequence after sorting is generated using a new coupled chaotic map; the permutation operation is governed by shifting the position of the group pixel.	Sine Map Logistic maps	Sorting based 2D chaotic map	Pixel	There must be a sorting of a sequence of equal length with the pixel number and this is time-consuming.
7	(W. Zhang et al., 2013b)	Used both Cat map and group bit shift algorithms	Cat Map	2D chaotic map	Bit	The permuted image has some repeated patterns.
8	(Y.-Q. Zhang and Wang, 2014)	The permutation process is controlled by a reverse 2D chaotic map.	Mixed linear-nonlinear coupled map lattices	2D chaotic map	Pixel	It uses a pixel level cipher with no consideration of the bit features.
9	(L. Y. Zhang et al., 2014)	It uses a logistic map-derived one-random sequence. The permutation is defined with a feedback mechanism using its sorted sequence.	Logistic Map	Sorting based	Pixel	Simultaneous modification of the pixel values is not considered. It encrypts only pixel positions.
10	(H. Liu and Wang, 2011)	The row and column permutations are governed by a WLCM system at bit level	Piecewise linear chaotic map	Sorting based	Bit	The algorithm is time-consuming

Table 2.2 Advantages and disadvantages of the most related works

No.	Ref	Algorithm	Chaotic Maps	Category	Level	Comments
11	(S. Wang et al., 2013)	A scrambling and diffusion method is used, with its control parameters generated by Logistic and Kent mapping.	Logistic Map Kent Map	Sorting based	Pixel	The total key space is large, but each stage (scrambling and diffusion) has small key space due to the use of the 1D chaotic map for each stage.
12	(Li, et. al., 2017)	chaotic keys stream for image encryption is generated by the modification of the chaotic tent map. A 1-D chaotic tent map generates the chaos-based keystream.	Tent Map	Sorting based	Pixel	The key space of the proposed algorithm was equal to 2^{106} . Cipher or PRNG must have more than 2^{128} different secret keys in order to resist brute-force attack(ECRYPT, 2011a).
13	(Huang and Yang, 2017b)	A system for the encryption of colored images using Logistic mapping and phase encoding. Uses logistic mapping to diffuse the colored image before scrambling and encoding the RGB components using Logistic mapping and double random-phase encoding.	Logistic Map	Sorting based	Pixel	The first stage implements 1D chaotic map for permuting the pixels, which may lead to the generation of weak sequences.
14	(Y. Li et al., 2017)	First, pixel level is implemented by generating a chaotic sequence for permuting the plain image. Then a bit-level permutation is implemented to scramble the image. Finally, in diffusion operation, some pixels added after pixel-level permutation.	Hyper-Chaotic map	Sorting based	Pixel & Bit	Combing the pixel level, and bit level, with sorting based strategy, takes much execution time. Also, the difficulty of the hardware/software implementation and computation complexity is increased by this multiple chaotic maps.

Table 2.2 Advantages and disadvantages of the most related works

No.	Ref	Algorithm	Chaotic Maps	Category	Level	Comments
15	(Xiaoqiang Zhang and Wang, 2017)	The algorithm is fast and attained good security results	Piecewise linear chaotic map	Sorting based	Pixel	<ul style="list-style-type: none"> • Due to the segmentation of many images, the algorithm has a very complex structure. • The algorithm works perfectly for encrypting multiple images, thus, encrypting a single image may lead to weak encryption results.

2.8 Standard Chaotic Maps

2.8.1 Logistic Map

Chaotic map is a new concept in modern science and an ideal preference for researchers in that it encompasses operational simplicity, high speed, and sensitive to initial conditions, parameters of control, stability and ergodicity, all of the necessary features required in security systems design.

The logistic map had been built on a single component which was represented by a specific mathematical formula to verify the utilization of biological populations, PRNG and cryptographic applications. Furthermore, the mathematical simplicity provided by the logistic map makes it an invaluable method for testing new concepts in chaos theory as well as data security. The simplified mathematical formula is:

$$X_{i+1} = \mu X_i (1 - X_i), \quad 2.1$$

Where $X_i \in (0, 1)$ signifies the distinct state, retaining the initial condition $X_0 \in (0, 1)$, while $\mu \in (3.999, 4)$ represents the control parameter and $i \geq 0$, is the number of iterations. To prevent digital downgrade and short period cycles, a 64-bit floating-point that influenced 10-15 decimals had been employed.

Figure 2.4 shows the different characteristics for the values of the horizontal axis shows the values of the parameter μ , and the vertical axis shows the possible long-term values of X_n .

The Lyapunov exponent is a numerical method that identifies chaos and orbital deviation once it has obtained a positive value, which is significant in substantiating the chaotic orbit in a logistic map. For fraction $x_{n+1} = f(x_n)$, its Lyapunov exponent λ is defined as:

$$\lambda = \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |f'(x_n)| \quad 2.2$$

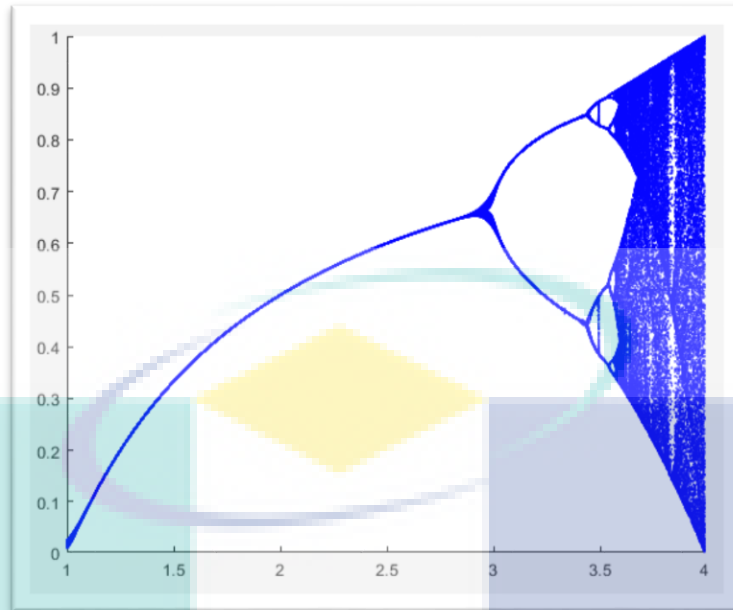


Figure 2.4 Bifurcation of the logistic map

The behavior of the chaotic function had been measured quantitatively and was given a positive value (i.e., $\lambda > 0$) by the Lyapunov exponent that had been calculated through the quantitative process with the exemption that the system control parameter was changed from 3.5 to 4, with step 0.01, as shown in the Lyapunov exponent in figure 2-5. It is calculated by using quantitative process with system. Figure 2.5 shows Lyapunov distribution for logistic map.

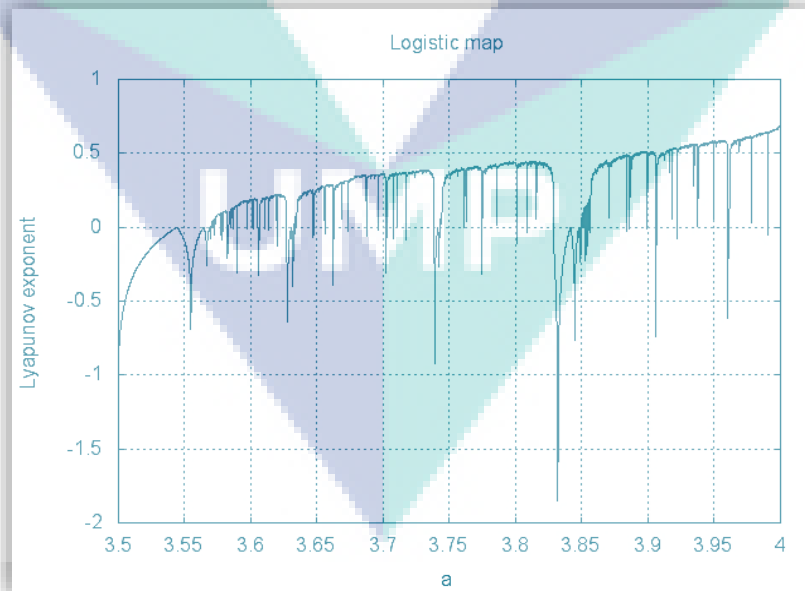


Figure 2.5 The logistic map Lyapunov exponent

2.8.2 The Tent Map

The Tent map is ergodic and the definition interval has unvarying invariant density function(Tommaso Addabbo et al., 2006). It's considered to be the simplest one-dimensional chaotic map, and defined as:

$$Y_{i+1} = \begin{cases} \omega Y_i & \text{if } Y_i < 0.5 \\ \omega(1 - Y_i) & \text{otherwise,} \end{cases} \quad (2.3)$$

where $Y_i \in [0, 1]$, $i \geq 0$, represents the system parameter. This map turns an interval $[0, 1]$ against itself and includes only one control parameter ω , where $\omega \in [0, 2]$. The group of actual values Y_0, Y_1, \dots, Y_n compose the system orbit, where Y_0 is the initial value, and an orbit can be obtained for every Y_i . According to the control parameter ω , various dynamical performances ranging from predictable to chaotic as shown in equation 2.3.

When the Lyapunov exponents in the interval $[1, 2]$ are positive, which indicates that the system is chaotic and the signal is acceptable in terms of traversal of the state, certainty and mixing. Figure 2.6 shows the general shape of Lyapunov exponents for tent map.

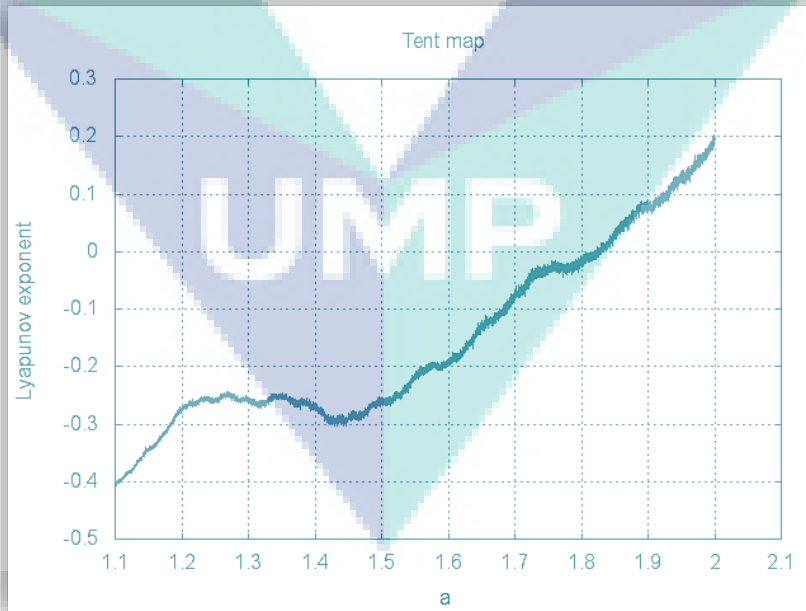


Figure 2.6 The tent map Lyapunov exponent

The generated chaotic sequence by this map are tended to hold a decent statistical asset. Moreover, they have a habit of convinced periodicity under finite precession. The value of ω is categorized into two scenarios as follow:

- When ω value becomes bigger, the sequences show robust randomness
- When ω value becomes smaller, periodicity appears on sequences behaviour.

A bifurcation diagram shows the value of the changing parameter and can be seen in Figure 2.7. Figure 2.7 shows the different characteristics for the values of the horizontal axis shows the values of the parameter ω , and the vertical axis shows the possible long-term values of X_n .

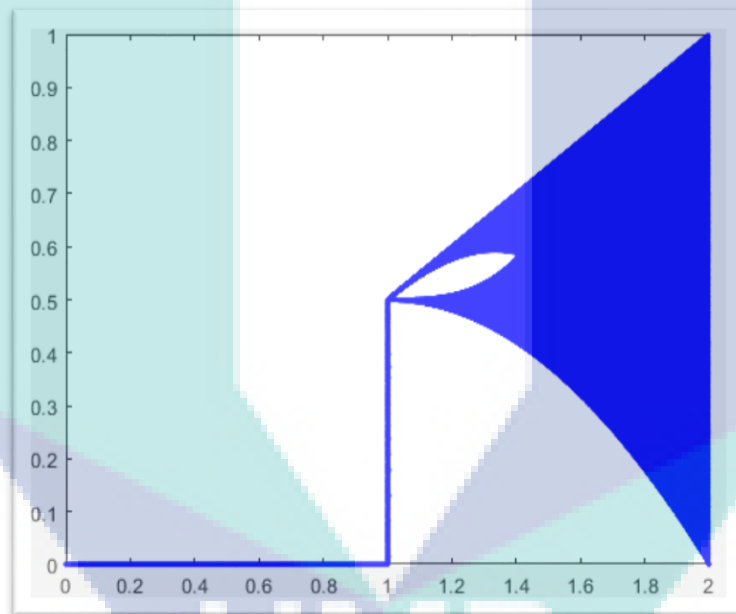


Figure 2.7 Bifurcation of Tent map

2.9 The NIST Statistical Test Suite

2.9.1 The NIST Test Suit

This is a set of statistical tests comprising of 16 tests which were developed for the testing of the randomness of long binary sequences generated either by a cryptographic pseudo or random number generator that is software or hardware-based. The focus of the tests is on the various forms of non-randomness which can be found in binary sequences. These set of tests are further grouped into parameterized and non-parameterized tests.

A) The Non-Parameterized Tests

The frequency or monobit test: The frequency or monobit test is mainly on the zeros and ones proportion within the whole sequence. It ascertains that the zeros to ones ratio in a particular sequence is approximately as expected of a real randomized sequence. It also checks the fraction of the ones proximity to $\frac{1}{2}$; indicating that the number of the zeros and ones ought to be the same in a sequence.

The runs test: This test focus mainly on the runs number of a given sequence; a run been the continuous sequence of similar bits. A run with K length exactly has k number of identical bits, which is bordered before and after by a bit that has the opposite value. The test ascertains that the run number of the zeros and ones with different lengths corresponds to the numbers expected of a given randomized sequence. The test particularly ascertains the speed of the oscillations between the zeros and the ones.

The test for the longest run of ones in a block: The test concentrates on the ones' longest run in M-bit blocks. It ascertains that in a sequence been tested, the length of the ones' longest run is the same with that of the longest run expected of a real randomized sequence.

The Lempel-Ziv compression test: The Lempel-Ziv compression test centers on the cumulative number of varying patterns within a sequence. It determines the extent a sequence under test can be compressed. A sequence that can be significantly compressed

is regarded as non-significant. There is a distinctive number of patterns for every random sequence.

The binary matrix rank test: This binary matrix rank test measures the disjoint sub-matrix ranks of the entire sequence. It checks for the linear dependence among the original sequence's fixed length substrings.

The cumulative sums test: The cumulative sums test focuses on the random walks' optimal excursion from zero. It is the sum of the sequence' adjusted -1, +1 digits. The test determines if the partial sum of sequence in a sequence being tested is too small or too large when related to the behavior expected of the cumulative sum of randomized sequences. The cumulative sum can be regarded as a random walk. The excursions of a random walk in a random sequence should not be zero.

The Discrete Fourier Transform Test (DFTT): This is a test on the height of the peaks in the DFT of the sequence. Its purpose is the detection of the periodic characteristics such as the repetitive proximity of peak patterns in a tested sequence to each other. This would signify the presence of a deviation from randomness.

The random excursion test: The random excursion test mainly tests the number of cycles in a cumulative sum random walk which has K number of visits. The cumulative sum random walk is a product of the partial sums after the transfer of the 0, 1 sequence to the appropriate -1, +1 forms. A random walk cycle is made up of a series of unit length steps which were randomly taken, beginning and ending at the origin. The test aims to determine whether the number of visits to a given state in a cycle is different from what is expected of a randomized sequence.

The random excursion variant test: This test focus on the total number of visits to a given state within a cumulative random walk. It establishes the deviances from expected number of visits in a randomized walk.

B) The Parameterized Tests

The frequency tests within a block: The frequency test within a block tests the proportion of the ones in M-bit of a sequence. It determines if the frequency of the ones

is nearly $M/2$ in M -bit as expected in a state of randomness. For a block of M size = 1, the frequency test will be degenerated to the monobit test.

The approximate entropy test: The approximate entropy test centers on the possible M -bit overlapping patterns across the whole sequence. It compares the overlapping frequency of two adjacent or consecutive block lengths against the results expected from a randomized sequence.

The linear complexity test: The linear complexity test checks the linear feedback length shift register of the sequence. It determines the level of complexity of a sequence to be regarded as a random sequence. A randomized sequence has longer linear feedback length shift register.

The Maurer's universal test: The Maurer's universal test checks the bit number between matching patterns. It relates to the compressed sequence's length. Its main aim is to ascertain the capability of a sequence to be compressed without losing any useful information. A sequence that can be significantly compressed is regarded as non-randomized.

The serial test: The major interest of the serial test is on the number of all the possible overlapping M -bit patterns across the sequence. It determines whether the number of overlapping pattern of 2^m M -bit is approximately as expected of a real randomized sequence. The randomized sequences are uniform, meaning that there is an equal chance of occurrence for each M -bit pattern as every other M -bit patterns. It is worthy to note that for $M = 1$, the serial test is the same as the frequency test.

The nonoverlapping template matching test: This one focus on the frequency of occurrence of target strings that are already specified. It detects the generators that are producing so many occurrences of a particular aperiodic pattern. It employs an M -bit window to search for a particular M -bit pattern for the non-overlapping and overlapping template matching tests. Should the pattern not be found, the window slides on bit position, but when found, the window resets to the bit of the found pattern and continues the search.

