Palestine Polytechnic University
Deanship of Graduate Studies and Scientific Research
Master of informatics

Selective Hybrid Chaotic-Based Cipher for Real-Time Image Application

Submitted by:

Rawan Imad Qumsieh

Thesis submitted in partial fulfillment of requirements of the degree Master of Science in Informatics
November, 2017

The undersigned hereby certify that they have read, examined and recommended to the Deanship of Graduate Studies and Scientific Research at Palestine Polytechnic University the approval of a thesis entitled: **Selective Hybrid Chaotic-Based Cipher for Real-Time Image Application**, submitted by **Rawan Imad Qumsieh** in partial fulfillment of the requirements for the degree of Master in Informatics.

Graduate Advisory Committee:

Dr. Mousa Farajallah (Supervisor), Palestine Polytechnic University.

Signature:_____ Date:_____

Dr. (Internal committee member), Palestine Polytechnic University.

Signature:_____ Date:_____

Dr. (External committee member), .

Signature:_____ Date:_____

Thesis Approved

Dr. Murad Abusubaih
Dean of Graduate Studies and Scientific Research
Palestine Polytechnic University

Signature:_____ Date:_____

DECLARATION

I declare that the Master Thesis entitled **"Selective Hybrid Chaotic-Based Cipher for Real-Time Image Application"** is my original work, and herby certify that unless stated, all work contained within this thesis is my own independent research and has not been submitted for the award of any other degree at any institution, except where due acknowledgement is made in the text.

Rawan Imad Qumsieh

Signature:_____ Date:_____

STATEMENT OF

PERMISSION TO USE

In presenting this thesis in partial fulfillment of the requirements for the master degree in Informatics at Palestine Polytechnic University, I agree that the library shall make it available to borrowers under rules of the library.

Brief quotations from this thesis are allowable without special permission, provided that accurate acknowledgement of the source is made.

Permission for extensive quotation from, reproduction, or publication of this thesis may be granted by my main supervisor, or in his absence, by the Dean of Graduate Studies and Scientific Research when, in the opinion of either, the proposed use of the material is for scholarly purposes.

Any coping or use of the material in this thesis for financial gain shall not be allowed without my written permission.

Rawan Imad Qumsieh

Signature:_____ Date:_____

DEDICATION

To my Father and Mother:

For being a great source of motivation, inspiration and endless support.

Thank you for all your sacrifices to help me becoming what I am now.

Thank you for being there during the hardest times.

Thank you for believing in me.

To my lovely sisters for making my life worth living by their support and endless love.

To my real friends for being there for me, for their true love and continuous encouragement.

ACKNOWLEDGEMENT

This thesis could have not been completed without the guidance, help and support of many people. I would like to express my appreciation to every person who supported me throughout the thesis project of this Masters of Informatics. I am genuinely grateful to them for sharing their honest and enlightening opinions about the project.

It gives me a great pleasure to acknowledge Dr. Mousa Farajallah for the continuous support and supervision for the success of this project.

I would like to thank deeply my parents for being a great model and encouraging me throughout my studies, they helped, guided and supported me all my life. My deepest gratitude goes to all of my friends who stayed with me during my masters journey.

"In all chaos there is a cosmos, in all disorder a secret order."

– Carl Jung

Arabic abstract

Cont..

Abstract

Image encryption is much different from that of the texts due to the bulk data capacity and the high redundancy of images. Thus, traditional methods are difficult to be used for image encryption as their pseudo-random sequences have a small space. Chaotic cryptography uses the chaos theory in specific systems working such as computing algorithms to accomplish dissimilar cryptographic tasks in a cryptosystem with a fast throughput. For higher security, encryption is the approach to guard information and decrease its leakage.

In this thesis, we showed some of the recent work on chaos-based cryptography, especially those cryptosystems with the Skew Tent Map (STM), which we address and evaluate in this thesis, as a large number of chaos-based cryptosystems, were implemented using it. We proposed a hybrid encryption scheme that combines both stream and block ciphering algorithms to achieve the required level of security with the minimum encryption time; this scheme is based on a mathematical model improved to cover the defects in a previous discredited model proposed by Masuda. The proposed chaos-based cryptosystem uses the improved STM (R_Q-FSTM) as a substitution based on a lookup table to overcome various problems, such as the fixed point, the key space restrictions, and the limitation of mapping between plain text and cipher text. It uses the same map as a generator to change the byte posi-

tion to achieve the required confusion and diffusion effects. The proposed cryptosystem is flexible, efficient, and more robust against cryptanalysis.

The robustness of the proposed cryptosystem was proven by the performance and the security analysis, as well as the high encryption speed (throughput). Depending on the results of the security analysis done on our cryptosystem, and after comparing the results with the previous cryptosystems. Our proposed system has a better dynamic key space than the previous ones using skew tent map with a difference that is more than the triple size, a double encryption quality that is much closer to the optimal quality and a better security analysis than the others in the literature with a speed convenient to the real-time applications.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

STM	Skew Tent Map
FSTM	Finite State Tent Map
R_Q**-FSTM**	Rawans Finite State Tent Map
DES	Data Encryption Standard
3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
EEC	Elliptic-curve cryptography
RSA	RivestShamirAdleman
MPEG	Moving Picture Experts Group
MSB	Most Significant bit
NPCR	Number of Pixel Change Rate
UACI	Unified Average Changing Intensity
NLDS	Non-linear Dynamical Systems
NCA	Non-linear Chaotic Algorithm
VLSI	Very-Large-Scale Integration
CKBA	Chaotic Key-Based Algorithm
FPGA	Field-Programmable Gate Array

PWLCM	Piecewise Linear Chaotic Map
OCML	One-way Coupled Map Lattice
RGB	Red, Green and Blue
CCP	Column Circular Permutation
EQ	Encryption Quality
ET	Encryption Throughput

Chapter 1

Introduction

Chaos theory is the study of the behavior of dynamical systems that are very sensitive to initial conditions. Started at first in mathematics [1, 2, 3], then chaos theory has also been developed by many other research areas including physics, chemistry and biology[4, 5, 6]. Despite the fact that these dynamical systems are based on deterministic models, their high sensitivity to initial conditions or control parameters cause their outputs to be unpredictable[7]. The beginning of the chaotic systems returns back to the 1880's by Henry Poincare in his attempt to prove the stability of the solar system through his work on the restricted three-body problem [8]. Later, Edward Lorenz in 1961 contributed to the chaos theory[9].

One of the interesting applications of chaos is in the field of cryptography, as it concerns about techniques to secure the transfer of messages between two ends by encrypting those messages. Thus, many researchers have highlighted the strong relationship between chaos and cryptography[10, 11, 12]. More interestingly, Shannon indicated in his paper: Communication Theory of Secrecy Systems that is published in 1949[13], that good transformation in good secrecy systems is achieved by basic operations that are the heart

of chaotic maps[14]. In the same paper, Shannon invented two terms that are considered the major concepts of block ciphers, namely confusion and diffusion, where the mixing property and sensitivity to initial conditions of chaos generators are mapped to the diffusion and confusion of cryptosystems. Hence, the tight relationship between chaos and cryptography, created a new field of research called chaotic cryptography, where a lot of work has been published[15, 16, 17, 18, 19, 20, 21].

Chaos was used in the two types of modern encryption, which are symmetric-key encryption in its both forms, the stream ciphers and the block ciphers, and public-key encryption. In stream ciphers, the chaos generators are used to generate a stream of pseudo-random numbers in which researchers used as keys to mask the plaintext as in [22, 23, 24]. On the other hand, in block ciphers, the key used as an initial conditions and the control parameters of the chaos generators and then it generate the cipher text after many encryption rounds as the image encryption block ciphers proposed in [25, 26].

The work of this thesis mainly an improvement of the Skew Tent Map (STM) proposed by Masuda et al. in [24], and use it in a hybrid encryption scheme that combines both stream and block ciphering algorithms to achieve the best encryption quality with the minimum encryption time. The robustness of the proposed cryptosystem was proven by the performance and security analysis.

1.1 Problem Statement

On this thesis we will be working on the encryption methods of digital images focusing on the chaos mapping as it gives the encoded advanced images to

hold the multilevel encryption strategy furthermore reduce the computational difficulty of the encryption process.

Chaos theory with its very simple rules can lead to an extremely complex and unpredictable behavior, where one of the serious challenges in cryptography is to generate sequences of random numbers to use as the dynamic encryption keys. On the other hand, chaotic functions can provide a practical and un-cumbersome solution to the long-standing problem with one-time-systems [17]. Chaotic functions have sufficient sensitivity to its initial conditions, which allows the function to produce an unlimited number of infinitely long random key stream regardless its simplicity.