The overlapping template matching test: The overlapping template matching test focus on the frequency of the occurrence of pre-specified string targets. The overlapping

and non-overlapping template matching tests employs an m-bit when searching for a particular bit pattern. The difference between them is that in a situation where a pattern is found, the overlapping template test slides only one bit and resumes the search.

These above-mentioned tests are further described in detail in the referenced NIST document (Soto, 1999).

2.10 Summary

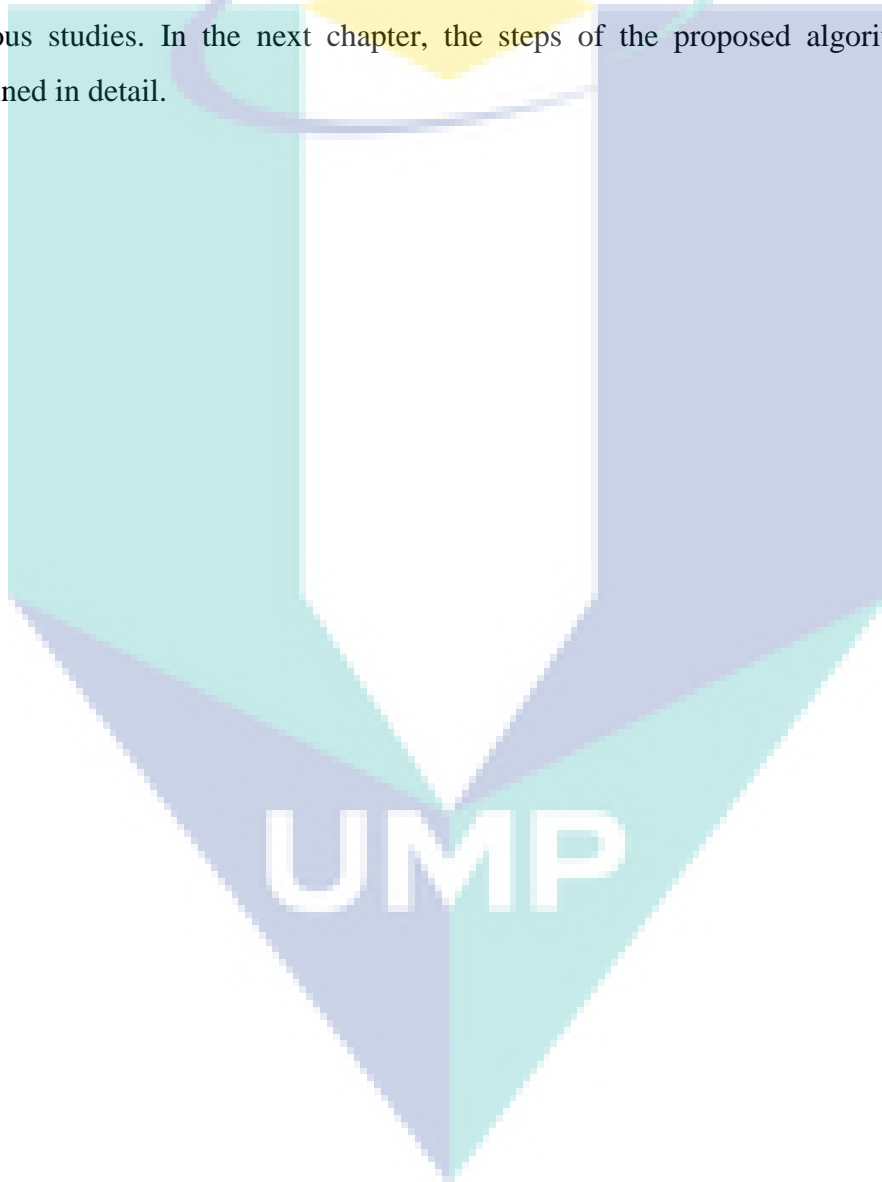
This chapter described in detail the concept of data encryption in general, and the concept of image encryption in particular. Also, it addressed the definition of the science of encryption and most of the important aspects in the field of image encryption based on Chaotic Map method. It also explained how these methods can be used to generate keys also called pseudorandom number generator (PRNG), which are used for data encryption.

Through the revision of the previous works which relates to the subject of images encryption based on Chaos theory, we reviewed many of the problems faced by the researchers, and most importantly, the drawbacks of using one-dimensional chaotic methods which can lead to weak encryption and keys generating processes. At the same time, relying on the chaotic method with more than one dimension was found to make the design or implementing the system difficult, and it often leads to time-consuming. Further, these studies have described the importance of image encryption for the protection of the user's important information when transferring them through networks. This topic has attracted the attention of many researchers and is considered one of the most discussed topics in the past 30 years.

On the other hand, a huge number of researches in the past ten years were conducted to study the design of color-coding algorithms based on chaotic methods, which was the focus of this chapter. The revision of these studies has led us to important conclusions: secure color image encryption can be achieved by using more than one chaotic map which works simultaneously as one-dimensional to take advantage of its fast and easy implementation character; while at the same time making the system easy to be implemented. This algorithm has a unique structure which has not been covered by the rest of the reviewed researches. As for the encryption algorithm, it is also a new algorithm of Hash Permutation algorithms. This algorithm is based on the principle of Fridrich

which was proposed in 1997 and it is expected to improve the confusion and diffusion processes. This is due to its dependency on the separation of the three basic color images (red - green - blue) and processing of each color separately in terms of confusion and diffusion before eventually merging the resulting images into one encrypted image.

The process of testing the proposed method as described in Chapter 4 was done through a set of statistical and security tests to prove its ability to protect the important information available in the images, as well as to compare it with the performance of previous studies. In the next chapter, the steps of the proposed algorithms will be explained in detail.



CHAPTER 3

METHODOLOGY

3.1 Introduction

Chaos has widely been used in cryptography in recent years. Chaotic maps are often used in encrypting images. Chaos is applied to expand the diffusion and confusion in the image. Due to the desirable properties of nonlinear dynamical systems, such as pseudorandom behavior, sensitivity to initial conditions, unpredictability and ergodicity, chaos-based encryption is suggested as a new and efficient way, to deal with the intractable problem of fast and highly secure image encryption.

A mammoth number of image encryption schemes have been proposed in the literature, and the key is generated by using various maps and methods. Most of the schemes are linear in nature, have a weak key (i.e., less randomness and can be predicted), equivalent key, less sensitivity in key and cipher image, high computation cost, low security and fail to withstand attacks and low speed. Thus, the proposed schemes attempted to alleviate the aforementioned problems and new pseudorandom number generator is designed to generate secret keys for encrypting the images.

This chapter explains the proposed image encryption in details, and it is divided into four parts. The first part explains the research methodology which has been followed in order to design the proposed algorithm. In the second part, the original logistic map, tent map, and the proposed pseudorandom number generator is explained in details. The third part explains the proposed encryption and decryption algorithm for colored images. Finally, the last part explains the main evaluation metrics for evaluating the proposed algorithms.

3.2 Proposed Image Encryption System

In this section, an image encryption algorithm is proposed based on the encryption method proposed by Fridrich (Huang and Yang, 2017b; Kanso and Ghebleh, 2012). The main reason behind proposing a new PRNG is the need for generating random key sequences with big key space. In other words, it is necessary to improve the pseudo random properties generated from the proposed hybrid chaotic to achieve better security in a cryptosystem. The proposed algorithm consists of three main stages- initialization and information extraction, PRNG, and encryption algorithm. Figure 3.1 shows the general block diagram of the proposed system.

Stage 1: Initialization and Information Extraction:

In this stage, all the parameters used in the system are initialized and the information is extracted from the original image. In other words, all the three colors (i.e. RGB channels) are extracted and kept in three matrices. Those matrices and parameters are used for the next two stages.

Stage 2: Pseudo-Random Number Generator (PRNG):

In this stage, three key sequences are generated using the proposed PRNG structure. Each key sequence is utilized for a single color, in other words, each key sequence is used for the confusion and the diffusion algorithms for single color only. The reason for using three key sequences instead of a single key sequence for all the colors is to increase the level of security of the algorithm. In addition, three key sequences can decrease the probability of generating repeated patterns and this is an issue faced by the encryption algorithms (explained in detail in Section 2.6).

Stage 3: Image Encryption Algorithm:

In this stage, the proposed enhancement to the encryption algorithm is given. As earlier above, the main structure of the encryption algorithm is called 'Fridrich Structure', consisting of three main stages - key generator, confusion, and diffusion stages. The output of the last two stages (i.e. three matrices and generated key sequences) are fed into this stage. The resulting matrices of this stage are combined for the generation of the final ciphered image.

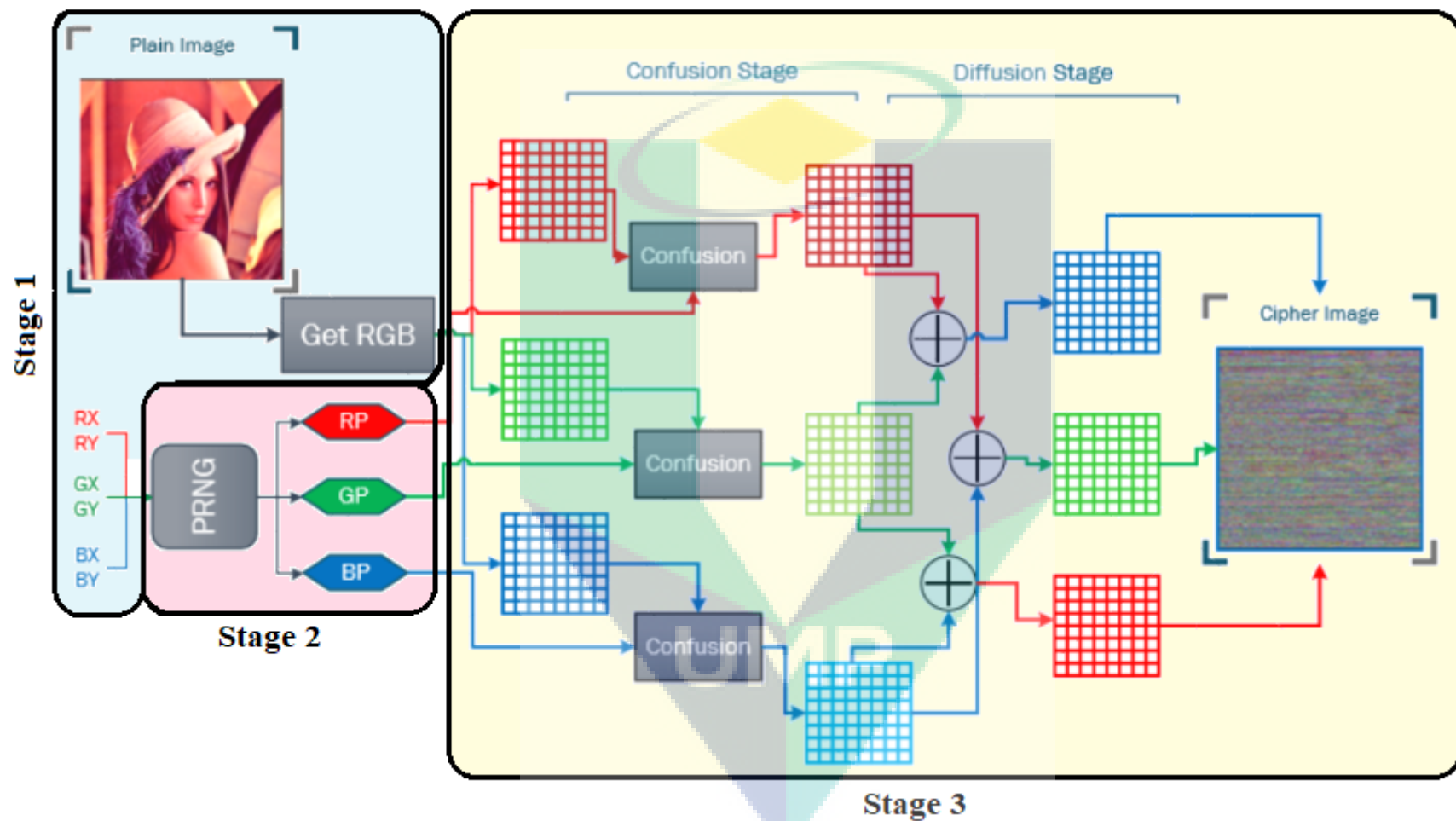


Figure 3.1 The block diagram of the proposed system

3.3 The proposed PRNG Algorithm

This section explains the proposed PRNG structure for generating a pseudo-random number, which is used for generating random keys. The proposed algorithm is called “LT-PRNG”, stands for (Logistic-Tent Pseudo Random Number Generator). The general block diagram of LT-PRNG is given in Figure 3.2. The structure consists of three main stages, initialization stage, chaotic number generator, and XOR processes Stage. The main reason behind designing a hybrid of two chaotic maps is to increase the number of input values to PRNG. In other words, there are four inputs (i.e., two initial values and two control parameters) used in the proposed PRNG rather than only two input values, which enhance the randomness of the key, and increase the key space.

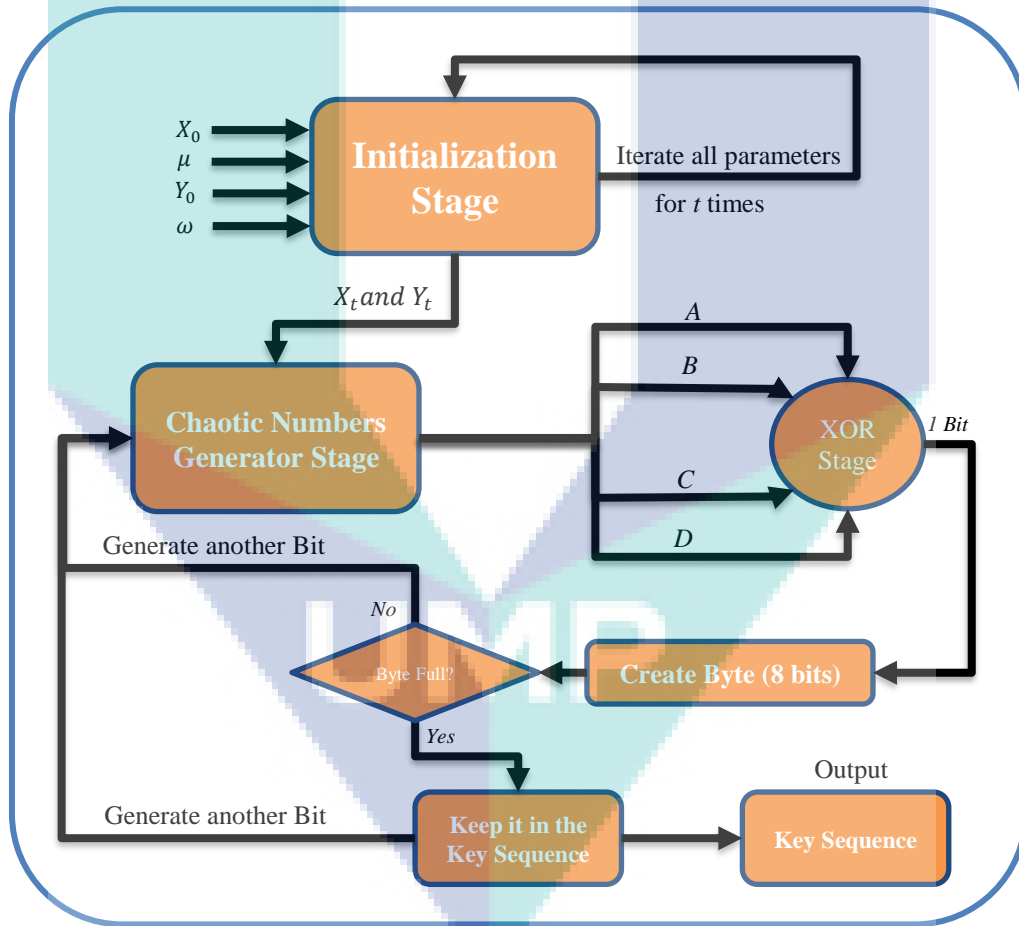


Figure 3.2 Block diagram of LT-PRNG

In Figure 3.2, there are three main stages; initialization, chaotic numbers generating and XOR processes which work together to generate the key sequences. For each main stage, there are several inputs, such as X_0 , Y_0 , μ , and ω which represent the main input values for the proposed PRNG. While A , B , C , and D represent the output

bytes from the second stages, and the input values to the XOR stage. These stages described as follow:

Stage 1: Initialization

1. Input initial values for logistic map X_0 in the range $[0,1]$, and $\mu = 3.99999988$.
2. Input initial values for tent map Y_0 in the range $[0,1]$, and $\omega = 1.99999988$.
3. Iterate both chaotic maps for t times.
4. The output X_t and Y_t will be the input value to next stage.

Stage 2: Chaotic numbers generator

This stage contains two phases of chaotic systems the first phase, is composed of logistic map (LM) and tent map (TM) to generate a sequence which will be used as an initial for each iteration between the phases. In second phase, two new chaotic maps referred as tent map to logistic map (TLM) and logistic map to tent map (LTM) are utilized and iterated by values generated by the first phase. Figure 3.3 shows the main flowchart of this stage.

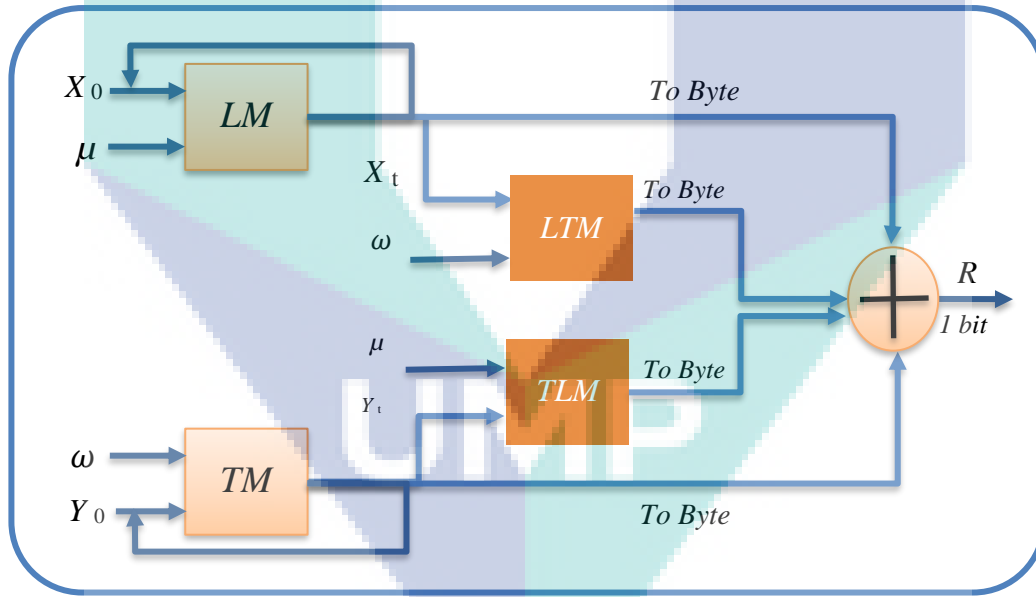


Figure 3.3 Chaotic numbers generator

The LTM and TLM chaotic maps enhanced the designed PRNG by generating two more outputs. Moreover, the design does not require any additional input or control parameters, only for the first logistic and tent map. This modification leads to better randomization without increasing the complexity of the structure.

LTM used the initial value from Logistic map (1st phase) according to Eq. 2.3 While, TLM is fed with the initial value from the tent map (1st phase) using Eq. 2.1. (Figure 3.6). This stage works as follows:

1. Initialize both chaotic maps (1st phase) with the last X_t and Y_t , which have been produced by stage 1.
2. Initialize both new chaotic maps (2nd phase) with the last X_t and Y_t , which have been produced by stage 1.
3. Generate the output by iterating both phases which referred as A, B, C, D.
4. Convert the generated numbers into bytes in the range [0,255], by applying the equation (3.1). Then, each byte will be fed into the next stage.

$$Byte(A) = Round (A \times 255) \quad 3.1$$

Stage 3: XOR process

The resulted output from the previous stage contains four outputs that were generated by the four chaotic maps (LM, LTM, TLM, and TM). Each output is 1 byte (i.e. a set of 8 bits), and linked with the consequent output using XOR, as shown in Figure 3.4. The XOR process contains three sequential phases.

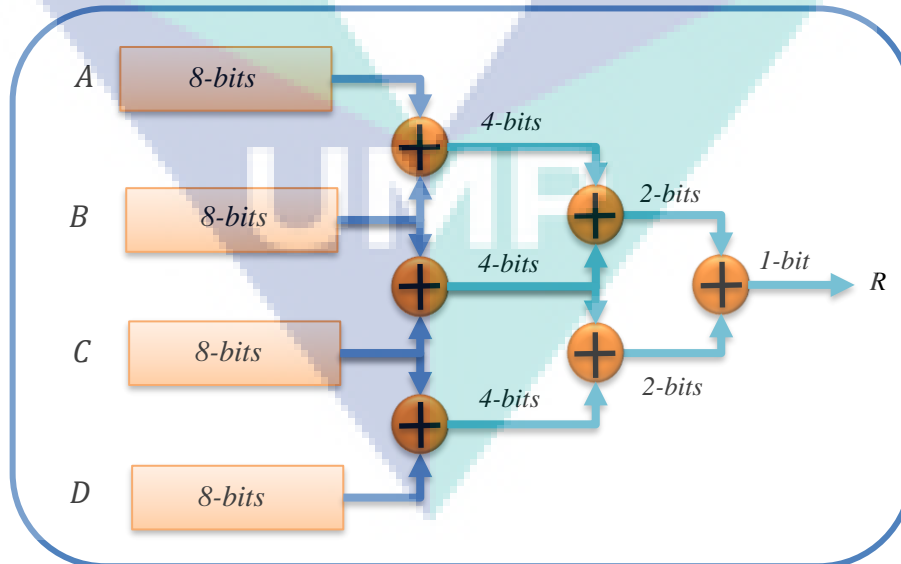


Figure 3.4 XOR Processes

The XOR stage consists of three phases. Inside each phase, half number of bits in specific position are selected which decrease the total number of bits to the half.

XOR phase 1:

This phase XORed only 4 specific 4-bits of the sequence for all bytes (A, B, C, D). As illustrated in Table 3.1, the results from this phase are 4 bits only.

Table 3.1 First phase of XOR process

<i>A</i>	<i>B</i>	$A \oplus B$	<i>B</i>	<i>C</i>	$B \oplus C$	<i>C</i>	<i>D</i>	$C \oplus D$
[1]	[4]	[1]	[1]	[4]	[1]	[1]	[4]	[1]
[4]	[1]	[2]	[4]	[1]	[2]	[4]	[1]	[2]
[5]	[8]	[3]	[5]	[8]	[3]	[5]	[8]	[3]
[8]	[5]	[4]	[8]	[5]	[4]	[8]	[5]	[4]

XOR phase 2:

This phase XORed only 2 specific 2-bits of the sequence for all bytes (AB, BC, CD). As illustrated in Table 3.2, the results from this phase are 4 bits only.

Table 3.2 Second phase of XOR process

<i>AB</i>	<i>BC</i>	$AB \oplus BC$		<i>BC</i>	<i>CD</i>	$BC \oplus CD$
[1]	[4]	[1]		[1]	[4]	[1]
[4]	[1]	[2]		[4]	[1]	[2]

XOR phase 3:

This phase XORed only 2 specific 2-bits of the sequence for all bytes (ABC, BCD). As illustrated in Table 3.3.

Table 3.3 Third phase of XOR process

<i>ABC</i>	<i>BCD</i>	$ABC \oplus BCD$
[1]	[2]	[1]
[2]	[1]	[2]

XOR Phase 4:

The output from the previous phase, is XORed to produce one bit only, as in the following equation:

$$R = ABCD_{1st\ bit} \oplus ABCD_{2nd\ bit} \quad 3.2$$

where $R \in [0, 1]$ is the output for only one iteration.

As explained above, the output for a single run is 1 bit only. To produce a sequence of permutation keys (i.e. set of pixels or bytes) which can be used for the encryption algorithm, the PRNG runs for $(8 \times N)$ iterations and the results are combined. Thus the total number of iterations can be calculated by the following equation:

$$TotalIterations = \beta \times N + t \quad 3.3$$

where β is the number of bits which is 8, N is the height or width of the plain image, and t is the initial number of iterations (i.e. initialization stage).

Figure 3.5 shows the main steps of the pseudocode for the proposed LT-PRNG.

In figure 3.5, line 10 and line 13 represent the main logistic map and tent map respectively, while line 11 and line 13 represent the two hybrid chaotic maps. The results of these chaotic maps are kept in four separated variables (A, B, C, and D). Therefore, the contribution of LT-PRNG is represented in these lines and variables. The four variables are XORed together to produce one single bit each time. As illustrated in chapter 2, PRNG based on chaotic maps have been used for encryption algorithms. Therefore, it is very important to test the proposed PRNG in terms of the security efficiency, and pseudorandom statics. The results of these tests are going to be presented in the next chapter.

Algorithm (3.1): Proposed LT-PRNG

Start

Initialization

get X_0, μ

get Y_0, ω

$X_t = \text{Iterate LM } t \text{ Times}$

// LM means Logistic Map

$Y_t = \text{Iterate TM } t \text{ Times}$

// TM means Tent Map

For $b = 1$ **To** 8

$X_{t_new} = \text{LM}(X_{t_old})$

$Y_{t_new} = \text{TM}(Y_{t_old})$

$A = \text{LM}(X_{t_new}) \times 255$

// Get 8 bits

$B = \text{LTM}(X_{t_new}) \times 255$

// Get 8 bits

$C = \text{TM}(Y_{t_new}) \times 255$

Hybrid 1 // Get 8 bits

$D = \text{TLM}(Y_{t_new}) \times 255$

Hybrid 2 // Get 8 bits

// XOR : First Phase

$AB = A \text{ XOR } B$

// Get 4 bits

$BC = B \text{ XOR } C$

// Get 4 bits

$CD = C \text{ XOR } D$

// Get 4 bits

// XOR : Second Phase

$ABC = AB \text{ XOR } BC$

// Get 2 bits

$BCD = BC \text{ XOR } CD$

// Get 2 bits

// XOR : Third Phase

$ABCD = ABC \text{ XOR } BCD$

// Get 2 bits

// XOR : Forth Phase

$R[b] = ABCD[1] \text{ XOR } ABCD[2]$

// Get 1 bits

Next b

Convert R **To** Byte

Generate KeySequence **From** Byte

Stop

Figure 3.5 Pseudocode for LT-PRNG

3.4 Image Encryption algorithm

In order to improve the weaknesses of one dimensional chaotic map in terms of small key space and less key sensitivity, a hybrid PRNG of two chaotic maps is proposed in this thesis. The proposed encryption algorithm based on the proposed PRNG is used to protect the contents of the colored images. The block diagram of the proposed algorithm is illustrated in Figure 3-1. The encryption algorithm contains two stages, confusion stage and diffusion stage. One more stage is needed, which is the input stage. The encryption algorithm consists of the following:

Stage 1: Input stage:

Step 1: Read a colored image as the plain image.

Step 2: Get the width or height of the image.

Step 3: Get the R, G, B channels for the plain image.

Step 3: Read RX, RY, GX, GY, BX, BY, μ and ω as the initial values for generating three random sequences by using LT-PRNG (Section 3.3).

Stage 2: Confusion Stage:

In this stage, all positions of the pixels of the three colors are re-arranged based on the generated random sequences. The main steps of this stage as follows.

Step 1: Generate three random sequences:

```
RP = LT-PRNG(RX,  $\mu$ , RY,  $\omega$ )    // for the red channel
GP = LT-PRNG(GX,  $\mu$ , GY,  $\omega$ )    // for the green channel
BP = LT-PRNG(BX,  $\mu$ , BY,  $\omega$ )    // for the blue channel
```

Step 2: Re-arrange the channels by using a proposed confusion algorithm, and generate three confused colors:

```
CRed = Confusion (Red Channel, RP)    // for the red channel
CGreen = Confusion (Green Channel, GP) // for the red channel
CBlue = Confusion (Blue Channel, BP)   // for the red channel
```

The confusion function in the previous step is an algorithm proposed in this research. The input to this algorithm is a color channel (i.e. matrix with $N * M$), while the output is re-arranged matrix for the same color. The new pixels order depends on the generated random sequences by the previous step. The confusion algorithm is given by the following pseudocode:

Stage 3: Diffusion

In this stage, the final cipher image is generated. An XOR operated is implemented on the confused colors generated by the previous stage. The pseudocode shows the diffusion algorithm:

Algorithm (3.2): Confusion Algorithm

Input: C (Color) , N (Height or Width) , CP (Color permutation generated by PRNG)

Output: CC (Confused Color)

Start

```
Y = CP[CP.Length]           // The last value in the sequence
RC = Y mod 2                 // Odd or Even value
For p = 1 To N
    If RC = 0 Then            // Check whether the RC is even or odd
        X = 1
        For i = 1 To N       // Row Swap
            CC[ i , P ] = C[CP[X], P]
            X +=1
        Next i
        RC = 1
    Else
        X = 1
        For i = 1 To N       // Column Swap
            CC[ P , i ] = C[ P , CP[X]]
            X +=1
        Next i
        RC = 0
    End If
Next P
Stop
```

Figure 3.6 Pseudocode for confusion algorithm

Algorithm (3.3): Diffusion Algorithm

Input: N (Height or Width), CP (Color permutation generated by PRNG)

CRed (Confused Red channel)

CGreen (Confused Green Channel)

CBlue (Conduced Blue Channel)

Output: Cipher Image

Start

```
For i = 1 To N
    X = 1
    For J = 2 To N
        GreenCipher [i,J] = CBlue[i , J]  $\oplus$  CRed[i , J - 1]  $\oplus$  (GP[X] mod 256)
        BlueCipher [i,J] = CRed[i , J]  $\oplus$  CGreen[i , J - 1]  $\oplus$  (BP[X] mod 256)
        RedCipher [i,J] = CGreen[i , J]  $\oplus$  CBlue[i , J - 1]  $\oplus$  (RP[X] mod 256)
        X= X+1
    Next J
Next i
CipherImage = ToRGB(RedCipher, GreenCipher, BlueCipher)
Stop
```

Figure 3.7 Pseudocode of diffusion algorithm

Figure 3-8 contains an example of encrypting 5 pixels only to illustrate the main steps of the proposed encryption algorithm. As can be seen, the resulted image is the cipher image, which is generated by using the proposed PRNG, a long side with the enhanced confusion and diffusion algorithms. The cipher image will be tested in the next chapter.

3.5 Summary

The proposed enhancement for image encryption has been explained in this chapter in details. It contains four parts; the first part presented the research methodology used to design the proposed algorithm, while the second part, explained the original logistic map, tent map, and the proposed LT-PRNG for generating random key. LT-PRNG contains three stages, initialization, chaotic numbers generating and XOR processes. Finally, the third part illustrated the proposed encryption algorithm for colored images in three stages; input stage, confusion stage and diffusion stage. In addition to, the Pseudocode for LT-PRNG, confusion algorithm and diffusion algorithm have been included.

In order to validate and evaluate our proposed algorithms, several tests are going to be implemented over the encrypted images. Next chapter shows all of these results, as well as their discussion.

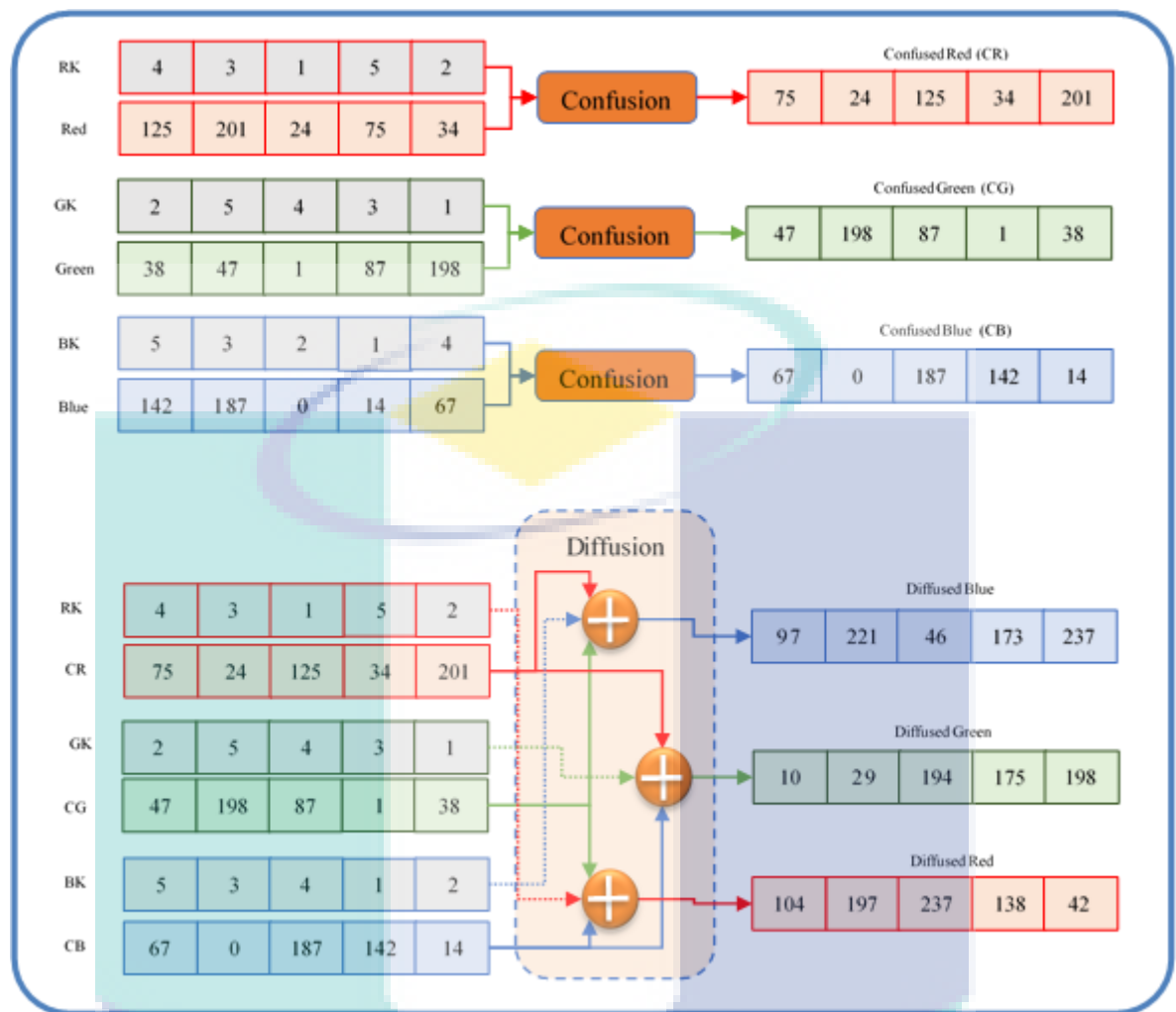


Figure 3.8 Example of Confusion and Diffusion stages

CHAPTER 4

RESULTS AND DISCUSSION

4.1 Introduction

The main aim of this thesis is to enhance the image encryption algorithm. The project focuses on the Fridrich structure, which contains two stages “confusion” and “diffusion”. Both stages are modified by using the LT-PRNG method, which depends on hybrid chaotic maps. Previous chapter illustrated the proposed image encryption algorithm, a long side with the LT-PRNG method.