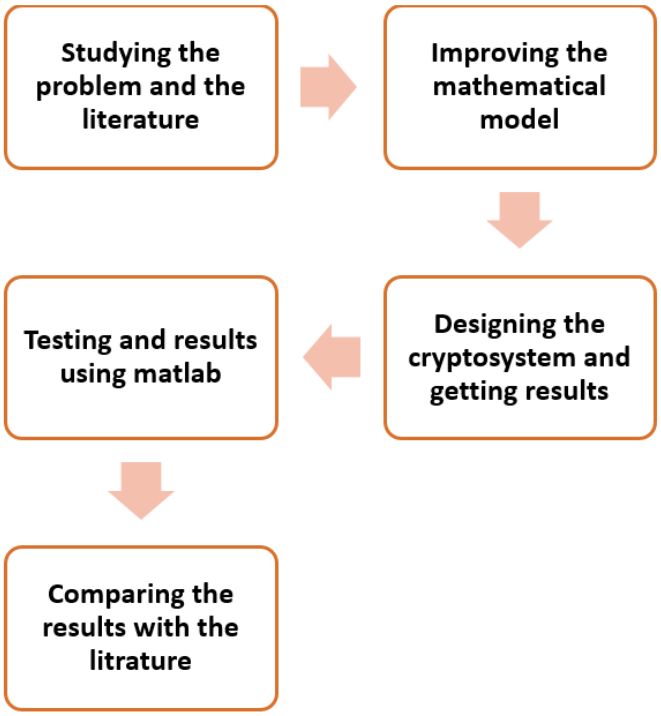
As a result, we chose to work with chaos theory as it has the most powerful and important property required in any cryptosystem which is producing random behaviors as well as many basic properties that can improve the robustness of the cryptosystem and its performance in many ways. In addition, chaotic maps can be used as symmetric or asymmetric encryption algorithms [27].

Also, compared to the classical cryptographic algorithms such as DES, 3DES, AES, etc., with the chaos-based cryptosystems, it was obvious that the chaotic cryptosystems provide several advantages more than the classical ones. They have a very high-security level, a high speed and time performance especially in stream ciphers, they increased the flexibility and the modularity of the system, they have less computational overheads and computational power, and they easier to be implemented. Such features make chaos-based methods more suitable for large scale-data encryption, such as images. Finally, a discredited model was used as a core of the chaos-based cryptosystems using the skew tend map since 2002, thus we decided to start from that weak point to improve the FSTM.

1.2 Contribution

The goal of this thesis is mainly to improve the core of one of the mathematical model of the chaos-based cryptosystems. Many researchers have been using Masudas model [24], since 2002 as the core mathematical model of those chaos-based cryptosystem using the skew tent map. Throughout the years, and after focusing on the chaos-based cryptosystems during the last decade, Masuda's model became a discredited model as the researchers showed many weaknesses in the model such as[28]. As a result, we decided to improve the mathematical model of Masuda to obtain a more robust model that will give us a better security level than the previous models with a faster cryptosystem. Later, depending on the literature review and the study of the researches done inside our university (Palestine Polytechnic University), we tested the cryptosystem against theoretical and statistical attacks to be the first who tested the robustness of our cryptosystem against that number of attacks.

1.3 Research Methodology



1.4 Thesis structure

The remaining of the thesis is organized as follows: the needed information and the background about the thesis content are proposed in Chapter 2. Chapter 3 represents the relation between the chaos theory and cryptography, the properties of the chaotic systems and review about previous systems used the chaos theory. Where Chapter 4 covers the proposed cryptosystem and its mathematical model, with the most important security analysis and their results comparing to the previous work. Finally, Chapter 5 contains the conclusion and the future work.

Chapter 2

Background

Everyone without any special procedures or methods can read implicit information, which is called the plaintext. It is important to protect particular material from the plaintext through a technique called encryption, which makes a message incomprehensible, except to the intended receiver.

Encrypting plaintext gives an indecipherable bunk called chiphertext. Encryption methods are used to guarantee that not intended receivers will not receive the encrypted information, even those who can recognize the encrypted data. On the other hand, the procedure of reverting the chiphertext to its original plaintext is called decryption.

Encryption algorithms during the last decade can be divided into two types according to the encryption scheme used. Encryption schemes are either symmetric which uses one private key for encryption and decryption, or asymmetric uses two keys public and private as shown in Figure 2.1 .

Symmetric encryption algorithms can be subcategorized to stream ciphers, where data is encrypted one bit at a time, or block ciphers where data is partitioned into blocks of fixed sizes and encrypted one block at a time. Data Encryption Standard (DES) [29], Twofish [30], Serpent [31] and

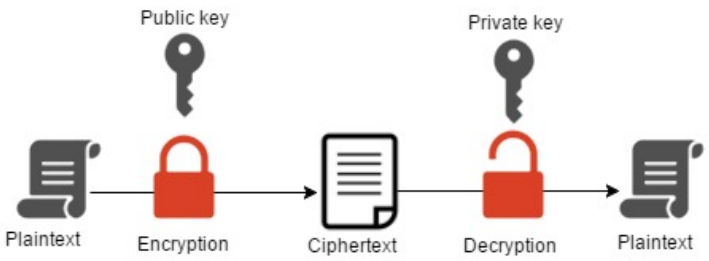


Figure 2.1: Public key encryption

the AES [32] are examples of symmetric block ciphers, where RC4 [33] and Sober-128 [34] are stream ciphers.

On the other hand, asymmetric key encryption algorithms use a public known key to encrypt the plaintext, however, the decryption can only be done by using the private key. On another word, the receivers can safely publish their public keys so anyone can use them to encrypt the plaintext as their private secret key is the only way for receiving the plaintext from the encrypted data. RSA [35] and El-Gamal [36] are the most popular examples of public key encryption algorithms.

2.1 Cryptography

The calculations and the mathematics behind the procedure to encrypt and decrypt data are called "Cryptography". Cryptography is the way to transform data, so that it is secret to all except those who are the intended recipients of the data [37]. Although cryptography is the skill or art of securing data, cryptanalysis is the skill of analyzing a cryptosystem to gain information about the secret key.

A cryptosystem is a five-tuple (P,C,K,E,D), where the following conditions are satisfied [38]:

1. P is a finite plaintexts set;
2. C is a finite ciphertexts set;
3. K, is the key space;
4. For each $K \in K$, there is an encryption rule $e_K \in E$ and a corresponding decryption rule $d_K \in D$.

Each $e_K : P \to C$ and $dK : C \to P$ are functions such that $d_K(e_K(x)) = x$ for every plaintext element $x \in P$.

Cryptography algorithm is a mathematical function utilized to encrypt and decrypt data; the algorithms are categorized into three main categories: symmetric cryptosystem, asymmetric cryptosystem, and cryptography hash function. A cryptosystem is a cryptographic algorithm that depends on certain parameters called keys [39]. The security of encrypted data is completely dependent on two important aspects i.e. the algorithm strength and the key confidentiality.

2.2 Cryptanalysis

Analyzing the cryptosystems and gain information about its secret key is called cryptanalysis, where any information can allow the eavesdropper to breaks the cryptosystem. Generally, breaking a cryptosystem is a term that refers to the ability of the eavesdropper to define the secret key or some information about it (a part of it). Following to Kirchhoffs principle, the eavesdropper has to know everything about the cryptosystem except the secret key.

Eavesdroppers can use many cryptanalysis attacks to know the key, such as; the chiphertext only attack, the known plaintext attack, the chosen plain-

text attack, the chosen chiphertext attack, and the brute force attack. The type of the cryptosystem being attacked determines the type of cryptanalysis, as each attack looks unique; a description of the assumption for each attack is listed in Table 2.1. In addition, it worth telling here, that differential attacks are an example of a chosen plaintext attack while a linear attack is an example of known plaintext attack. [38, 40].

Table 2.1: Descriptions of Cryptanalysis

Cryptanalysis Method	**Information available to the eavesdropper**
chiphertext Only	Has access to the chiphertext only.
Known plaintext	Has a string of plaintext and its corresponding chiphertext.
Chosen plaintext	Has the access to the encryption machine and can choose a plaintext to create its corresponding chiphertext.
Chosen chiphertext	Has the access to the decryption machine and can choose a chiphertext to create its corresponding plaintext.
Brute Force	Does an exhaustive search of every possible key.

Referring to Shannons theory, perfect secrecy means that the attacker can obtain no information about the plaintext by observing the chiphertext. [38] Consequently, perfect secrecy is obtained in cryptosystems if the probability of the plaintext is equal to the probability of the chiphertext [38].