Most of the image encryption techniques have some security issues. So, there is a need to evaluate and analyze the efficiency of the algorithms used for encryption. The analysis of the algorithm is done in terms of the tests like histogram analysis, number of pixels change rate (NPCR), and unified average changing intensity (UACI). In addition to these tests, the LT-PRNG method should be tested statistically by using NIST test suite.

These tests are useful in judging the quality of encryption algorithms used for encryption, and can also be used for checking the level of security, the algorithm actually provides to the actual image. This chapter presents the results of the proposed algorithm, and also presents the comparison with the most related works.

4.2 Security Analysis

Some simulation results are demonstrated in this section for the encryption algorithm. The algorithm has been implemented by using Microsoft C#.net version 6.0,

visual studio 2017. The computational platform is Microsoft Windows 10, with Intel core i5, CPU 2.4 GHz, and EMS memory 4 GB. Table 4-1 shows the key parameters, and values used in the implementation. The proposed encryption algorithm are going to be tested and evaluated in the next subsections in terms of the strength of the generated key sequences and the quality of the proposed encryption algorithm.

Table 4.1 Parameters values for the experiments

Parameter	Symbol	Value
<i>Mutation “LM”</i>	μ	3.99999998564
<i>Mutation “TM”</i>	α	1.9999998654
<i>Initial Value for Red “LM”</i>	X_R	0.1897526
<i>Initial Value for Green “LM”</i>	X_G	0.188542489
<i>Initial Value for Blue “LM”</i>	X_B	0.48547878
<i>Initial Value for Red “TM”</i>	Y_R	0.348795124
<i>Initial Value for Green “TM”</i>	Y_G	0.76548123
<i>Initial Value for Blue “TM”</i>	Y_B	0.54248711114

4.2.1 Key Space Analysis

According to (ECRYPT, 2011b), a key space size must contain more than 2^{128} possible keys. If the key space is too small, an attacker attempted to brute-force the system. Nevertheless, the sequence produced by LT-PRNG system depends on initial states, and the control parameters. The encryption algorithm with the PRNG is applied in C# with 10^{14} precision. For PRNG method, there are two initial values $X_0 \in [0,1]$ and $Y_0 \in [0,1]$ for two chaotic maps, and two control parameters $\mu \in [0,4]$, $\omega \in [0,2]$. Therefore, the key space for the LT-PRNG can be calculated as follows:

$$(10^{14}) \times (4 \times 10^{14}) \times (10^{14}) \times (2 \times 10^{14}) = 8 \times 10^{56} \cong 2^{208}$$

In addition, the result for the calculation above is only for one generated sequence, however, there are three different sequences generated by the proposed PRNG within the encryption algorithm. The calculation above proofed that the proposed PRNG has enough size of key space as compared with required. This indicates that all produced keys are

considered strong. A comparison of the key space of the suggested algorithm in this study with other PRNG algorithms was made and presented in Table 4-2. From the table, the key space of the suggested method was significantly larger towards resisting any form of brute-force attack.

Table 4.2 The key space results

PRNG	Key Space
Proposed Method	2^{208}
(Murillo-Escobar et al., 2017)	2^{128}
(Wang et al., 2016)	2^{186}
(Manish Kumar et al., 2016)	2^{144}
(García-Martínez and Campos-Cantón, 2015)	2^{159}
(Stoyanov and Kordov, 2015)	2^{183}

4.2.2 Key Sensitivity

An image encryption algorithm is perfect when it is sensitive to the secret key, i.e. any small change in the initial values will effect on the encrypted image. In order to analyse the sensitivity of the proposed algorithm, two outputs should be tested. The first output is a random sequence which is generated by using the PRNG method, while the second output is the cipher image which is generated by the encryption algorithm.

An algorithm of generating PRNG should be considerably subtle to the smallest changes in the generated keys. In order to test the sensitivity of the suggested PRNG method, the following test cases have been used to verify the sensitivity:

Case 1: Both X_0 and Y_0 equal 0.123456789,

Case 2: X_0 is changed from 0.123456789 to $X_0 + 2^{-48}$,

Case 3: Y_0 is changed from 0.123456789 to $Y_0 + 2^{-48}$,

Case 4: X_0 and Y_0 are changed from 0.123456789 to $X_0 + 2^{-44}$ and $Y_0 + 2^{-45}$.

Based on the above cases, the sequences of 2000 numbers are generated and compared with the original case. Figure 4-1 illustrates the first 20 numbers of each case.

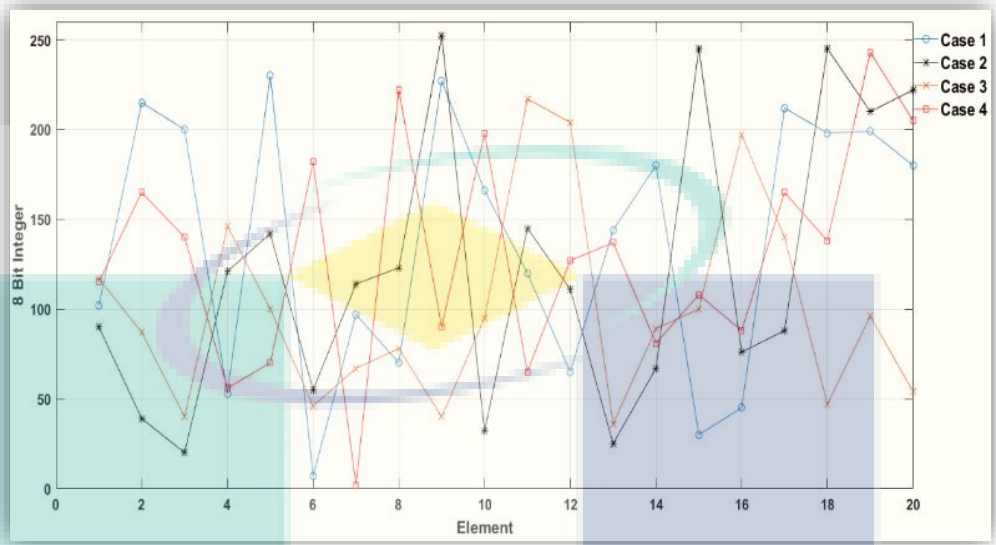


Figure 4.1 Key sensitivity analysis

For testing the key sensitivity of the proposed image encryption algorithm, the following test cases have been performed on Lena with length and width equal to 512 (Figure 13 – A):

Case 1: A plain image is encrypted by using same initial value for X_R , Y_R , X_G , Y_G , X_B , and Y_B , which is set to 0.123456789 (Figure 13-B).

Case 2: A cipher image is decrypted by using same initial values in Case1 (Figure13-C).

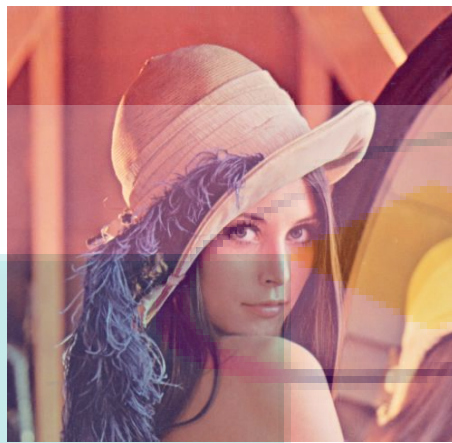
Case 3: A cipher image is decrypted by using same initial values in Case1, except for X_R , which is changed with a small value to 0.123456788 (Figure 13-D).

Case 4: A cipher image is decrypted by using same initial values in Case1, except for Y_G , which is changed with a small value to 0.123456788 (Figure 13-E).

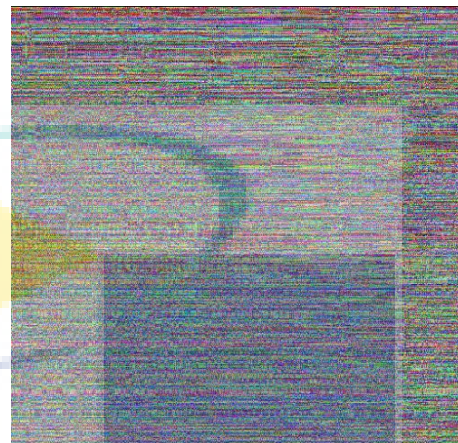
Case 5: A cipher image is decrypted by using same initial values in Case1, except for Y_B , which is changed with a small value to 0.123456788 (Figure 13-F).

As can be noted, the cases above (i.e. initial values) differ in a very small range, as well as they differ in only one initial value. The output of cases 3-4 have significant

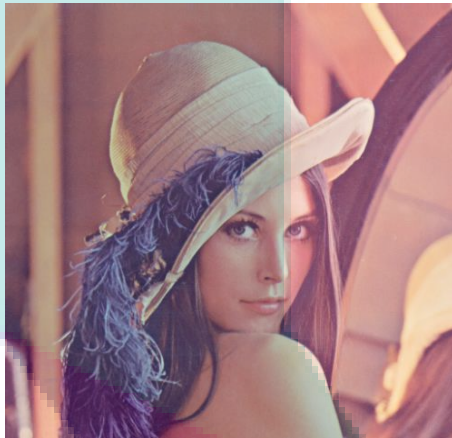
differences, which proves that the suggested encryption algorithm is highly sensitive to initial values.



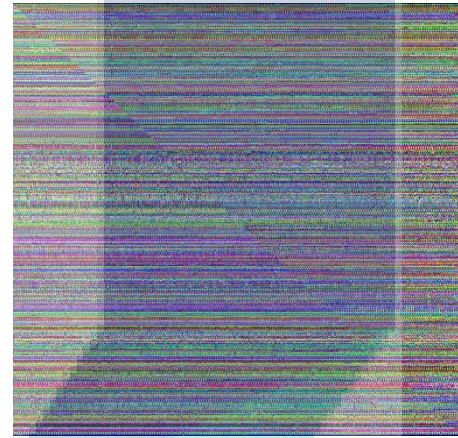
A – Original Image



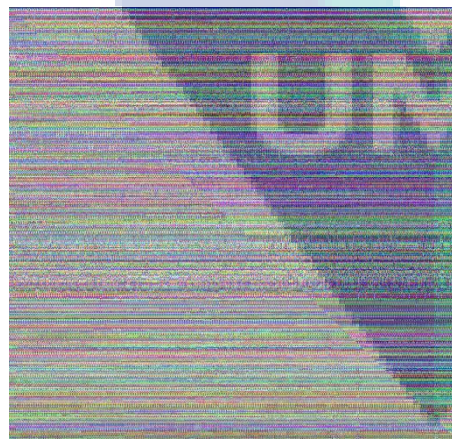
B – Case 1



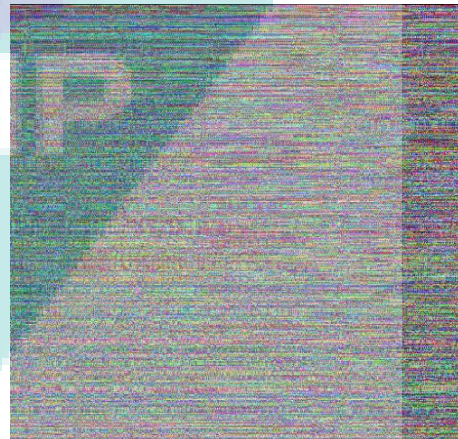
C – Case 2



D – Case 3



E – Case 4



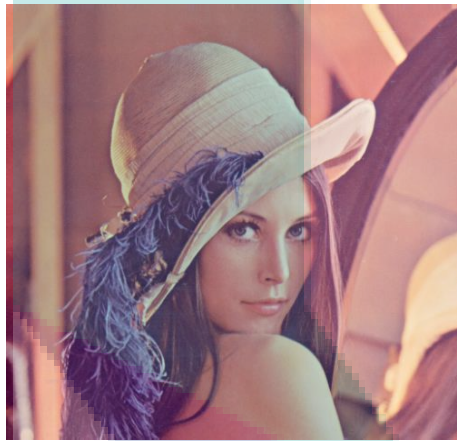
F – Case 5

Figure 4.2 Sensitivity analysis for encryption algorithm

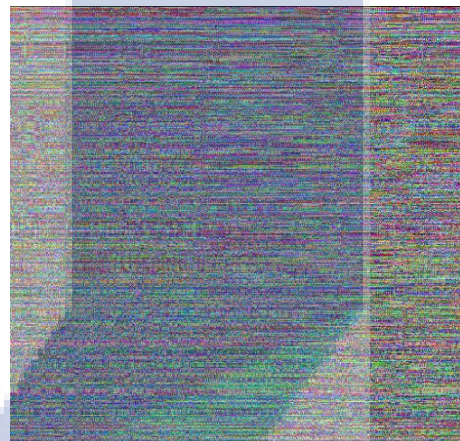
4.2.3 Histogram Analysis

The pixel distribution in an image obtained by plotting the pixel number at each level of color intensity is presented in the histograms. The histogram of Lena image, Baboon image, and Peppers image are shown in Figures 4.3, 4.4, and 4.5, respectively. The red, green, and blue channel histograms for the original image are displayed on the left side for each figure, while those of the cipher images are displayed on the right side.

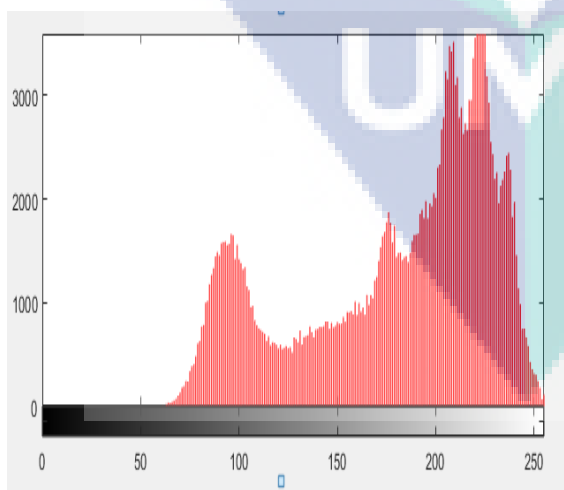
The histograms of the cipher images are evidently uniform and differed significantly from their respective plain image histograms, and hence, does not give any clue towards a possible statistical attack on the encryption scheme.



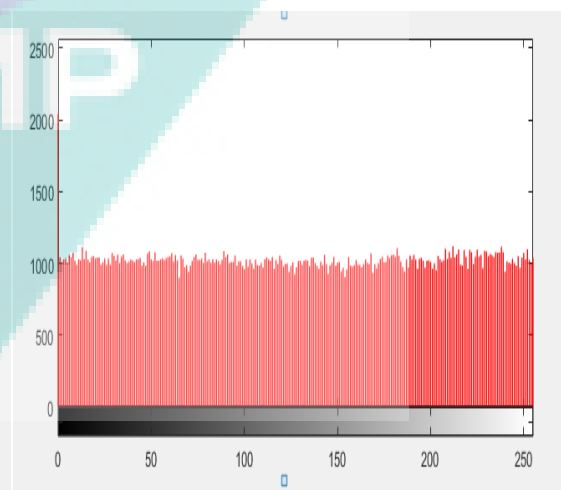
Original Image



Cipher image



Histogram for Red channel



Histogram for Red channel

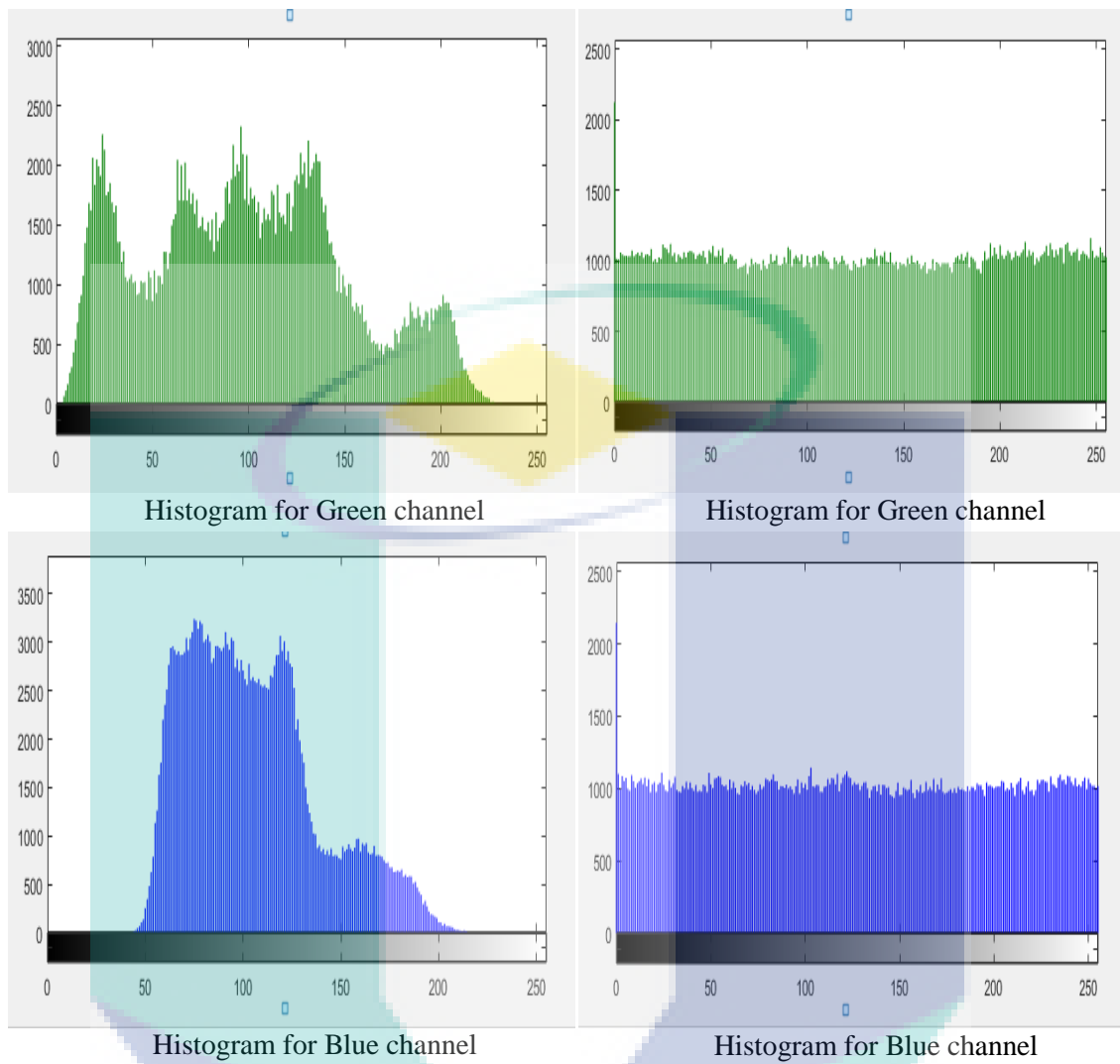
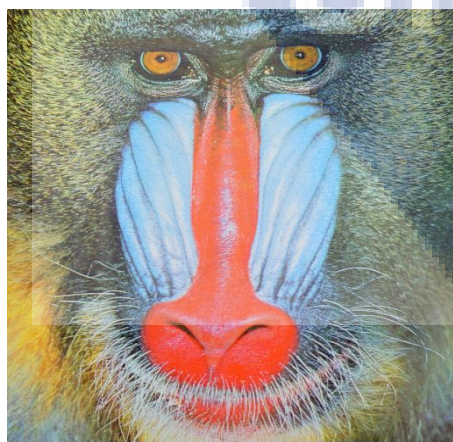
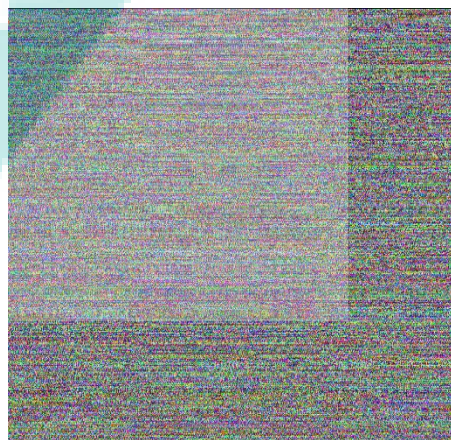