The main goal of cryptanalysis is to define the accepted security of any cryptosystem following the various types of security: computational, provable, and unconditional. As the computational security, measures the computational costs required breaking any cryptosystem, the system will be considered as computationally secure, if breaking it requires at least N computations (N is a very large number). On the other hand, provable security provides a proof of security related to a simpler problem. This is not an absolute proof, but it proves that determining the key is at least as challenging

to break as another problem. Finally, unconditional security is determined by a system that cannot be broken regardless of an infinite amount of computational time and resources, and no cryptosystem can be proven to have unconditional security [38].

It is possible to prove the security against a specific type of attack; however, it does not mean that the cryptosystem is secure for all types of attacks.

To ensure the statistical security of any cryptosystem, we should add many rounds of computations or implementations to the cryptosystem to prevent statistical analysis. Statistical data helps the eavesdropper to define the secret. Shannon in [13] showed that the confusion and the diffusion are the two main principles in encryption, that makes the system more robust against statistical analysis; therefore make a cryptosystem more secure. Confusion is the process that radically changes data from the input to the output; thus, we have to make the relation between the key and ciphertext as complex as possible. On the other hand, diffusion means that a single change in the input characters will change several ones from the output; that is the reason to make the output bits dependable on the input bits in a very complex way, so if we change one bit in the plaintext, the ciphertext will completely change.

2.3 Image encryption

The major thought about image encryption is to carry images safely over the Internet (or any system) so no unapproved clients can decode and see the image. The image information has uncommon properties, such as, mass limit, high severance and high association among the pixels that forces exceptional prerequisites on any encryption procedure [41]. The most well-known system

to secure the advanced images is to shuffle the computerized information so unique message of the records must not be specified, such as instance steganography, packing, advanced watermarking and cryptography.

In fact, image encryption is the methodology of changing data using an algorithm to make it ambiguous, and a structure that cannot be deciphered without the key of decryption. From the other point of view, decrypting images is to recover the actual data from the encrypted structure image.

2.4 Image encryption techniques

2.4.1 Classical image encryption

Advanced Encryption Standard (AES) is a symmetric cryptosystem that proposed for content encryption by Rijmen and Daemen in 1999 [41], which is known as Rijndael algorithm. Scientists used the Rijndael algorithm for image encryption with few changes in key generation and some other requirements, such that, an improved AES algorithm including a keystream generator to guarantee enhancing the encryption execution for image encryption process proposed by Zeghid et al.[42].

An alternative algorithm proposed by Subramanyan et al.[43] focused on the expansion of the AES key, in which the encryption methodology is an XOR operation of a block (set of image pixels) with a 128-bit key that varies for each block. The used keys are produced freely at the sender and receiver side.

The DES is another common block cipher algorithm that uses a 64-bit key. An alternative cryptosystem for image encryption proposed by Qian Gong-canister et al.[44] conjoined the DES with a chaotic map introduced to enhance the security and develop the key space. The results explained that

blending a word-based cryptosystem with different strategies will adequately enhance the security and against anti-attack capacity of those algorithms.

2.4.2 Public Key Image Encryption

Mostly, the application does not guarantee a secure channel to transfer the private key, so we need to utilize public key cryptography. In the first place, Diffie and Hellman spread the technique of public key encryption in 1976 [45]. The main reason for this technique is to import the secret key over a verified correspondence channel without using a former imparted secret key.

Another public key system focused on Chebyshev chaos map proposed by K. Ganesan et al. [41] for colored images encryption. At the beginning, they tried to cryptanalyze the encryption done using a Chebyshev polynomial map, which showed that it is not powerful on few attacks, so they improved the security of this map by using a non-Xoring hash function to secure it against the attack of known plaintext.

While another image encryption technique using ECC was proposed by K. Gupta et al. [46] by transforming every pixel into the elliptic arc point to encrypt the plain image. They only suggested a framework, and experiments done with a simple elliptic arc function with few points, so it is not an appropriate system, but as an innovative idea, results gave the sufficient encryption time in contrast with the traditional public key techniques such as RSA.

2.4.3 Selective Encryption

A methodology that is offered for the reason to encrypt a part of the image instead of encryption the whole image is called selective encryption also acknowledged as partial encryption, perceptual encryption, or soft encryption.

The primary inspiration is to minimize the computation time for real-time applications in which the runtime performance is much serious. The major objective of this technique is to divide the image content into two parts, public and encrypted. One of the most significant features in selective encryption is to decrease the encrypted part to the least as it can be. Maples et al. in 1995 did the first studies about selective multimedia encryption [47] by recommending a mechanism focused on the transferring of the MPEG video and DES cryptosystem to secure MPEG video sequences from insecure access.

A selective encryption way for images is to encrypt 4 to 5 least significant bits, as plaintext attack on such data is harder. Another different method in selective encryption is to extract some special and secret features in an image and encrypt them instead of encrypting the whole image. An idea in this scope is to detect faces of the input image and encrypt them, for some applications such as transmission of images with a guilty, accused persons or members of security organizations or military applications. K. Hong and K. Jung [48] proposed a partial encryption method using the face region as a feature because a face has the semantic information and is the most important part in an image or video.

The selective encryption way that is proposed on our work, is to encrypt the Most two Significant Bit (MSB), as its contribution from the total information in the pixel is 2^7 and 2^6 which means that they have an effect more than the whole remaining bits in the byte [37].

Chapter 3

Literature Review

3.1 Chaos Theory and Cryptography

Chaos hypothesis is the investigation of a nonlinear dynamical frameworks that are affectable to initial conditions and produces random behaviors, proposed by Edward Lorenz in 1963 [49]. Little contrasts in initial conditions, such as those because of adjusting errors in numerical calculation, at the most part yield generally separating results for chaotic systems, while the explanations for long-term prediction are usually intolerable. This happens despite the fact that these frameworks are deterministic, meaning that their future behavior is completely dictated by their initial conditions, with no arbitrary components included. That conclude, the deterministic nature of these frameworks makes them volatile [50].

Applying chaos maps in cipher systems has two general ways according to [51]:

- Using the plaintext or the secret key(s) as the initial conditions and control other parameters then apply some repetitions on chaotic systems to obtain ciphertext corresponding to the block ciphers.

- Using chaotic systems to generate a stream of pseudo-random keys which corresponds to stream ciphers.

This behavior is well known as the deterministic chaos or the basically chaos. Making it an appropriate choice to connect it with cryptography depends on three features; the irregular like behavior, non-anticipating, and affectability to initial value. The main uniqueness is that encryption operations are characterized by limited sets of numbers while chaos maps are characterized by true numbers.

3.2 Security analysis of encrypted image

Security investigation is the specialty of discover the shortcoming of a cryptosystem and recovering the entire ciphered message or discover the secret key without knowing the decryption key or the algorithm. A good encryption scheme should resist all kinds of known attacks, such as known-plaintext attack, ciphertextonly attack, statistical attack, differential attack, and various brute-force attacks [52]. There are numerous methods to investigate what access the expert (hacker) has to the different parts of the cryptosystem such as the key or the plaintext. The following are probably the most widely recognized sorts of assaults on encrypted images:

3.2.1 Statistical Analysis

Regarding Shannon's hypothesis [13], it is possible to solve many kinds of ciphers by statistical analysis, as original and encrypted image relationship can be determined by analyzing data statistically. For this reason, the encrypted image must be totally different from the original one. For an image, there are a few approaches to figure out if the encrypted image reveals any

data about the original one.

3.2.2 Key Space Analysis

The key space is the aggregate number of the diverse keys that can be utilized in the encryption and decryption techniques. For an operational cryptosystem, the key space should be huge to make exhaustion attack unfeasible; as resisting brute force attack requires a large secret key, with at least 128 effective and independent bits based on the available resources these days.

The attempts to discover the decryption key by checking all imaginable keys and the number of attempts to discover the key space of the cryptosystem is called the key space analysis. An encryption algorithm with a 128-bit key size describes a key space of 2^{128}, which takes almost 1021 years with superior computers to check all possible keys. Therefore, a cryptosystem with a key size of 128 effective and independent bits computationally sounds resistance against brute force attacks[53].

3.2.3 Key Sensitivity Analysis

In addition to the wide key space to strengthen a cryptosystem against brute force attack, a protected algorithm must be totally delicate to the secret key which implies that the encrypted image can't be decrypted by any changes might happen in the secret key. Which means that any slight change in the secret key will produce a completely different ciphered image and in other words, one bit different from the correct secret key will never decrypt the image and will give a completely incorrect image [54].

3.2.4 Correlation Analysis

The pixels in the encrypted image should have as low redundancy and correlation values as possible, even though the adjacent pixels in the plain images are very redundant and correlated. The most extreme estimation of relationship coefficient is 1 and the base is 0 considered as the property of an image, where a strong image that has been encrypted to measurable attacks should have a correlation coefficient estimation of 0 [55].

3.2.5 Differential Analysis

This type of analysis focuses on the affectability of the encryption algorithm to any minor changes, in which the attacker can make a little change (e.g. one pixel) in the plain image to watch the results. In strong cryptosystems, the attacker must not have any capacity to discover a compelling relationship between the original and encrypted images. Two criteria, NPCR (number of pixel change rate) and UACI (unified average changing intensity), are usually active to measure the diffusion capacity of an image cryptosystem.

3.3 Basic Properties of Chaotic Systems

The chaos theory has been seen to be involved in many natural and laboratory systems where a considerable number of science such as physics, biology, ecology, electronics, computer science and economy has been used.

Chaos system manages with schemes that develop in time with a specific sort of dynamical action, these types of systems follow some particular laws of evolution, so they are deterministic. It worth telling, that chaos happens only in some deterministic nonlinear systems [56]. Obviously, chaos gives the impression as if there is a nonstop randomly look that is extended to fulfill

certain mathematical standards.

There is a set of features that enclose the characteristics of the chaotic systems, which are the mathematical standards that define chaos. The most appropriate ones are:

3.3.1 Dynamic instability

Regarding [57], the dynamic instability is the property of sensitivity to initial conditions, where two randomly closed initial situations progress with considerably dissimilar and deviating trajectories, which is also mentioned as the butterfly effect.

3.3.2 A periodicity

The system progresses in an orbit that on no occasion replicates itself, where these orbits are never periodic [58].

3.3.3 Topological mixing

Mixing colored dyes can be considered one of the topological mixing as it represented to explain that the system would progress in time so that any specified section of states is constantly converted or overlaps with any other particular section [59].

3.3.4 Ergodicity

A system that exhibits the same behavior averaged over time or space is an ergodic system [60], where time averages are generally taken over one experiment, and space averages are taken over many experiments gave the same parameter value and different initial conditions.

3.3.5 Dense periodic orbits

The system follows a dynamics that can approach every potential asymptotic state in random. Chaotic orbit is described as one that forever continues to experience the unstable behavior that an orbit exhibits near an unstable point, but that is not itself fixed or periodic.[60], unlike periodic orbits, chaotic orbits never repeat the same behavior.

Chaotic orbits are considered dense when they have a disorderly-looking orbit where any initial condition will expand over the entire region of the state space. The orbit of any initial condition will never repeat itself which implies that any orbit will arbitrarily closely approach every possible asymptotic state [61].

3.3.6 Self-similarity

During the progress of a chaotic system, in time or space, self-similarity explains the similar presence at dissimilar scales of observation. This feature makes the system to appear auto repetitive at dissimilar scales of observation [62].

3.4 The connection between Chaos and Cryptography

Chaotic systems are executed with deterministic non-linear dynamical systems (NLDS). While having the ability to deliver the pseudo-randomness property is needed in cryptography, NLDS have the capacity to produce complex configurations of progression, where the base uniqueness in any contribution of the cryptosystems is to give a very distinctive output when a little

change is connected to its introductory conditions or control parameters. [63].

The main components that create the pseudo-random behavior are confusion and diffusion. Confusion is a property, which makes it challenging to see a connection between the plaintext and the cipher text. For chaotic cryptosystems, confusion occurs when the encryption rule and the secret key combination in a way that makes finding a function that maps the two together with a complex and involved process. On the other hand, diffusion makes it harder to process statistical data, as it is inherently connected with sensitivity to initial conditions and control parameters.

The main characteristics of a chaotic system relate directly to what makes a cryptographic system good or secure. Table 3.1 summarizes the connection between chaos and cryptography [64]. This strong connection between chaotic and cryptographic property is what drew researchers to the study of chaos-based cryptosystems.

Table 3.1: Comparison of some properties of Chaos and Cryptography

Chaotic Property	**Cryptographic Property**	**Description**
Ergodicity / self-similarity	Confusion	The output of the system seems similar for any input
Dynamic instability (Sensitivity to initial conditions)	Diffusion with small changes in plaintext/secret key	A small difference in the input produces a very different output
Topological Mixing	Diffusion with small changes in one plain-block of the whole plaintext	Small deviation in the local area causes a large change in the whole space
Structure Complexity	Algorithmic (Attack) Complexity	A simple algorithm that produces highly complex outputs

3.5 Review of Chaos Based Encryption Techniques

Cryptography has two main methodologies. These have been known as, analogue and digital techniques as shown in Table 3.2 [64]. Chaos is a clear

truth that happens in nonlinear determinable systems as the sensitivity for initial conditions, and the pseudo-randomness feature.

Many chaos based cryptographic algorithms are proposed till now and some of them are being used in the way that fits for image encryption and additionally message encryption. An image encryption framework must have a suitable pace for image information ciphering. Therefore, one of the most important benefits of chaotic system's is the simplified key management methodology.

Table 3.2: Different kinds of chaos based cryptosystems presented in literature

Category	**Method**	**Description**	
Analog Cryptosystems	Additive chaos masking	A chaotic signal is added to the message.	
	Chaotic shift keying	A digital message signal,switches among different chaotic systems to be added to the message	
	Chaotic modulation	A message signal is used to change the parameters or the phase space of the chaotic transmitter.	
	Chaotic Control	A message signal is ciphered in a classical way and used to disturb the chaotic system.	
Digital Cryptosystems	Stream ciphers	Chaotic PRNG	A chaotic signal generates a pseudo-random sequence (keystream) to XORed the message.
		Chaotic inverse System approach	A message signal is added to the output of the chaotic signal, which is fed by the ciphered message signal in previous instants.
	Block Ciphers	Backwards iterative	A block of a clear message is ciphered using inverse chaotic systems.
		Forwards iterative	A block of ciphered message is obtained by pseudo-random permutations acquired from a chaotic system.
		S-Boxes	An S-Box is created from the chaotic system. S-boxes can be static or dynamic.
	Miscell-aneous	Searching based chaotic ciphers	A table of characters is generated from a chaotic system. The table is used to cipher the characters of the message.
		Cell. Automata	The chaotic system is a Cellular Automata.

3.6 The Architecture of the Chaotic Image Cryptosystems

The basic architecture of any image cryptosystem is consist of two main phases, namely; confusion and diffusion phases. Permutations of image pixels are prepared in the confusion phase in a secret demand, deprived of varying their values. On the other hand, we use the diffusion phase in cryptosystems to alter the pixel values in sequence so that any small change in one pixel will end up changing several pixels in the output.

The confusion phase is performed n times, where n is usually more than one time, to disassociate the connection among the adjacent pixels in the image, while to achieve a satisfactory level of security, an overall n-round of confusion and a single round diffusion are replicated m times which is typically higher than 1 [37].

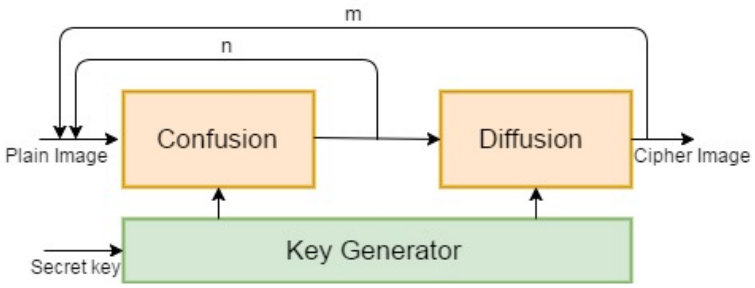


Figure 3.1: Chaos-based Image Cryptosystems Architecture.

3.7 The Selection of the Right Chaotic Map

Chaotic systems are described as being the non-direct and impulsive method. Those systems seem to be irregularly arranged but in reality, there exist a specific arrangement among them. Chaotic systems are sensitive to initial conditions, as any small variation in the initial point may lead to various

results. Chaos has many applications in encryption, modulation, and compression.

For image encryption, logistic maps are easy and have great effectiveness, but on the other hand, they have a weak security and a small key space, where chaotic maps are utilized in image encryption for that reason. In chaos-based algorithm, the correspondence between image pixels is usually reduced to gain a good encrypted image.

We should consider chaotic maps that have the subsequent properties for chaotic systems like mixing, robust chaos and huge parameter set [65], as it difficult to select the right chaotic map for each encryption algorithm.

1. **Mixing:** The mixing property of chaotic maps is frequently attached to the diffusion property in encryption algorithms. It is in other terms, the sensitivity to initial conditions, which indicates spreading out the effect of a single plaintext digit over several ciphers text digits.