Figure 4.3 Histogram analysis for Lena image



Original Image



Cipher image

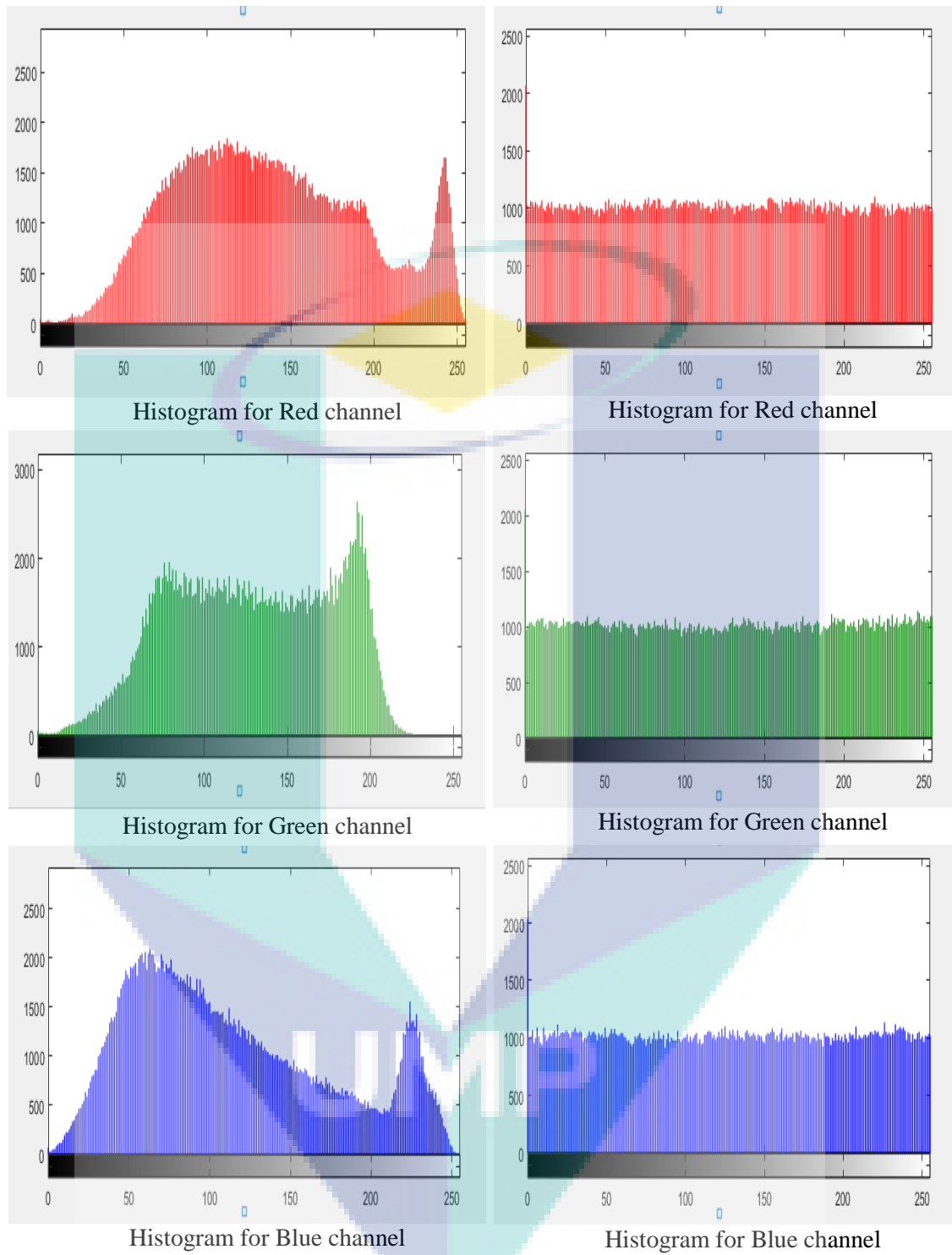
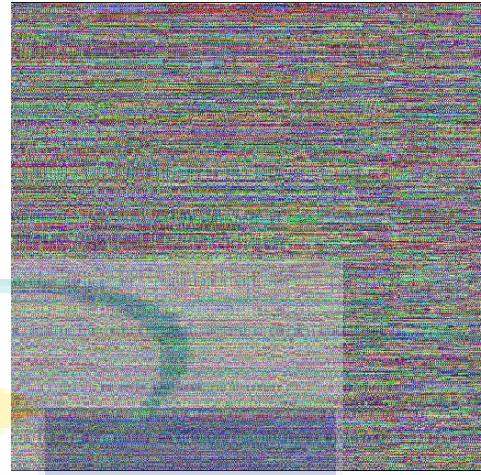


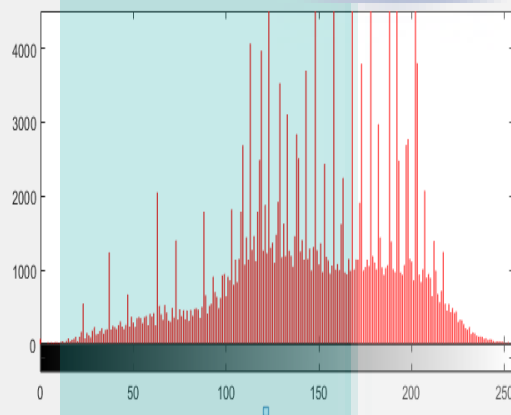
Figure 4.4 Histogram analysis for Baboon image



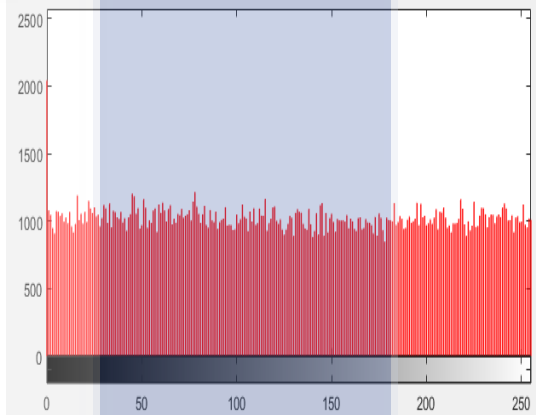
Original Image



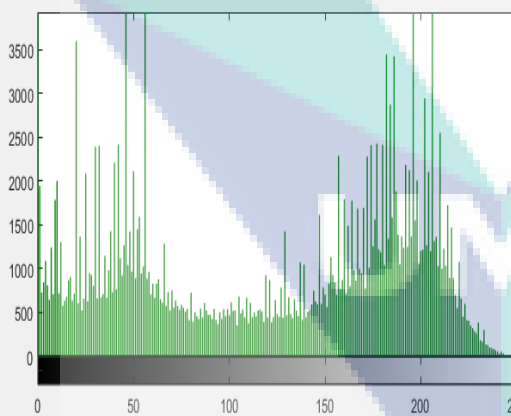
Cipher image



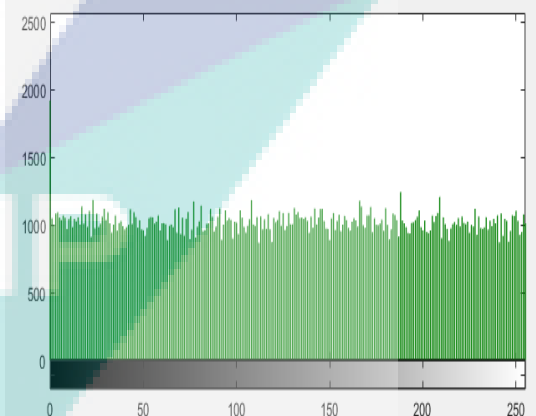
Histogram for Red channel



Histogram for Red channel



Histogram for Green channel



Histogram for Green channel

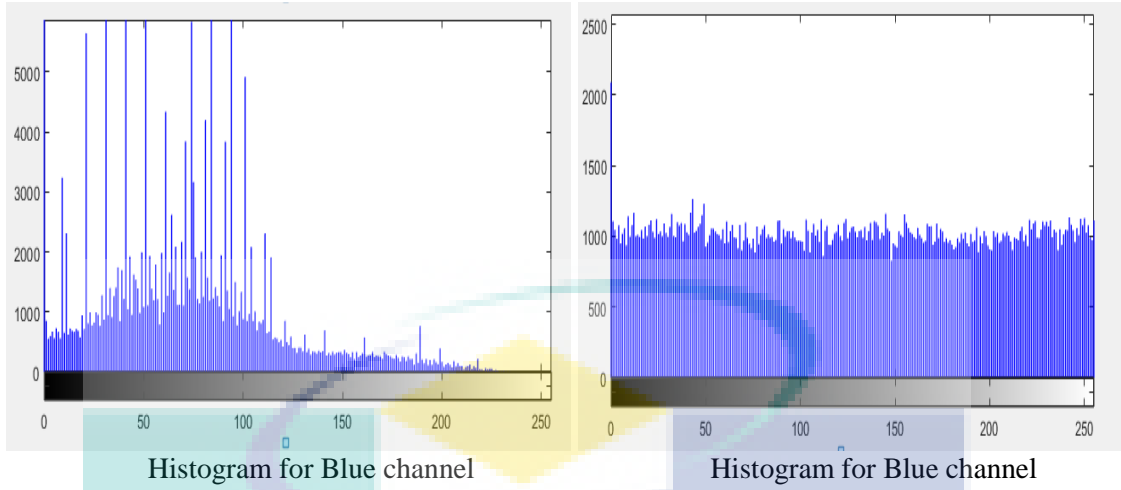


Figure 4.5 Histogram analysis for Peppers image

4.2.4 Correlation of Two Adjacent Pixels

There are three ways to test the correlation between two adjacent pixels, either by considering two vertically adjacent pixels, considering two horizontally adjacent pixels or by considering two diagonal adjacent pixels in the encrypted image. In this study, 5000 pairs of adjacent pixels were randomly selected for the correlation studies. The correlation results obtained are presented in Tables 4.3, 4.4, 4.5. The correlation factor for the original and encrypted Lena, Baboon, and Peppers images were calculated as:

$$r_{xy} = \frac{cov(x, y)}{\sqrt{D_x} \sqrt{D_y}}$$

$$cov(x, y) = E[(x - E(x))(y - E(y))]$$

$$E(x) = \frac{1}{L} \sum_{i=1}^L x_i; \quad D_x = \frac{1}{L} \sum_{i=1}^L (x_i - E(x))^2$$

Where x and y are the value of the adjacent pixels and L is the number of samples taken.

Figures 4.6, 4.7, and 4.8 show the respective scatter plots of the horizontal correlation of the 3 processed images. Furthermore, it can be deduced from the comparison table (Table 4.6) that the suggested algorithm can adequately secure Lena images.

Table 4.3 Correlation coefficients of two adjacent pixels in vertical direction

Image	Colour	Original Image	Cipher
Lena	Red	0.9899	0.0256
	Green	0.9889	0.0134
	Blue	0.9577	-0.0191
Baboon	Red	0.8631	0.0113
	Green	0.8585	-0.0182
	Blue	0.8889	0.0192
Peppers	Red	0.9754	0.0025
	Green	0.9798	-0.0197
	Blue	0.9766	0.0148

Table 4.4 Correlation coefficients of two adjacent pixels in horizontal direction

Image	Colour	Original Image	Cipher Image
Lena	Red	0.9791	0.0476
	Green	0.9698	-0.0400
	Blue	0.9344	-0.0619
Baboon	Red	0.9242	0.0179
	Green	0.8647	-0.0187
	Blue	0.9114	0.0215
Peppers	Red	0.9775	0.0271
	Green	0.9892	-0.0676
	Blue	0.9777	0.0254

Table 4.5 Correlation coefficients of two adjacent pixels in diagonal direction

Image	Colour	Original Image	Cipher Image
Lena	Red	0.9687	0.0096
	Green	0.9714	0.0068
	Blue	0.9143	0.0067
Baboon	Red	0.8615	-0.0096
	Green	0.8463	-0.0053
	Blue	0.8331	-0.0245
Peppers	Red	0.9559	-0.0207
	Green	0.9519	0.0072
	Blue	0.9617	-0.0028