2. **Robust chaos:** A straightforward encryption algorithm should expand the effect of a single digit over several digits of the cipher text. On the other hand, the keys of the system and their exchange ways represent many constraints on an encryption algorithm. For that reason, we should conceive those transformations in which parameters and variables are mutually involved in a subtle approach.

3. **Parameter set:** The huge space of parameters in the dynamical system marks that its distinct description will have bigger keys.

3.8 Chaotic Maps Used For Image Encryption

3.8.1 Logistic Map

The one-dimensional logistic map which was proposed in [5], is one of the simplest non-linear chaotic discrete systems that offers chaotic behavior which is defined by equation 3.1:

$$zn + 1 = \lambda zn(1 - zn) \tag{3.1}$$

where z_0 is the initial condition, λ is the system parameter and n is the number of iterations. Based on [5], the map is chaotic for $3.57 < \lambda < 4$ and $zn + 1$ belong to the interval (0,1) for all n. And the sequence generated from the equation has random-like behavior, and used to encrypt the shuffled image.

3.8.2 Tent Map

This map is similar to the logistic map. It produces chaotic sequences in the interval (0,1) assuming the subsequent equation 3.2:

$$Xn + 1 = \begin{cases} \mu Xn & Xn < 0.5 \\ \mu(1 - Xn) & Xn \geq 0.5 \end{cases} \tag{3.2}$$

where μ is a positive number and depends on its value which is found from the tent map showing dynamic behavior ranging from predictable to chaotic.

3.8.3 Arnold Cat Map

This map was named after the mathematician Vladimir I. Arnold, who first illustrated it using a diagram of a cat. Arnold cat map is a two-dimensional invertible chaotic map uses the theory of linear algebra to bring a variation in the position of pixels of original image [66]. The original image is specified as blocks, and then Arnold transformation is completed.

Let X is a vector, $X = \begin{bmatrix} x \\ y \end{bmatrix}$, then Arnold cat map transformation is,

$$\Gamma : \begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} 1 & p \\ q & 1+q \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} mod n \tag{3.3}$$

About conditions such as p and q are positive integers and

$$\begin{vmatrix} 1 & p \\ q & 1+q \end{vmatrix} = 1$$

3.8.4 Circle Map

This map is defined by equation 3.4:

$$Xn+1 = Xn + d - (\frac{c}{2\pi}) sin(2\pi Xn) mod 1 \tag{3.4}$$

where $d = 0.2$, $c = 0.5$, and $x_0 \in [0, 1]$ produces chaotic sequence in the interval [0,1].

3.8.5 Sine Map

Sine map is defined as:

$$Xn + 1 = axn2sin(\pi xn) \tag{3.5}$$

when $x_0 = 0.7$ and $a = 2.3$, the equation will be in the simplified form and will produce the chaotic sequence for the interval (0, 1).

3.9 Chaotic Image Encryption

The properties of the chaos theory consist of the random performance, deterministic dynamics, and non-linear transform and can be used in chaotic image encryption. This theory gives indications to the techniques that can immediately offer security functions and a general visual check, which might be appropriate for some applications.

Digital images are extensively used in numerous applications, such as military, legal and medical systems and those applications that need monitoring access to images and the authorize reliability of images is so important. The stream cipher converts the plaintext bits directly into the ciphertext by XORing them with pseudo-random cipher bits, while block cipher encrypts fixed size blocks that contain a group of bits from the plaintext [37]. Block encryption is more susceptible to cryptanalysis attacks than stream cipher because of identical blocks of plaintext yield identical blocks of ciphertext[67].

Tables 3.3, 3.4 below shows a review of the block and the stream ciphers image encryption schemes:

Table 3.3: Chaotic Block Encryption Scheme

CHAOTIC BLOCK ENCRYPTION SCHEMES			
#	**Authors**	**Chaotic map used**	**Short Summary**
1	G. Jakimoski and L.Kocarev (2001)	Exponential and logistic maps	A chaos-based cipher uses block encryption procedure.The two chaotic maps, exponential and logistic, are respectively defined on the unit interval by $x \to a^x \alpha x \bmod 1$ and $x \to 4x(1-x)$.
2	Y.B. Mao, G. Chen, S.G. ban (2004)	2D baker map	3D baker map is an extension of the 2D baker map; it is used to compose a fast and secure image encryption scheme.
3	H. Gao, Y. Zhang, S. Liang, and D. Li (2006)	A new non-linear chaotic algorithm (NCA)	This scheme uses power function and tangent function instead of linear function. The authors did an experimental analysis to get the structural parameters. They designed an image encryption algorithm based on one-time-one-password system.
4	S. S. Maung, and M. M. Sein (2008)	Logistic and 2D standard map	The authors proposed a fast chaotic-based encryption scheme. Using the logistic map and the 2D standard map, they formed a 8x8 S-Box, then a sequence of pseudo random bytes is generated by using the 2D chaotic cat map to index the entries of the S-box. The output bytes from the S-box are XORed with the plaintext to produce the cipher text.
5	M. Ahmad and Ni S. Alam (2009)	2D cat map and logistic map	The plain image here is decomposed into 8x8 size blocks and then using the 2D cat map, a block-based shuffling of image is carried out. Later, the shuffled image is encrypted using chaotic sequence generated by one-dimensional logistic map.
6	F. Wang, Y.Zhang and T.Cao (2009)	logistic map	This technique produces a chaotic-based stream on logistic map. The system parameter of the logistic map is generated by m-sequence; it also uses another m-sequence's perturbation to raise the period of logistic mapping sequence. The system also provides an output feedback mechanism.

Table 3.4: Chaotic Stream Encryption Scheme

CHAOTIC STREAM ENCRYPTION SCHEMES			
1	1 Yen, and J. Quo (2000)	Chaotic binary sequence	This paper proposed an image encryption/decryption algorithm with its very-large-scale integration (VLSI) architecture. The gray level of each pixel is XORed or XNORed bit-by-bit to one of the two predetermined keys. The proposed algorithm has a low computational complexity, high security, and no distortions.
2	P. Pt and Y. Chen (2003)	2D map	The authors here used a known chaotic dynamical system to generate a pseudo-random bytes sequence, and later applied an appointed permutations to them, using a discredited version of another two-dimensional chaotic map.
3	Socek D et. al. (2005)	Piecewise linear chaotic map (PWLCM)	The authors enhanced the chaotic key-based algorithm (CKBA) proposed by [68] as follows: 1. Replacing the 1D chaotic Logistic map with a piecewise linear chaotic map (PWLCM) to improve the balance property. 2. Increasing the size of the key to be 128 bits. 3. Adding two more cryptographic primitives and extend the scheme to operate on multiple rounds so that the chosen/known plaintext attacks are no longer possible. The new cipher has a stronger security and its performance characteristics remain very good.
4	D. Rao and K Gangadhar (2007)	Piecewise linear chaotic map (PWLCM)	The authors here proposed another algorithm to enhance the security part in the chaotic key-based algorithm (CKBA), where they analyzed the security through cryptanalysis.
5	H.E.H. Ahmed, ILM. 'Calash, and O.S.F. Allah (2007)	Logistic map	The proposed method in this paper is based on the chaotic logistic map and an external secret key of 256-bit. The system has additional features such as: the use of data-dependent iterations, data-dependent inputs, and the inclusion of three independent feedback mechanisms.

6	S. Liu, 3.Stra, Z.Xu (2009)	Logistic map	The proposed system in this paper consists of a keystream generator, which generates random numbers XORed with the plaintext in a binary format.
7	A Awad, A.Saadane (2010)	Piecewise linear chaotic map (PWLCM)	The authors of this paper compared the performance of the logistic and piecewise linear chaotic map with their performance when they are boosted by a new technique proposed by the authors. Later, the four chaotic maps are used to control three-bit permutation methods to have good inherent cryptographic properties.
8	Ai-hongZhu, Lia L (2010)	Logistic map	A new algorithm is proposed in this paper to produce nine chaotic sequences using only one secret-key. Six sequences were used to change the position of the image pixels, and the others were used to confuse and diffuse the image pixels value.

Matthews suggested the first chaotic encryption algorithm in 1989 [17]. Later, researches on chaos-based encryption increased, Baptista [65] completed one of these primary studies. A simple one-dimensional logistic map was used to encrypt each character of a text message as the integer number of iterations achieved in the logistic equation.

Ge Xin et[69] attempted to examine Baptista cryptosystem and concluded that it has two imperfections; the encryption speed is average in correlation with other cryptosystems due to essential number of iterations, on the other hand, this system is not robust to known-plaintext attack, however, it was the outset of using chaos theory in cryptography. The authors of [70], grouped

the chaotic image encryption into spatial and frequency domain, where in spatial they deal with images as it is. However, in a frequency domain, they deal with the rate at which the pixel values are changing in a spatial domain.

Fredric in 1997 [71], [72] proposed the first chaos-based image cryptography. Researchers focused more on chaotic image encryption by using different chaotic maps to overcome the traditional cryptosystem disadvantages, and it worth telling that this technique was a sufficient way for image encryption due to the speed and the strong security.

On the other hand, the authors of [73] used a one-dimensional chaotic equation alternative map that can be used for twofold image encryption with the probability of consuming a huge number of keys. Later, Z. Han et al. in [74] proposed a non-linear map which is used for duplicating pixel values. Where the authors of [75] utilized three different chaotic maps for image encryption. The authors spread the 2D cat map on 8×8 blocks of an image to achieve the shuffling of the pixels and used the 2D coupled logistic map to produce control parameters of shuffling. Later the shuffled image is encrypted by 1D Logistic map; thus, there was no data leakage from encrypted image.

Finally, three encryption algorithms named as Triple-Key chaotic proposed by [76] in 2011. Those keys are an initial parameter key, 80-bit session key and control parameter key. The work was a combination between [77] and [78] which focus around the logistic chaotic map and chaotic neural network.

3.10 Chaos Based Image Encryption Techniques

3.10.1 Multi Chaotic Systems Based Pixel Shuffle For Image Encryption, 2009

The authors proposed a new pixel shuffle technique with multi chaotic systems for image encryption. The chaotic systems are extremely sensitive to initial conditions and system parameters, and have an enormous key space. The designed method in this paper, combined four chaotic systems with the pixel shuffle which can completely displaced the outlines of the original image, and massively declined the probability of exhaustive attacks. The correlation coefficient, NPCR, and UACI to test the security analysis. They showed examples to highlight the confidential encrypted images and to determine a good potential in the application of the image encryption with digital color [79].

3.10.2 An Improved Image Encryption Algorithm Based On Chaotic System, 2009

Shuboo Liu, Jing Sun, and Zhengquan Xu offered in this paper an encryption algorithm using the chaos-based encryption by focusing on the logistic map. The experiment in this paper depends on coupled chaotic maps that support the efficiency of the method, gives an enormous key space and advanced security. They used the stream-cipher structural design in their proposed system, where two chaotic maps, allocating the resolution of stream generation and random mixing, make the pseudo-random keystream generator (PRKG).

Statistical analysis on the cryptosystem are specified, they tested the

correlation coefficients in the vertical and horizontal dimensions, and the key sensitivity attack as well. The systems throughput showed that the system is practical for fast real-time encryption applications [80].

3.10.3 Cryptanalysis of a Multi-Chaotic Systems Based Image Cryptosystem, 2010

In this paper, the authors predicted the proposed method for image encryption by testing newly recommended image cryptosystem against two separate attacks. The main blemish of the proposed cryptosystem came from the result of merging the utilization of the same rearranging methodology for each simple image. In addition to the outcome of utilizing the same sequences created by the four chaotic systems.

The cryptosystem suggested mixing the bits of the plaintext image to utilize a chaotic system, and the cycles of four 3D chaotic systems produces the rearranging of the parameters, while the key of this cryptosystem is the positioned of 12 starting conditions for the chaotic maps. The parameters of the chaotic systems are permanent and unrestricted, and the shuffling is done in two stages: only the designated bits of all the pixels are shuffled in the first stage, while the bits of each pixel are shuffled among themselves in the next stage. In this method, the original plaintext is $m \times n$ RGB image where each pixel color is represented as a byte. Using the usual row scan, the plain image is transformed into a vector for the sake of encrypting it. The resulting vector is $N \times 1$ of bytes, where N = mn. In order to manipulate the bits of pixels, the vector is further split into its bits, resulting in an $N \times 8$ plaintext matrix, where each entry takes values 0 or 1 [81]. On the other hand, the rearranging is done in two stages as well, by rearranging the assigned bits of every last one of pixels in the first stage and in the second stage the bits of

every pixel are rearranged among themselves.

3.10.4 A Modified Image Encryption Scheme Based On 2D Chaotic Map, 2010

The proposed image encryption scheme Rashidah Kadir, Rosdiana Shahril, Mohd Aizaini Maarof here is designed as an external secret key as the one used by Chen et al [52] for image encryption and by Pareek et al [82] for text ciphers. This key is consists of 80-bit and two chaotic logistic maps that are engaged together.

In the proposed algorithm, the first logistic map is used to generate numbers between 1 to 24, in where they might be repetitive. The initial conditions of the second logistic map are improved from the numbers produced by the first logistic map. By adjusting the initial condition of the second logistic map accordingly, its dynamics gets additionally randomized [83].

In this paper, they only calculated the correlation coefficients and the information entropy to evaluate their cryptosystem.

3.10.5 New Image Encryption Algorithm Based On Arnold and Coupled Chaos Maps, 2010

Yunpeng Zhang et. al suggested another innovative algorithm that focuses on multi-digital image chaotic encryption systems, that used the Arnolds map to replace pixels, and recalled the Logistic map to generate a chaotic sequence. The paper tested an algorithm that can rapidly encrypt and decrypt digital images, with good outcomes. The testing of the algorithm's security verifies that the algorithm has a high sensitivity towards the key, has a sufficient key space and the encrypted pixel value is evenly distributed, and likewise. [84].

3.10.6 Image Encryption Based On Diffusion and Multiple Chaotic Maps, 2011

The authors of this paper suggested a secured image encryption technique using multiple chaotic based circular mapping. Two separate sorts of examining strategies that are used in this paper and their performances broke down.

A pair of subkeys in this algorithm was given by using the chaotic logistic map, were one of them is used to encrypt the image and in its transformation leads to the diffusion process. On the other hand, four different chaotic maps generate the other subkeys. Regarding the initial conditions, each map used in the algorithm may produce different random numbers. Among those random numbers, a particular number is selected to be the key for the encryption algorithm.

The proposed image encryption algorithm in this paper has a good peak signal to noise ratio (PSNR), less cross correlation, and key-dependent pixel value replacement. The system is a symmetric key encryption uses a very large number of secret keys. [85]

3.10.7 Image Encryption Based On the General Approach for Multiple Chaotic Systems,2011

Qais H. Alsafasfeh and Aouda A. Arfoa proposed a new technique for image encryption that focused on a new chaotic system by accumulation the Lorenz and the Rssler chaotic systems. After experimental testing they proved that the image encryption algorithm has a large key space and high-level of security [86]. They tested in the paper, the correlation coefficient and the key space analysis.

3.10.8 The Chaotic Feature of Trigonometric Function and Its Use for Image Encryption, 2011

Trigonometric function is the most essential and a mandatory function in nature, as it is has many great features in encryption field. Indeed, not the majority of the trigonometric functions can be used in cryptography, as the encryption feature of a trigonometric function is controlled by the parameters. Chenghang Yu, Baojun Zhang and Xiang Ruan [87] proposed the chaotic features of trigonometric function, and proposed another algorithm focused on that trigonometric function to get a quick and secure image encryption. The function was used as a mask to confuse the plain image and to shuffle the image pixels.

Trigonometric functions increase the resistance to statistical and differential attacks, also the results of the statistical analysis, correlation coefficient analysis and key sensitivity tests showed that the algorithm is secure and practicable. In this technique image encryption is a complicated chaotic system that uses the boundary property of trigonometric function for image encryption [87].

3.10.9 A Novel Image Encryption Scheme Based On Dynamical Multiple Chaos And Baker Map, 2012

An encryption algorithm consisting of two stages were presented in this paper. First, the authors used the Baker map, to permute the locations of the original image pixels, and then encrypt the permuted pixels using multiple chaotic maps. The security analysis done were the sensitivity analysis, numerical analysis, and information entropy. Those tests showed that the proposed encryption system is secure taking into account the most widely

recognized attacks.

The investigational consequences showed that the image encryption technique used had an advanced security against statistic attacks and more sensitive to the secret key [88].

3.10.10 New Image Encryption Algorithm Based On Logistic Map and Hyper-Chaos,2013

A new image encryption algorithm focused on logistic map and hyper chaotic systems was proposed by the authors of this keys, where two types of keys were formed by using the logistic chaotic iteration and hyper chaotic systems, both are used in the image encryption process.

The simulation results of the experiment showed the systematically spreading ciphered pixels, the large key space, the minor correspondence of neighbor-ciphered pixels (correlation coefficient), and the key sensitivity. For that reason, the algorithm is more or less probable in the field of image secure storage and image secure correspondence [89].