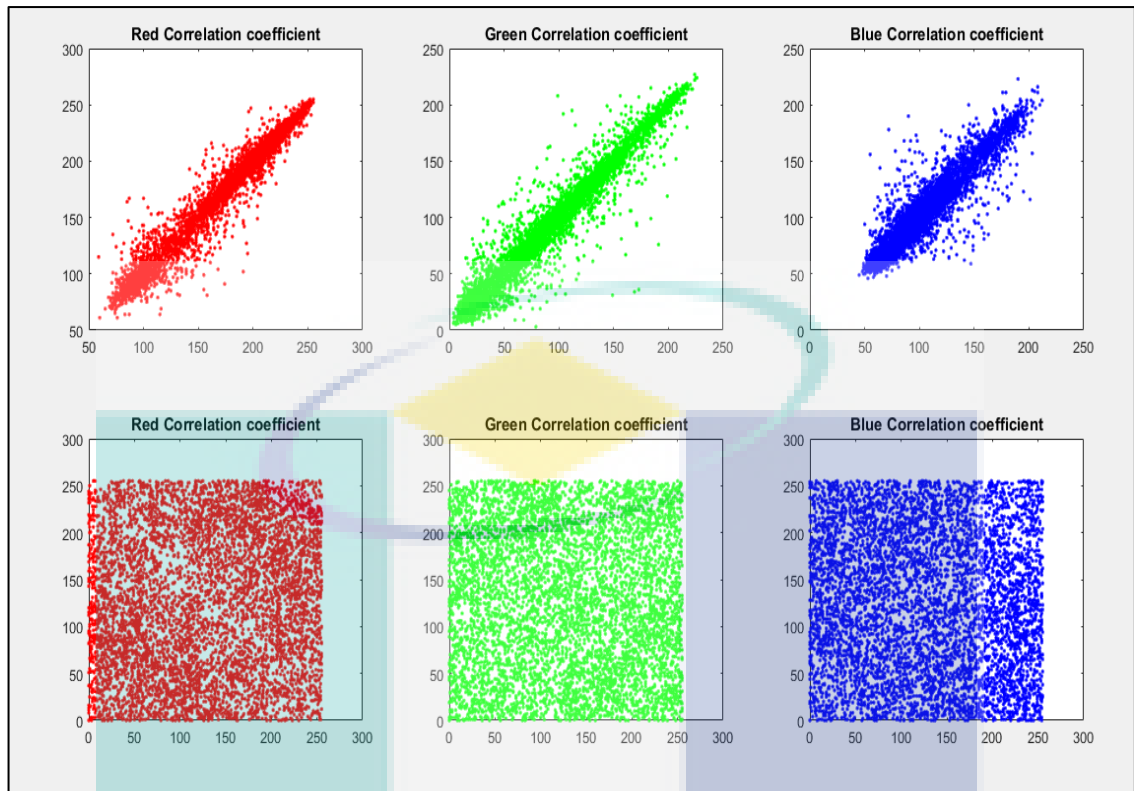


Figure 4.7 Horizontal correlation of the original and cipher Lena image

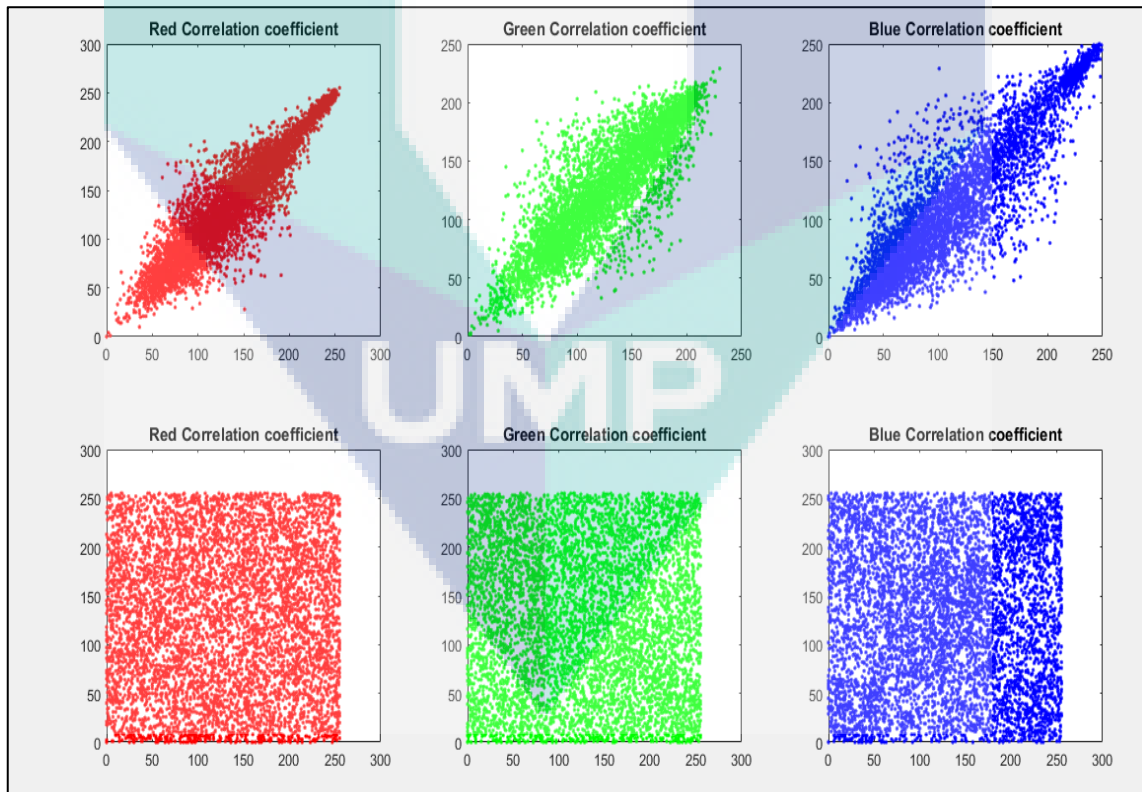


Figure 4.6 Horizontal correlation of the original and cipher Baboon image

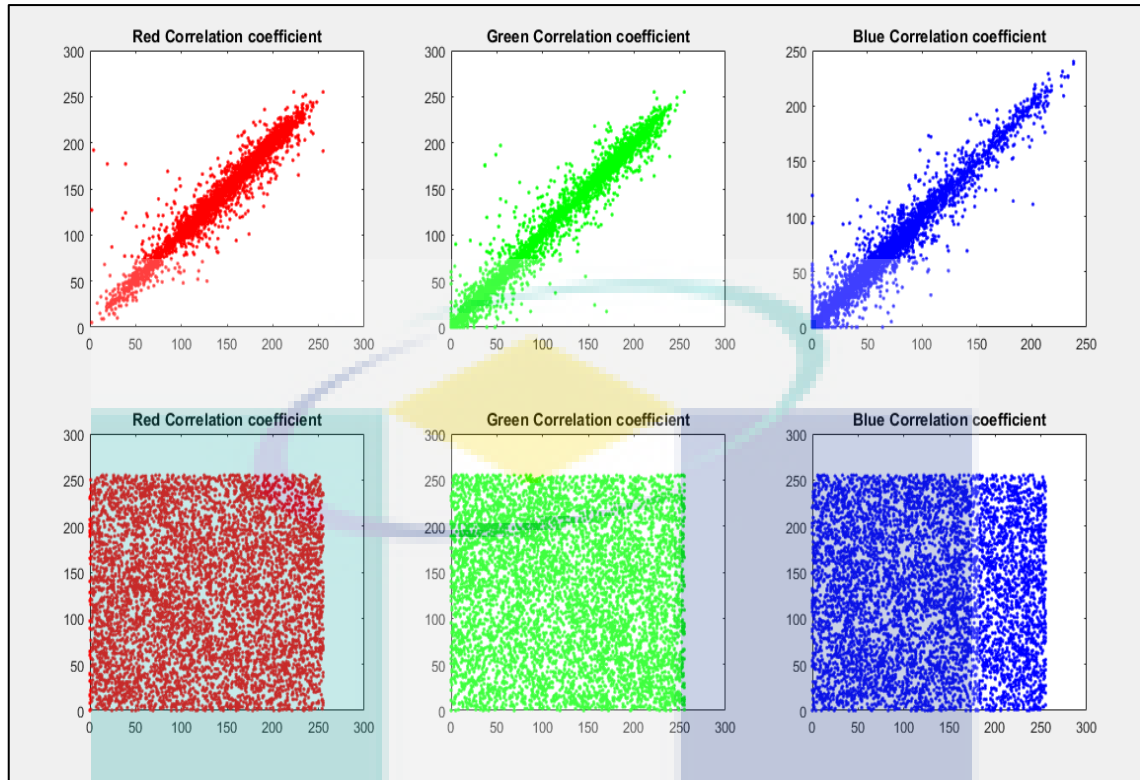


Figure 4.8 Horizontal correlation of the original and cipher Peppers image

Table 4.6 Correlation coefficients of two adjacent pixels for Lena

Algorithm	Direction	Red	Green	Blue
Original	Vertical	0.9890	0.9893	0.9540
	Horizontal	0.9812	0.9705	0.9338
	Diagonal	0.9663	0.9702	0.9212
Proposed	Vertical	0.0256	0.0134	-0.0191
	Horizontal	0.0476	0.0400	0.0271
	Diagonal	0.0096	0.0068	0.0067
(Y. Zhang and Xiao, 2014)	Vertical	-0.0009	0.0024	0.0021
	Horizontal	-0.0020	0.0018	0.0046
	Diagonal	0.0037	-0.0049	-0.0022
(Huang and Yang, 2017b)	Vertical	-0.0013	-0.0034	0.0038
	Horizontal	0.0027	0.0034	0.0046
	Diagonal	0.0039	-0.0021	0.0013
(Wu et al., 2014)	Vertical	0.00488	-0.00147	0.00188
	Horizontal	0.00249	-0.00337	-0.00283
	Diagonal	-0.00118	0.00438	0.00260

4.2.5 Correlations between Plain and Cipher Images

An analysis of the correlation coefficients (CC) between several plain/cipher image pairs was performed via a computation of the 2D CCs between the original and the cipher images. The CC was calculated thus:

$$CC = \frac{\sum_{i=1}^M \sum_{j=1}^N (A_{ij} - \bar{A}) (B_{ij} - \bar{B})}{\sqrt{(\sum_{i=1}^M \sum_{j=1}^N (A_{ij} - \bar{A})^2) (\sum_{j=1}^N (B_{ij} - \bar{B})^2)}}$$

where the plain and cipher images are represented as A and B respectively; \bar{A} and \bar{B} represent the mean values of A and B , respectively; and M and N represent the height and width of the original image and cipher image, respectively. From Table 4.7, the CC of the encryption process is pointed out for the 3 processed colors, followed by the CC between the original image and the cipher image shown in Table 4.8. The CCs between the analyzed pairs of the original/encrypted images are evidently small (almost zero).

Table 4.7 Correlations between Plain and Cipher image for all colors

Image	Direction	Correlation Coefficient		
		Red	Green	Blue
Lena	Horizontal	0.0083	-0.0026	0.0089
	Vertical	0.0103	-0.0020	0.0078
	Diagonal	0.0104	-0.0014	0.0079
Baboon	Horizontal	0.0064	0.0067	-3.2e-04
	Vertical	-0.0028	-0.0018	-0.0063
	Diagonal	0.0067	-8.1e-04	-0.0062
Peppers	Horizontal	0.0098	-0.0056	-0.0046
	Vertical	0.0051	-0.0093	-0.0048
	Diagonal	0.0054	-0.0094	-0.0054

Table 4.8 Correlation coefficient between the image and cipher image

Image	Correlation Coefficient		
	Horizontal	Vertical	Diagonal
Lena	0.0036	0.0040	0.0043
Baboon	0.0036	-0.0041	-0.0039
Peppers	-0.0014	-0.0039	-0.0040

The proposed algorithm had a better performance when applied to Lena images compared to the performance of other related works (as evidenced by the CC values shown in Table 4.9). There encrypted images significantly varied from the original images.

Table 4.9 Correlation coefficient comparison to other related work on Lena

Algorithm	Direction	Cipher Image		
		Red	Green	Blue
Proposed	Horizontal	0.0083	-0.0026	0.0089
	Vertical	0.0103	-0.0020	0.0078
	Diagonal	0.0104	-0.0014	0.0079
(Seyedzadeh, 2015)	Horizontal	0.0023	0.0003	0.0006
	Vertical	0.0005	0.0012	0.0003
	Diagonal	0.0009	0.0007	0.0007
(Wu et al., 2015)	Horizontal	0.0023	-0.0056	-0.0078
	Vertical	0.0009	-0.0036	0.0031
	Diagonal	-0.0147	-0.0295	-0.0246
(Niyat et al., 2017)	Horizontal	0.0049	0.0054	0.0053
	Vertical	0.0031	0.0001	0.0022
	Diagonal	0.0007	0.0017	0.0007

4.2.6 Information Entropy Analysis

Entropy is defined as the measure of uncertainty and can be used to express the uncertainties in the information of an image. The color-level distribution values in an image can also be determined via entropy analysis. If there is more uniformity in the color-level values distribution, there will be a greater entropy, and a higher entropy value portrays a better-secured encryption. Entropy is calculated thus:

$$H(S) = \sum_{i=0}^{2^M-1} P(S_i) \log_2 \frac{1}{P(S_i)}$$

where $P(S_i)$ is the probability of S_i , while 2^M is the state of the total source of information. An image is truly random (RI) if its pixel intensities are uniform in the range of $[0, 255]$, i.e., $P(RI) = 1/256$ for all $i \in [0, 255]$, hence, $H(RI) = 8$ bits. This means that an ideally random image has an entropy information value of 8.

In this study, we computed the entropy information values of the three standard plain-images and their respective cipher images, and the results of the computation are presented in Table 4-10. The obtained entropy values were close to the theoretical entropy value of $H = 8$ for an ideal random image, suggesting a negligible information leakage during the encryption process, and the closeness of the cipher-image to a random source. When compared to other existing algorithms based on the Lena image in Table 4-11, the proposed algorithm was closer to the ideal situation compared to the other algorithms, as the output was similar to a random output. The new encryption algorithm could, therefore, be said to be secure against entropy attacks.

Table 4.10 Information entropy of the proposed algorithm

Image	Plain Image				Cipher Image			
	Red	Green	Blue	Mean	Red	Green	Blue	Mean
Lena	7.2763	7.5834	7.0160	7.2919	7.9971	7.9970	7.9972	7.9971
Baboon	7.7603	7.4887	7.7787	7.6759	7.9972	7.9970	7.9971	7.9971
Peppers	7.3830	7.6072	7.1250	7.3717	7.9970	7.9969	7.9969	7.9969

Table 4.11 Comparison of information entropy

Algorithm	Cipher Image			
	Red	Green	Blue	Mean
Proposed	7.9971	7.9970	7.9972	7.9971
(H. Liu et al., 2015)	7.9808	7.9811	7.9814	7.9811
(Dong, 2014)	7.9901	7.9912	7.9921	7.9911
(Parvaz and Zarebnia, 2018)	7.9975	7.9970	7.9970	7.9971
(Wu et al., 2016)	7.9914	7.9907	7.9907	7.9909

4.2.7 NPCR and UACI Analysis

NPCR is the rate/number of pixel changes as one plain image pixel is changed. As the NPCR approaches 100%, the sensitivity of the cryptosystem to the plan image changes also increase, indicating the effectiveness of the cryptosystem towards resisting plaintext attacks. UACI is the average differences in the intensity of the plain and ciphered images. Bigger UACI represents more effectiveness of the cryptosystem towards resisting differential attacks. $NPCR_{R,G,B}$ and $UACI_{R,G,B}$ can be calculated thus:

$$NPCR_{R,G,B} = \frac{\sum_{ij} D_{R,G,B}(i,j)}{W \times H} \times 100\%$$

$$UACI_{R,G,B} = \frac{1}{W \times H} \left[\sum_{i,j} \frac{|C_{R,G,B}(i,j) - \bar{C}_{R,G,B}(i,j)|}{512 * 512} \right]$$

where W and H are the image width and height, respectively. $C_{R,G,B}(i,j)$ and $\bar{C}_{R,G,B}(i,j)$ are the encrypted images before and after changing one pixel of the plain image. For the pixel at position (i,j) , if $C_{R,G,B}(i,j) \neq \bar{C}_{R,G,B}(i,j)$, let $D(i,j) = 1$; else, let $D(i,j) = 0$.

In this study, two plain images (the original plain-image and the image obtained by changing the first pixel value of R channel from ‘235’ to ‘236’) were used to perform these tests. These images are encrypted using the same key to generate their respective cipher images (c1 and c2) after 2 cycles. The test results were obtained via simulation studies (as shown in Table 4-12). The $NPCR_{R,G,B}$ was found to be more than 99%, while

the $UACI_{R,G,B}$ was over 33%. These results present the proposed algorithm as a sensitive algorithm to small changes in the plain image. Even in the presence of just a bit difference between the two plain images, there will be a significant difference between the decrypted images and the plain images. Thus, the proposed algorithm is robust against differential attacks.

Table 4.12 NPCR and UACI of ciphered image with one bit different

Image	NPCR			UACI		
	Red	Green	Blue	Red	Green	Blue
Lena	99.614	99.621	99.612	33.572	33.644	33.638
Baboon	99.619	99.617	99.614	33.612	33.620	33.618
Peppers	99.618	99.619	99.618	33.688	33.685	33.694

4.2.8 The NIST Testing Strategy

The basis for the NIST statistical tests is based on hypothesis testing just like other statistical tests. A hypothetical test is a process of determining the extent of reasonability of a given assertion about the features of a given population. The hypothetical test in the present scenario is the determination of the randomness of a specific sequence of zeros and ones (referred to as the null hypothesis (H_0)). A relevant static randomness is selected for each test and used to determine whether to accept or reject the null hypothesis. When randomness is assumed, there is a distribution of possible values for such static. Mathematical methods are used to determine the statistic theoretical reference distribution under the null hypothesis. The corresponding p-value provides the supporting evidence for the null hypothesis rejection. The p-value for each test is the chances of producing a sequence that has less randomness than the sequence under test by a random number generator; given the type of non-randomness been assessed by the test. When the p-value of a test is 1, it shows a perfect randomness for the sequence, while a p-value of zero shows a total non-randomness of the sequence.

A level of significance can be assigned to the test. If the p-value is more than or equal to α , the sequence will be considered randomized and the null hypothesis will be

accepted; but if the p-value is less than α , the sequence will be considered non-randomized and the null hypothesis will be rejected. A typical level of significance α is selected within the interval of 0.001 and 0.01. When α is equal to 0.01, it signifies that one out of a hundred sequences will be rejected; but a α of ≥ 0.01 indicates that the sequence is considered random with a confidence level of 99 %. The numerical analysis of the proposed PRBG involved 3000 different sequences with each of the sequence having 1,000,000 bits each. These bits were generated by the PRNG. The p-value of each sequence was calculated for the 16 tests in the NIST suit. Table 4.13 shows the sequences and the corresponding p-values. Also calculated was the percentage of sequences that passed these tests. From the reports of (NIST) (Patidar et al., 2009), the acceptable range of proportion is [0.9766,0.9966]. From Table 4.13, it was evident that about 98.60 % of the sequences passed the whole random tests with each lying within the confidence interval. Therefore, the generated sequence had good properties with regard to the 16 tests in the NIST suit.

Table 4.13 Results of NIST

Test	Proportion	p-value	Result
Frequency	0.9800	0.445772	random
Block frequency	0.9966	0.543803	random
Cumulative sums-forward	0.9800	0.434157	random
Cumulative sums-backward	0.9766	0.485046	random
Runs	0.9866	0.451583	random
Longest run	0.9966	0.492972	random
FFT	0.9966	0.478362	random
Non-overlapping template	0.9900	0.498682	random
Overlapping template	0.9900	0.494927	random
Universal	0.9833	0.499759	random
Approximate entropy	0.9900	0.475617	random
Random excursions*	0.9862	0.308323	random
Random excursions variant*	0.9872	0.308269	random
Serial	0.9833	0.514053	random
Serial	0.9866	0.488291	random
Linear complexity	0.9933	0.493688	random

CHAPTER 5

CONCLUSION AND FUTURE WORKS

5.1 Introduction

At the existing eras where the most important communication is through wireless techniques using internet network to transfer data, the main concerns are on the subject of the security of such personal or countries defense data. Encryption is a unique way to guarantee worthy security from unofficial access at many grounds. Image encryption is striking extent for research in this case because communication with the support of multimedia objects is growing promptly. Various important encryption techniques have been presented in demand to acquainted it with a number of encryption algorithms used in encrypting the image which has been transmitted over network. The outcomes of every algorithm has advantages and disadvantages based on their techniques which are being practiced on images.

Further chaos based image encryption has been reviewed in detailed. Relating to current chaotic maps, the chaotic systems are capable of producing a huge number of new chaotic maps. They all have comparable properties together with exceptional chaotic behaviors, big chaotic range and uniform distributed density function. To investigate application encryption in time samples pattern, an enhanced image encryption based on Fredric structure has been proposed.