3.10.11 Digital Image Encryption Algorithm Based On Chaos and Improved DES, 2013

Rajinder Kaur et al. work was focusing on the chaotic encryption, and to enhance a better quality of the DES encryption where the arrangement of image encryption algorithm is used to discover the gaps. The Logistic map was used in this paper to generate a pseudo-random, which could create twice within the encryption time, thus enhancing the DES. Merging Chaos with the enhanced DES created a more secure algorithm, more rapid and more appropriate for digital image encryption [90].

3.10.12 Benchmarking AES and Chaos Based Logistic Map for Image Encryption,2013

The authors of this paper proposed a classical cryptosystem that focuses on the AES and the chaotic logistic map .The reason of this effort is to analyze the security eligibility of the both cryptosystems and to evaluate the speed of both algorithms. The effectiveness of the two image encryption techniques have been connected twice, once with the AES algorithm and then with the chaotic map.

The study showed that the AES algorithm offered a better security performance, but slower regarding the encryption running speed. On the other hand, because of the computational cost, and the easiness of implementation the logistic map is more substitute for image encryption in real-time correspondence [91].

3.10.13 A RGB image encryption algorithm based on total plain image characteristics and chaos, 2014

The authors in this paper, presented a color image encryption algorithm based on the plain image characteristics to resist a chosen and known plain image attack, and a 1D logistic map with to get a faster encryption process based on Murillo-Escobar's algorithm [92]. Dimensional chaotic maps have some drawbacks to be used in encryption as their data distribution is not uniformed, their periodicity is relatively short, and have small key space. Thus, the authors used the 1D logistic map, as it has many powerful advantages such as the simple structure and the ease of implementation, and they are ideal for fast encryption. The security analysis confirms that the RGB image encryption is fast and secure against several known attacks; therefore, it can

be implemented in real-time applications where a high security is required.

A robust and fast color image encryption was presented in this paper; the pseudorandom sequence for encryption process is based on the plain image characteristic and a 128 bits secret key [93].

3.10.14 A novel chaos-based image encryption algorithm using DNA sequence operations, 2016

The image encryption algorithm proposed in this paper, is based on a chaotic system and deoxyribonucleic acid (DNA) sequence. The plain image is first converted to a DNA matrix, and then a new wave-based permutation scheme is performed on it. The initial values and parameters of the chaotic system are the hashed of the plain image. Later, a row-by-row image diffusion method at a DNA level is applied to the matrix.

The chaotic map are used to generate a key matrix that is used to merge the confused DNA matrix; and then the initial values and system parameters of the chaotic system are updated by the hamming distance of the plain image and finally decoded the diffused DNA matrix, to get the ciphered image.

Experimental results and security analyses confirmed that the proposed scheme has a good encryption effect, larger secure key space, and it is sensitive to the secret key and to the plain image. In addition, it can resist the differential attack, entropy attack, known-plaintext and chosen-plaintext attacks which showed that the algorithm is suitable for digital image encryption [94].

Chapter 4

Proposed Solution

4.1 Overview

Our proposed system is done based on the Finite State Tent Map (FSTM), in which its mathematical model was introduced by Masuda et. al. in [24, 95] as shown in equation4.1

$$F_A(X) = \begin{cases} \left\lfloor \frac{256}{A} \times X \right\rfloor + 1 & 1 \leq X < A \\ 256 & X = A \\ \left\lfloor \frac{256 \times (256 - X)}{256 - A} \right\rfloor & A < X \leq 256 \end{cases} \tag{4.1}$$

where

$$X_1 = \left\lfloor \frac{A \times Y}{256} \right\rfloor \tag{4.2}$$

and

$$X_2 = 256 - \left\lfloor (1 - \frac{A}{256}) \times Y \right\rfloor \tag{4.3}$$

Q here is the block size, and it is equal to 256. And $X, A, Y \in \{1, 2, 3...Q\}$.

This version excluded the value 0, so the authors shifted the model to include 0 and exclude Q. Still, this model had many drawbacks, such as the division by zero in the equation when A = Q, and some values of the output

decreases the probability of guessing the value of the input [28]. Masuda model became a discredited version, and the last updated and robust model was modified by [28], where $X, Y \in \{0, 1, 2, 3...Q\}$, $A \in \{1, 2, 3...Q\}$ and $Q = 256$ as in equation 4.4.

$$F_A(X) = \begin{cases} \left\lceil \frac{Q}{A} \times (X+1) \right\rceil mod Q & 0 \leq X < A \\ \left\lfloor \frac{Q \times (Q-X)}{Q-A} \right\rfloor + 1 mod Q & A \leq X < Q \end{cases} \tag{4.4}$$

And for this reason, we started our modifications from Farajallah's model.

4.2 Proposed Cryptosystem

4.2.1 Proposed Equation

Our proposed mathematical model is shown in equation 4.5

$$R_Q(X) = \begin{cases} \left\lceil \frac{Q}{A(X-1)} + \frac{Q(A+1)}{X} \right\rceil mod Q & 0 \leq X < A \\ \left\lfloor \frac{Q \times (Q-X)}{\frac{1.5}{Q-A}} \right\rfloor mod Q & A \leq X < Q \end{cases} \tag{4.5}$$

where $X, Y, A \in \{0, 1, 2, 3...Q-1\}$ and $Q = 257$.

Following to the study of Equation 4.1, and its improvement in [28], the domain of the output seemed to be concentrated around several values, so we added another part for the first interval of the equation ($\frac{Q(A+1)}{X}$) to make sure that the domain will be more distributed in the proposed equation. Thus, to distribute that data in the right way, we added another fraction with many changes where we calculated the encryption quality and the information entropy for the proposed model by each change. The values started to increase and after $\frac{Q(A+1)}{X}$, the values became to decrease, so we stopped at that point

so we will not lose any information from the image. We also deleted the middle interval of Masuda's equation which gives us the same result when A is equal to X. Those changes were done to obtain the following:

1. **A better key space**

   After studying the range of the key space in [24, 28], we found that the only active bits in the key space are 66 odd values out of the 256, which makes it weak, as for some values its easy to guess the input value. On the other hand, the model doesn't reach the perfect secrecy, as the key space is not equal to the plaintext space and not equal to the ciphertext space as well, which is proposed in their model to be equal to 256.

   In number theory, a and b are said to be relatively prime, or co-prime if the only positive integer that divides both of them is one. Thus, their greatest common divisor being 1 [96]. To increase the security level of the model, A and Q have to be co-prime. Pointing to the models of [24, 28], when Q=1, with $X, Y, A \in \{0, 1, 2, 3...Q\}$, the key space will contain only: $A = \{51, 53, 55, , 117, 139, 141, 143, , 201\}$ that are the cop-rime to 256 that counts 66 active bits in the key space.

   Following the same concept, we suggested Q to be 257 instead of 256 to increase the security level. Depending on the fact that 257 is a prime number, $A \in \{0, 1, 2, 3...Q - 1\}$ will give us 256 active bits in the keys space as all the numbers under 257 are co-prime with it, which in the same time will decrease the probability of guessing any input from the output value.

2. **A secure model against theoretical attacks**

   Masuda's model had an interval that made it easy to make the possibilities less when guessing the input value. As the output is always 256 when X=A. Thus, by increasing the possibilities of guessing the output, the cryptosystem is considered more robust against the theoretical attacks. Depending on that point, we merged X=A to the second interval of our proposed mathematical model.

3. **To have a more uniformly distributed domain**

   The strength of the cryptosystems output is directly proportional to the distribution of its domain. As the main goal of our thesis is to obtain a stronger core model for the chaotic systems, we changed the model in [28] to be as distributed as possible. Depending on the evaluation of the results, our model gave a better distribution domain than the previous models of Masuda[24], and Farajallah [28]. The result of the information entropy analysis and the encryption quality analysis that are shown in the section of the security analysis, shows that our system has a better-distributed domain than the previous models the nearer to the uniformly distributed domain among others.

It worth telling here, that we are going to reproduce the whole security analysis that will be done for our proposed cryptosystem for Masuda [24], and Farajallah [28] to compare the results with our results.

4.2.2 Cryptosystem design

Our proposed cryptosystem is based on a hybrid encryption scheme that combines both stream and block ciphering algorithms to achieve the required security level, with a minimum encryption time. Both stream and block

ciphers in cryptography belong to the family of symmetric key ciphers in which we use the same key for both of the encryption and the decryption processes.

The stream cipher converts the plaintext bits directly into the ciphertext by XORing them with pseudo-random cipher bits, while block cipher encrypts fixed size blocks that contain a group of bits from the plaintext [97]. The stream cipher has a higher speed of transformation and a low error rate, as an error that occurs in one bit will not affect the other bit. The block cipher has a high level of diffusion which any block effect will be spread into several blocks. On the other hand, the diffusion effect is low in the stream cipher, as all information of the plaintext is contained in a single ciphertext symbol. The block cipher has low encryption speed, as the entire block must be accumulated before the encryption or decryption process starts. Furthermore, the entire block here may corrupt due to an error in one bit.