The algorithm contains two stages, confusion and diffusion. The confusion stage changes the positions of the pixels (i.e. the colors), while the diffusion stage changes in the contents of the pixels. Both stages depend on a key generated by using a random generator. The key is generated by using pseudo random number generator (PRNG), which is mainly dependent on chaotic maps. The chaotic maps can be classified into two

types, one dimension and multi dimensions. One-dimension chaotic maps are simple structure and easy to implement. Despite these advantages, the main limitation of the one-dimension chaotic maps is that when using them for the generation of a pseudo-random number, the key space is usually small and leads to the development of weak encryption algorithms. On the other hand, multi dimension chaotic maps have larger key space, but with difficulties in hardware/software implementation. Moreover, the computational complexity is increased when these chaotic maps are used for encryption algorithms.

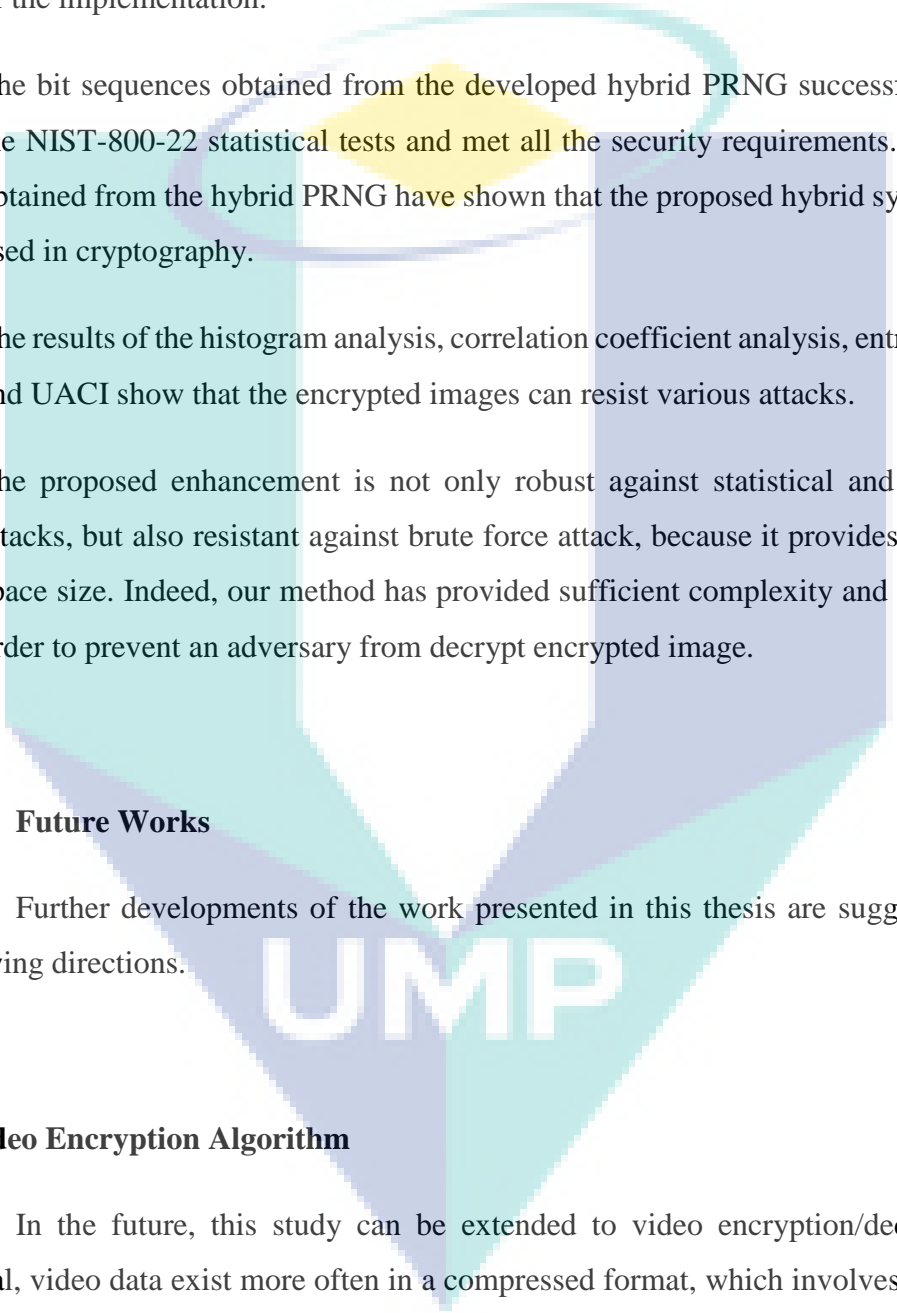
In this thesis, an enhanced image encryption algorithm has been proposed. The encryption algorithm contains a new pseudo random number generator PRNG based on hybrid chaotic maps. The research deals with the drawbacks of chaotic maps mentioned above. The proposed PRNG has a unique combination of logistic map and tent map, both of them are one-dimension maps. The results of these maps are used as an input to two inner chaotic maps. The inner chaotic maps are “Tent Logistic map (LTM)”, and “Logistic Tent map (TLM)”. The proposed PRNG produces random sequences, the output used for both mentioned encryption stages (i.e. confusion and diffusion).

The next section presents the conclusions of this research, while the last section presents the recommendation for the future work.

5.2 Conclusion

In this thesis, a new PRNG based on hybrid chaotic maps has been designed. The proposed PRNG is used for enhancing the colored image encryption algorithm. The proposed enhancement achieved better confusion and diffusion. A variety of simulation tests and analyses were carried out to prove the security and the performance of the proposed encryption scheme including statistical, differential, quality, contrast and speed analyses. The following goals have been achieved in this study:

- i) The proposed PRNG which is a hybrid of two chaotic maps (Logistic map and Tent map) and two more modified chaotic maps (Logistic-Tent map “LTM” and Tent-Logistic map “TLM”). These four chaotic maps represent the main contribution of this study.

- 
- ii) The proposed PRNG has shown its ability to produce a very large number of pseudo random sequences which can be useful in several cryptographic applications.
 - iii) The advantages of the PRNG are the adaptive size of the key space, the sensitivity to initial inputs (keys), the quality of pseudo-random sequences, and the simplicity of the implementation.
 - iv) The bit sequences obtained from the developed hybrid PRNG successfully passed the NIST-800-22 statistical tests and met all the security requirements. The results obtained from the hybrid PRNG have shown that the proposed hybrid system can be used in cryptography.
 - v) The results of the histogram analysis, correlation coefficient analysis, entropy, NPCR and UACI show that the encrypted images can resist various attacks.
 - vi) The proposed enhancement is not only robust against statistical and differential attacks, but also resistant against brute force attack, because it provides a large key space size. Indeed, our method has provided sufficient complexity and difficulty in order to prevent an adversary from decrypt encrypted image.

5.3 Future Works

Further developments of the work presented in this thesis are suggested in the following directions.

a) Video Encryption Algorithm

In the future, this study can be extended to video encryption/decryption. In general, video data exist more often in a compressed format, which involves intra frame compression and motion compensation. The extended cipher could be designed to operate on the Intra frames (I-frames), Predicted frames (P-frames), and Bi-predictive frames of the compressed video. Besides, selective encryption techniques on video have long been considered as an attractive research direction. Its basic concept is to encrypt only a portion of the entire plain video to protect it from illegal attempts to reconstruct the video.

b) Combined Compression to reduce Cipher Size

In image storage or transmission, lossless or lossy compression is usually applied, so as to reduce the information to be stored or transmitted. Similarly, it is also expected that a reduction of the cipher image size by combined compression encryption techniques should increase the encryption efficiency. In general, the compression part should consume a considerably lesser time in the whole process.

c) Theoretical aspects of cipher

The chaos theory consistently plays an active role in modern cryptography. In future, the work can be extended, by applying the theoretical aspects of cipher design, to Integrated Circuit (IC) chip based implementation, and make an effort to better the performance of chaotic image encryption.

UMP

REFERENCES

- Abutaha, M., El Assad, S., Jallouli, O., Queudet, A., & Deforges, O. (2016). Design of a pseudo-chaotic number generator as a random number generator. *IEEE International Conference on Communications*.
<https://doi.org/10.1109/ICComm.2016.7528291>
- Addabbo, T., Alioto, M., Fort, A., Pasini, A., Rocchi, S., & Vignoli, V. (2007). A Class of Maximum-Period Nonlinear Congruential Generators Derived From the Rényi Chaotic Map A Class of Maximum-Period Nonlinear Congruential Generators Derived From the Rényi Chaotic Map. *IEEE Transactions on Circuits and Systems*, 54(4), 816–828. <https://doi.org/10.1109/TCSI.2007.890622>
- Addabbo, T., Alioto, M., Fort, A., Rocchi, S., & Vignoli, V. (2006). The digital tent map: Performance analysis and optimized design as a low-complexity source of pseudorandom bits. *IEEE Transactions on Instrumentation and Measurement*, 55(5), 1451–1458. <https://doi.org/10.1109/TIM.2006.880960>
- Akhshani, A., Akhavan, A., Mobaraki, A., Lim, S.-C., & Hassan, Z. (2014). Pseudo random number generator based on quantum chaotic map. *Communications in Nonlinear Science and Numerical Simulation*, 19(1), 101–111. <https://doi.org/10.1016/j.cnsns.2013.06.017>
- Aljawarneh, S., Yassein, M. B., & Talafha, W. A. (2017). A resource-efficient encryption algorithm for multimedia big data. *Multimedia Tools and Applications*, 76(21), 22703–22724. <https://doi.org/10.1007/s11042-016-4333-y>
- Arroyo, D., Diaz, J., & Rodriguez, F. B. (2013). Cryptanalysis of a one round chaos-based Substitution Permutation Network. *Signal Processing*, 93(5), 1358–1364. <https://doi.org/10.1016/j.sigpro.2012.11.019>
- Baptista, M. S. (1998). Cryptography with chaos. *Physics Letters A*, 240(1–2), 50–54. [https://doi.org/10.1016/S0375-9601\(98\)00086-3](https://doi.org/10.1016/S0375-9601(98)00086-3)
- Callegari, S., Rovatti, R., Member, S., Setti, G., & Member, S. (2005). Embeddable ADC-Based True Random Number Generator for Cryptographic Applications Exploiting Nonlinear Signal Processing and Chaos. *IEEE TRANSACTIONS ON SIGNAL PROCESSING*, 53(2), 793–805.
- Chai, X. (2017). An image encryption algorithm based on bit level Brownian motion and new chaotic systems. *Multimedia Tools and Applications*, 1159–1175.

<https://doi.org/10.1007/s11042-015-3088-1>

- Chai, X., Chen, Y., & Broyde, L. (2017). A novel chaos-based image encryption algorithm using DNA sequence operations. *Optics and Lasers in Engineering*, 88, 197–213. <https://doi.org/10.1016/j.optlaseng.2016.08.009>
- Chang, S., Li, M., & Lin, W. (2009). Asymptotic synchronization of modified logistic hyper-chaotic systems and its applications. *Nonlinear Analysis: RealWorld Applications*, 10(2), 869–880. <https://doi.org/10.1016/j.nonrwa.2007.11.010>
- Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2010). Digital image steganography: Survey and analysis of current methods. *Signal Processing*. <https://doi.org/10.1016/j.sigpro.2009.08.010>
- Chen, S., Hwang, T., & Lin, W. (2010). Randomness Enhancement Using Digitalized Modified Logistic Map. *IEEE Transactions on Circuits and Systems*, 57(12), 996–1000.
- Cicek, I., Pusane, A. E., & Dundar, G. (2014). A novel design method for discrete time chaos based true random number generators. *Integration, the VLSI Journal*. <https://doi.org/10.1016/j.vlsi.2013.06.003>
- Dăscălescu, A. C., Boriga, R. E., & Diaconu, A. V. (2013). Study of a new chaotic dynamical system and its usage in a novel pseudorandom bit generator. *Mathematical Problems in Engineering*. <https://doi.org/10.1155/2013/769108>
- Delfs, H., & Knebl, H. (2015). *Introduction to cryptography: Principles and applications: Third edition*. *Introduction to Cryptography: Principles and Applications: Third Edition*. <https://doi.org/10.1007/978-3-662-47974-2>
- Dong, C. (2014). Color image encryption using one-time keys and coupled chaotic systems. *Signal Processing: Image Communication*, 29(5), 628–640. <https://doi.org/10.1016/j.image.2013.09.006>
- ECRYPT, I. (2011a). *Ecrypt II Yearly Report on Algorithms and Keysizes (2010-2011). Revision*. Retrieved from http://www.witi.cs.uni-magdeburg.de/~alang/paper/dittmann_lang_steinebach_katzenbeisser-ecrypt-noe_gi2005.pdf%5Cnhttp://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:ECRYPT+II+Yearly+Report+on+Algorithms+and+Keysizes#0%5Cnhttp://scholar.google.com/
- ECRYPT, I. (2011b). *Ecrypt II Yearly Report on Algorithms and Keysizes (2010-2011). Revision*.

- François, M., Defour, D., & Negre, C. (2014). A fast chaos-based pseudo-random bit generator using binary64 floating-point arithmetic. *Informatica (Slovenia)*.
- François, M., Grosge, T., Barchiesi, D., & Erra, R. (2014). Pseudo-random number generator based on mixing of three chaotic maps. *Communications in Nonlinear Science and Numerical Simulation*, 19(4), 887–895. <https://doi.org/10.1016/j.cnsns.2013.08.032>
- Fridrich, J. (1998a). Symmetric ciphers based on two-dimensional chaotic maps. *International Journal Of Bifurcation And Chaos*, 8(6), 1259–1284. <https://doi.org/10.1142/s021812749800098x>
- Fridrich, J. (1998b). Symmetric ciphers based on two-dimensional chaotic maps. *International Journal Of Bifurcation And Chaos*, 8(6), 1259–1284. <https://doi.org/10.1142/s021812749800098x>
- García-Martínez, M., & Campos-Cantón, E. (2015). Pseudo-random bit generator based on multimodal maps. *Nonlinear Dynamics*, 82(1), 2119–2131.
- Hamza, R. (2017). A novel pseudo random sequence generator for image-cryptographic applications. *Journal of Information Security and Applications*, 35, 119–127. <https://doi.org/10.1016/j.jisa.2017.06.005>
- Hu, H., Liu, L., & Ding, N. (2013). Pseudorandom sequence generator based on the Chen chaotic system. *Computer Physics Communications*, 184(3), 765–768. <https://doi.org/10.1016/j.cpc.2012.11.017>
- Hua, Z., Zhou, Y., Pun, C. M., & Chen, C. L. P. (2015). 2D Sine Logistic modulation map for image encryption. *Information Sciences*, 297, 80–94. <https://doi.org/10.1016/j.ins.2014.11.018>
- Huang, H., & Yang, S. (2017a). Colour image encryption based on logistic mapping and double random-phase encoding. *IET Image Processing*. <https://doi.org/10.1049/iet-ipr.2016.0552>
- Huang, H., & Yang, S. (2017b). Colour image encryption based on logistic mapping and double random-phase encoding. *IET Image Processing*. <https://doi.org/10.1049/iet-ipr.2016.0552>
- Kanso, A., & Ghebleh, M. (2012). A novel image encryption algorithm based on a 3D chaotic map. *Communications in Nonlinear Science and Numerical Simulation*, 17(7), 2943–2959. <https://doi.org/10.1016/j.cnsns.2011.11.030>

- Kanso, A., & Ghebleh, M. (2017). An algorithm for encryption of secret images into meaningful images. *Optics and Lasers in Engineering*. <https://doi.org/10.1016/j.optlaseng.2016.10.009>
- Katz, J., & Lindell, Y. (2008). Introduction to Modern Cryptography. *Chapman & Hall/CRC*, 1–498. <https://doi.org/10.1080/10658989509342477>
- Kaur, N., & Behal, S. (2014). Audio Steganography Techniques-A Survey. *Journal of Engineering Research and Applications*, 4(6), 94–100. Retrieved from www.ijera.com
- Kumar, M., Aggarwal, A., & Garg, A. (2014a). A Review on Various Digital Image Encryption Techniques and Security Criteria. *International Journal of Computer Applications*. Retrieved from <http://www.ijcaonline.org/archives/volume96/number13/16854-6720>
- Kumar, M., Aggarwal, A., & Garg, A. (2014b). A Review on Various Digital Image Encryption Techniques and Security Criteria. *International Journal of Computer Applications*.
- Kumar, M., Iqbal, A., & Kumar, P. (2016). A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie – Hellman cryptography. *Signal Processing*. <https://doi.org/10.1016/j.sigpro.2016.01.017>
- Kwok, H. S., & Tang, W. K. S. (2007). A fast image encryption system based on chaotic maps with finite precision representation. *Chaos, Solitons & Fractals*, 32(4), 1518–1529. <https://doi.org/10.1016/j.chaos.2005.11.090>
- Lambic', D., & Nikolic', M. (2017). Pseudo-random number generator based on discrete-space chaotic map.pdf. *Nonlinear Dynamics*, 90(1), 223–232.
- Li, Chunhu and Luo, Guangchun and Qin, Ke and Li, C. (2017). An image encryption scheme based on chaotic tent map. *Nonlinear Dynamics*, 87(1), 1–7. <https://doi.org/10.1109/IWCFTA.2009.48>
- Li, C., Li, S., Asim, M., Nunez, J., Alvarez, G., & Chen, G. (2009). On the security defects of an image encryption scheme. *Image and Vision Computing*, 27(9), 1371–1381. <https://doi.org/10.1016/j.imavis.2008.12.008>
- Li, C., Xie, T., Liu, Q., & Cheng, G. (2014). Cryptanalyzing image encryption using chaotic logistic map. *Nonlinear Dynamics*, 78(5), 1545–1551. <https://doi.org/10.1007/s11071-014-1533-8>

- Li, D., Han, M., Member, S., & Wang, J. (2012). Chaotic Time Series Prediction Based on a Novel Robust Echo State Network. *TRANSACTIONS ON NEURAL NETWORKS AND LEARNING SYSTEMS*, 23(5), 787–799.
- Li, P., Li, Z., Halang, W. A., & Chen, G. (2006). A multiple pseudorandom-bit generator based on a spatiotemporal chaotic map. *Physics Letters A*, 349(6), 467–473. <https://doi.org/10.1016/j.physleta.2005.09.060>
- Li, X., Li, C., & Lee, I. K. (2016). Chaotic image encryption using pseudo-random masks and pixel mapping. *Signal Processing*, 125, 48–63. <https://doi.org/10.1016/j.sigpro.2015.11.017>
- Li, Y., Wang, C., & Chen, H. (2017). A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation. *Optics and Lasers in Engineering*, 90, 238–246. <https://doi.org/10.1016/j.optlaseng.2016.10.020>
- Lian, S. (2009). Efficient image or video encryption based on spatiotemporal chaos system. *Chaos, Solitons & Fractals*, 40(5), 2509–2519. <https://doi.org/10.1016/j.chaos.2007.10.054>
- Liu, H., Kadir, A., & Gong, P. (2015). A fast color image encryption scheme using one-time S-Boxes based on complex chaotic system and random noise. *Optics Communications*, 338, 340–347. <https://doi.org/10.1016/j.optcom.2014.10.021>
- Liu, H., & Wang, X. (2011). Color image encryption using spatial bit-level permutation and high-dimension chaotic system. *Optics Communications*, 284(16–17), 3895–3903. <https://doi.org/10.1016/j.optcom.2011.04.001>
- Liu, L., & Miao, S. (2016). A new image encryption algorithm based on logistic chaotic map with varying parameter. *SpringerPlus*, 5(1), 289. <https://doi.org/10.1186/s40064-016-1959-1>
- Liu, L., Zhang, Q., & Wei, X. (2012). A RGB image encryption algorithm based on DNA encoding and chaos map. *Computers & Electrical Engineering*, 38(5), 1240–1248. <https://doi.org/10.1016/j.compeleceng.2012.02.007>
- Liu, W., Sun, K., & Zhu, C. (2016). A fast image encryption algorithm based on chaotic map. *Optics and Lasers in Engineering*, 84, 26–36. <https://doi.org/10.1016/j.optlaseng.2016.03.019>
- Machkour, M., Saaidi, A., & Benmaati, M. L. (2015). A Novel Image Encryption Algorithm Based on the Two-Dimensional Logistic Map and the Latin Square Image Cipher. *3D Research*, 6(4), 1–18. <https://doi.org/10.1007/s13319-015-0068-1>

- Maguire, L. P., Roche, B., McGinnity, T. M., & McDaid, L. J. (1998). Predicting a chaotic time series using a fuzzy neural network. *Information Sciences*, 5(6), 125–136.
- Matthews, R. (1989). On the derivation of a “chaotic” encryption algorithm. *Cryptologia*, 13(1), 29–42. <https://doi.org/10.1080/0161-118991863745>
- Mazloom, S., & Eftekhari-Moghadam, A. M. (2009). Color image encryption based on Coupled Nonlinear Chaotic Map. *Chaos, Solitons & Fractals*, 42(3), 1745–1754. <https://doi.org/10.1016/j.chaos.2009.03.084>
- Menezes, a. J., Van Oorschot, P. C., & Vanstone, S. a. (1997). Handbook of applied cryptography. *Annals of Physics*, 54, 258. Retrieved from <http://books.google.com/books?hl=en&lr=&id=nSzoG72E93MC&oi=fnd&pg=PA1&dq=Handbook+of+applied+cryptography&ots=MUFeAboIgO&sig=bJ1xKtSAULJIA6xVAaddnwXp6g>
- Murillo-Escobar, M. A., Cruz-Hernández, C., Abundiz-Pérez, F., López-Gutiérrez, R. M., & Acosta Del Campo, O. R. (2015). A RGB image encryption algorithm based on total plain image characteristics and chaos. *Signal Processing*, 109, 119–131. <https://doi.org/10.1016/j.sigpro.2014.10.033>
- Murillo-Escobar, M. A., Cruz-Hernández, C., Cardoza-Avendaño, L., & Méndez-Ramírez, R. (2017). A novel pseudorandom number generator based on pseudorandomly enhanced logistic map. *Nonlinear Dynamics*, 87(1), 407–425. <https://doi.org/10.1007/s11071-016-3051-3>
- Nejati, H., Beirami, A., & Ali, W. H. (2012). Zigzag map: a variability-aware discrete-time chaotic-map truly random number generator. *Electronics Letters*. <https://doi.org/10.1049/el.2012.2762>
- Nian-sheng, L. (2011). Pseudo-randomness and complexity of binary sequences generated by the chaotic system. *Communications in Nonlinear Science and Numerical Simulation*, 16(2), 761–768. <https://doi.org/10.1016/j.cnsns.2010.04.021>
- Nien, H. H., Huang, W. T., Hung, C. M., Chen, S. C., Wu, S. Y., Huang, C. K., & Hsu, Y. H. (2009). Hybrid image encryption using multi-chaos-system. In *ICICS 2009 - Conference Proceedings of the 7th International Conference on Information, Communications and Signal Processing*. <https://doi.org/10.1109/ICICS.2009.5397632>
- Niyat, A. Y., Moattar, M. H., & Torshiz, M. N. (2017). Color image encryption based on hybrid hyper-chaotic system and cellular automata. *Optics and Lasers in Engineering*, 90(October 2016), 225–237.

<https://doi.org/10.1016/j.optlaseng.2016.10.019>

- Oğraş, H., & Türk, M. (2016). A Secure Chaos-based Image Cryptosystem with an Improved Sine Key Generator. *American Journal of Signal Processing*, 6(3), 67–76. <https://doi.org/10.5923/j.ajsp.20160603.01>
- Ostrovsky, R. (2010). *Foundations of Cryptography Volume 2. Foundations and Trends* (Vol. 1). <https://doi.org/10.1561/04000000001>
- Pande, A., & Zambreno, J. (2013). *Embedded multimedia security systems: Algorithms and architectures. Embedded Multimedia Security Systems: Algorithms and Architectures* (Vol. 9781447144). <https://doi.org/10.1007/978-1-4471-4459-5>
- Pareek, N. K., Patidar, V., & Sud, K. K. (2006). Image encryption using chaotic logistic map. *Image and Vision Computing*, 24(9), 926–934. <https://doi.org/10.1016/j.imavis.2006.02.021>
- Pareek, N. K., Patidar, V., & Sud, K. K. (2010). A Random Bit Generator Using Chaotic Maps. *International Journal of Network Security*, 10(1), 32–38.
- Parvaz, R., & Zarebnia, M. (2018). A combination chaotic system and application in color image encryption. *Optics and Laser Technology*, 101, 30–41. <https://doi.org/10.1016/j.optlastec.2017.10.024>
- Patidar, V., Sud, K., & Pareek, N. (2009). A pseudo random bit generator based on chaotic logistic map and its statistical testing. *Journal of Informatical*, 33(October 2015), 441–452. Retrieved from <http://www.freepatentsonline.com/article/Informatica/216411794.html>
- Radwan, A. G., AbdElHaleem, S. H., & Abd-El-Hafiz, S. K. (2016). Symmetric encryption algorithms using chaotic and non-chaotic generators: A review. *Journal of Advanced Research*. <https://doi.org/10.1016/j.jare.2015.07.002>
- Rani, M., & Agarwal, R. (2009). Chaos , Solitons and Fractals A new experimental approach to study the stability of logistic map. *Chaos, Solitons and Fractals*, 41(4), 2062–2066. <https://doi.org/10.1016/j.chaos.2008.08.022>
- Rathore, D., & Suryavanshi, A. (2016). A proficient image encryption using chaotic map approach.pdf. *International Journal of Computer Applications* (0975, 134(10), 0975-8887.
- Riaz, M., Jameel, A., Shah, A., & Hussain, A. (2017). Novel Secure Pseudorandom

- Number Generator Based on Duffing Map. *Wireless Personal Communications*, 1(1), 1–9.
- Savi, M. A. (2007). Effects of randomness on chaos and order of coupled logistic maps. *Physics Letters A*, 364(9), 389–395. <https://doi.org/10.1016/j.physleta.2006.11.095>
- Seyedzadeh, S. M. (2015). A novel color image encryption algorithm based on spatial. *Nonlinear Dynamics*, 511–529. <https://doi.org/10.1007/s11071-015-2008-2>
- Shannon, C. E. (1949). Communication Theory of Secrecy Systems. *Bell System Technical Journal*, 28(4), 656–715. <https://doi.org/10.1002/j.1538-7305.1949.tb00928.x>
- Sharif, A., Mollaefar, M., Habibi, M., & Nazari, M. (2016). Novel Method for Image Encryption Using Chaotic Maps. In *3rd International Conference on Applied Research in Computer & Information Technology* (pp. 1–10).
- Short, K. M. (1994). Steps Toward Unmasking Secure Communications. *International Journal of Bifurcation and Chaos*, 4(4), 959–977.
- Short, K. M. (1996). Unmasking A Modulated Chaotic Communications Scheme. *International Journal of Bifurcation and Chaos*, 6(2), 367–375.
- Singh, G. (2013). A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security. *International Journal of Computer Applications*, 67(19), 975–8887. <https://doi.org/10.5120/11507-7224>
- Solms, R. von, & Niekerk, J. van. (2013a). From information security to cyber security. *Computers & Security*, 38(October 2013), 97–102. <https://doi.org/10.1016/j.cose.2013.04.004>
- Solms, R. von, & Niekerk, J. van. (2013b). From information security to cyber security. *Computers & Security*, 38(October 2013), 97–102. <https://doi.org/10.1016/j.cose.2013.04.004>
- Stallings, W. (2011). *Cryptography and Network Security*. Network (Vol. 139). <https://doi.org/10.1007/11935070>
- Stoyanov, B., & Kordov, K. (2015). Novel secure pseudo-random number generation scheme based on two tinkerbell maps. *Advanced Studies in Theoretical Physics*. <https://doi.org/10.12988/astp.2015.5342>

- Sun, F. Y., Liu, S. T., Li, Z. Q., & Lu, Z. W. (2008). A novel image encryption scheme based on spatial chaos map. *Chaos Solitons & Fractals*.
- Wang, L., Song, H., & Liu, P. (2016). A novel hybrid color image encryption algorithm using two complex chaotic systems. *Optics and Lasers in Engineering*, 77, 118–125. <https://doi.org/10.1016/j.optlaseng.2015.07.015>
- Wang, L., Zou, F., & Hei, X. (2014). A hybridization of teaching – learning-based optimization and differential evolution for chaotic time series prediction. *Neural Computing and Applications*, 25(2), 1407–1422. <https://doi.org/10.1007/s00521-014-1627-8>
- Wang, S., Sun, W., Guo, Y., Yang, H., & Jiang, S. (2013). Design and analysis of fast image encryption algorithm based on multiple chaotic systems in real-time security car. *International Journal of Security and Its Applications*. <https://doi.org/10.14257/ijisia.2013.7.6.23>
- Wang, X., Teng, L., & Qin, X. (2012). A novel colour image encryption algorithm based on chaos. *Signal Processing*, 92(4), 1101–1108. <https://doi.org/10.1016/j.sigpro.2011.10.023>
- Wang, X. Y., & Qin, X. (2012). A new pseudo-random number generator based on CML and chaotic iteration. *Nonlinear Dynamics*, 70(2), 1589–1592. <https://doi.org/10.1007/s11071-012-0558-0>
- Wang, Y., Liu, Z., Ma, J., & He, H. (2016). A pseudorandom number generator based on piecewise logistic map. *Nonlinear Dynamics*, 83(4), 2373–2391. <https://doi.org/10.1007/s11071-015-2488-0>
- Wong, K., & Yuen, C. (2008). Embedding Compression in Chaos-Based. *IEEE Transactions on Circuits and Systems*, 55(11), 1193–1197.
- Wu, X., Bai, C., & Kan, H. (2014). A new color image cryptosystem via hyperchaos synchronization. *Communications in Nonlinear Science and Numerical Simulation*, 19(6), 1884–1897. <https://doi.org/10.1016/j.cnsns.2013.10.025>
- Wu, X., Li, Y., & Kurths, J. (2015). A New Color Image Encryption Scheme Using CML and a Fractional-Order Chaotic System, 1–28. <https://doi.org/10.1371/journal.pone.0119660>
- Wu, X., Wang, D., Kurths, J., & Kan, H. (2016). A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system, 350, 137–153. <https://doi.org/10.1016/j.ins.2016.02.041>

- Xu, L., Li, Z., Li, J., & Hua, W. (2016). A novel bit-level image encryption algorithm based on chaotic maps. *Optics and Lasers in Engineering*, 78, 17–25. <https://doi.org/10.1016/j.optlaseng.2015.09.007>
- Ye, G. (2010). Image scrambling encryption algorithm of pixel bit based on chaos map. *Pattern Recognition Letters*, 31(5), 347–354. <https://doi.org/10.1016/j.patrec.2009.11.008>
- Yu, Z., Zhe, Z., Haibing, Y., Wenjie, P., & Yunpeng, Z. (2010). A chaos-based image encryption algorithm using wavelet transform. In *2010 2nd International Conference on Advanced Computer Control* (pp. 217–222). IEEE. <https://doi.org/10.1109/ICACC.2010.5486684>
- Yuan, H., Liu, Y., Gong, L., & Wang, J. (2017). A new image cryptosystem based on 2D hyper-chaotic system. *Multimedia Tools and Applications*, 76(1), 8087–8108. <https://doi.org/10.1007/s11042-016-3454-7>
- Zhang, L. Y., Hu, X., Liu, Y., Wong, K. W., & Gan, J. (2014). A chaotic image encryption scheme owning temp-value feedback. *Communications in Nonlinear Science and Numerical Simulation*, 19(10), 3653–3659. <https://doi.org/10.1016/j.cnsns.2014.03.016>
- Zhang, W., Wong, K., Yu, H., & Zhu, Z. (2013a). A symmetric color image encryption algorithm using the intrinsic features of bit distributions. *Communications in Nonlinear Science and Numerical Simulation*, 18(3), 584–600. <https://doi.org/10.1016/j.cnsns.2012.08.010>
- Zhang, W., Wong, K., Yu, H., & Zhu, Z. (2013b). A symmetric color image encryption algorithm using the intrinsic features of bit distributions. *Communications in Nonlinear Science and Numerical Simulation*, 18(3), 584–600. <https://doi.org/10.1016/j.cnsns.2012.08.010>
- Zhang, W., Yu, H., Zhao, Y., & Zhu, Z. (2016). Image encryption based on three-dimensional bit matrix permutation. *Signal Processing*, 118, 36–50. <https://doi.org/10.1016/j.sigpro.2015.06.008>
- Zhang, X., Han, F., & Niu, Y. (2017). Chaotic Image Encryption Algorithm Based on Bit Permutation and Dynamic DNA Encoding.pdf. *Computational Intelligence and Neuroscience*, 2017(1), 1–11.
- Zhang, X., & Wang, X. (2017). Multiple-image encryption algorithm based on mixed image element and permutation. *Optics and Lasers in Engineering*, 92, 6–16. <https://doi.org/10.1016/j.optlaseng.2016.12.005>

- Zhang, Y.-Q., & Wang, X.-Y. (2014). A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice. *Information Sciences*, 273, 329–351. <https://doi.org/10.1016/j.ins.2014.02.156>
- Zhang, Y., & Xiao, D. (2014). International Journal of Electronics and Communications (AEÜ) Self-adaptive permutation and combined global diffusion for chaotic color image encryption. *AEUE - International Journal of Electronics and Communications*, 68(4), 361–368. <https://doi.org/10.1016/j.aeue.2013.10.002>
- Zhou, Y., Bao, L., & Chen, C. L. P. (2014). A New 1D Chaotic System for Image Encryption. *Signal Processing*, 00, 1–21.
- Zhou, Y., Cao, W., & Philip Chen, C. L. (2014). Image encryption using binary bitplane. *Signal Processing*, 100, 197–207. <https://doi.org/10.1016/j.sigpro.2014.01.020>
- Zhu, A., & Li, L. (2010). Improving for chaotic image encryption algorithm based on logistic map. In *2010 The 2nd Conference on Environmental Science and Information Application Technology* (pp. 211–214). IEEE. <https://doi.org/10.1109/ESIAT.2010.5568374>
- Zhu, Z., Zhang, W., Wong, K., & Yu, H. (2011). A chaos-based symmetric image encryption scheme using a bit-level permutation. *Information Sciences*, 181(6), 1171–1186. <https://doi.org/10.1016/j.ins.2010.11.009>

PUBLICATIONS

The contents of this thesis had been published in the fallowing publication:

Saba M. Ismail, Muamer N. Mohammed, Mohammed A. Ameendeen, Hussam Alddin S. Ahmed, (2018), '*A New Trend of Pseudorandom Number Generator using Multiple Chaotic Systems*', , Advanced Science Letters, 24(10) .

Hussam Alddin S. Ahmed, Mohamad F. Zolkipli, Yazan A. Alsariera, **Saba M. Ismail**, (2018), '*Pseudo random bits' generator based on Tent chaotic map and linear feedback shift register*' , Advanced Science Letters, 24(10) .

The logo of the University of Mosul (UMP) is a large, stylized shield shape. It is composed of several triangular and quadrilateral sections in shades of teal, light blue, and white. The letters 'UMP' are prominently displayed in white, bold, sans-serif font across the center of the shield.

UMP