In our cryptosystem, we divided the image into several numbers of blocks with a block size of 256 and encrypted it block by block to minimize the error bits. As shown in Figure 4.1, using the CBC mode in our cryptosystems, which is a confidentiality mode as it chains (combine) the plaintext block with the previous ciphertext block. The CBC mode requires an initialization vector to combine it with the first plaintext block which is generated in our system by the chaotic generator.

Our proposed algorithm encrypts the whole image using Alg_2 and Alg_3 shown in Figure 4.1, it encrypts the odd and the even blocks using different algorithms as shown in Figure 4.2. Alg_2 encrypts the odd blocks based on our model R_Q-FSTM as shown in Figure 4.3, where the substitution and the permutation are done in one step to decrease the encryption time. As in Figure 4.4, Alg_3 encrypts the even blocks usisng a selective substitution based

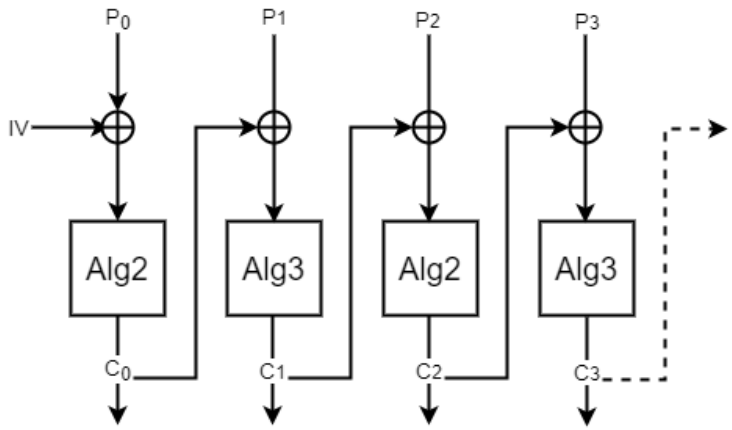


Figure 4.1: The proposed algorithm encryption process

on R_Q-FSTM to decrease the time and to increase the encryption quality in the same time.

Afterward, the diffusion and confusion effects in our cryptosystem are transferred between blocks using the Cipher-Block Chaining mode (CBC) [98]. It worth telling as well, that the model (equation number) was implemented based on a look-up table to decrease the encryption time. The input of this look-up table is the generated dynamic key from the implemented version of El Assad et, al. [98] chaotic generator, in addition to the byte from the plaintext.

Algorithm 1: Encryption Process
Divide image into n blocks 1- For odd blocks call Algorithm 2 2- For even blocks call Algorithm 3

Figure 4.2: Algorithm 1: The Encryption Process

Algorithm 2: Odd Blocks

For i=0: 1 to Block size
1- Calculate the new position of the block (posn)
2- Permutation and substitution for data at posn
Block [j][posn]=Block[j][i]⊕Key
3- Update the Key
Key=lookup(Key, Block[j][posn])
End i

Figure 4.3: Algorithm 2: Odd Block Encryption

Algorithm 3: Even Blocks

For i=0: 1 to Block size
1- Calculate the new position of the block (posn)
2- Perform permutation and selective substitution for data at posn
DataByte[j][posn]= the most 2 significant bits of the
DataByte[j][posn] ⊕ the least 2 significant bits of the dynamic key
3- Update the Key
Key=lookup(Key, Block[j][posn])
End i

Figure 4.4: Algorithm 3: Even Block Encryption

El Assad chaotic generator was implemented to avoid the weakness in the chaotic systems regarding periodicity-generating sequences. This generator consists of two chaotic maps, i.e., the Skew Tent Map (STM) and the discrete Piece-Wise Linear Chaotic Map (PWLCM), in which are connected in parallel to generate the sequence values of 32-bit samples [37].

Following the Figure 4.1, P_0 represents the first plain block, the IV is the initial vector that is generated by El Assad generator [98], and C_0 is the ciphered block.

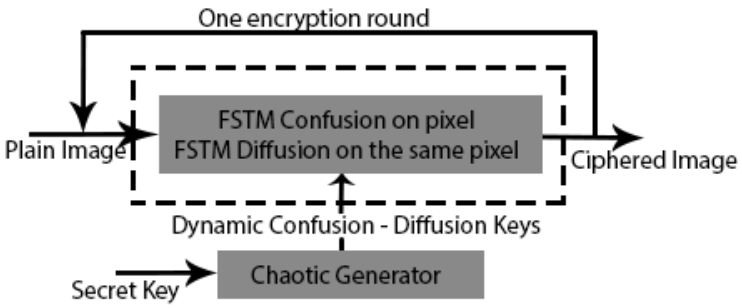


Figure 4.5: General block diagram of the proposed cryptosystem

4.3 Security Analysis

To design and develop a chaos-based cryptosystem, the system should be suitable and efficient for the target application, achieve the degree of the security level, and not to consume time or memory. It should offer the required security level. Analyzing the complexity of any cryptosystem is an important assessment factor. Researchers typically take this evaluation as the time of encryption/decryption, however, measure that is more comprehensive are needed to evaluate the cryptosystem.

4.3.1 Theoretical analysis

Key space

Resisting the brute force attack needs a large secret key, with at least 128 effective and independent bits. Depending on that fact, our proposed cryptosystem is robust against the brute force attack as it has a secret key with 169 bits. And a dynamic key that consists out of 8 bits that are changeable and unique for each new block, and have been chosen out of 257 active values.

Ciphertext only attack

In this theoretical attack, a group of ciphertexts is available to the attackers, where they try to find the corresponding plaintexts. Where the complexity to resist such an attack is based on the available amount of the ciphertexts. This type of attack is facilitated when the attacker has multiple pieces of ciphertext generated from the same key.

Known plaintext attack

In this attack the attackers have a group of plaintexts and a group of corresponding ciphertext as well, where they try to get the secret key.

Chosen plaintext attack

The attackers here have the access to the system itself without knowing the secret keys. Then, he has the possibility to choose a plaintext message and to encrypt it.

Chosen ciphertext attack

The attacker chooses the ciphertext and obtains the corresponding plaintext using the decryption system, without knowing the secret key. In this type of attack, the attacker's objective is to find the secret key.

4.3.2 Statistical analysis

plaintext sensitivity attack

Depending on the diffusion definition, any slight change in the plain image, even a change of a single bit, should statistically, change one bit out of two

of the cipher image, and similarly, if we change one bit of the cipher image, then approximately one half of the plain image bits should change.

We selected two plain images to be encrypted using the same secret key and have a difference in one bit in the first block. Most probably, the researchers chose the first bit in the image to be the different one, but we chose another scenario the chosen bits will be located in the beginning, in the middle, and at the end of the first block so as to get closer results to the real application.

The Unified Average Changing Intensity (UACI), and the Number of Pixels Change Rate (NPCR) are the two parameters used to measure the resistance to the plaintext sensitivity attack [99, 100].

$$UACI = \frac{1}{L \times C \times P \times 255} \times \sum_{p=1}^{P} \sum_{i=1}^{L} \sum_{j=1}^{C} |C_1 - C_2| \times 100\% \tag{4.6}$$

$$NPCR = \frac{1}{L \times C \times P} \times \sum_{p=1}^{P} \sum_{i=1}^{L} \sum_{j=1}^{C} D(i,j,p) \times 100\% \tag{4.7}$$

In equations 4.6 & 4.7, i, j and p are the row, column, and plane indexes of the image, respectively. While L, C and P are the length, width, and plane sizes of the image. D(i,j,p) = 0 when it is the same value in C_1 and C_2 while it is 1 when it is different. Table 4.1 presents the results of the plaintext sensitivity attacks of our proposed cryptosystem for the image Lena 512×512, where the optimal value for UACI is 33.46% and for NPCR is 99.61% which are given in [99, 100].

Table 4.1: Plaintext sensitivity tests for the proposed cryptosystem

Test Name	**Image Name**		**Masuda**	**Farajallah**	**Qumsieh**
Plaintext Sensitivity Attack	Lena 256	NPCR	99.614939	99.381388	99.275431
		UACI	33.456859	33.411513	33.386265
		HD	0.499860	0.499240	0.498203
	Lena 512	NPCR	99.609308	99.543568	99.513695
		UACI	33.448059	33.481259	33.431584
		HD	0.499962	0.499812	0.499354
	Lena 1024	NPCR	99.619961	99.594720	99.494553
		UACI	33.510279	33.454623	33.353363
		HD	0.499922	0.500345	0.499837
	Baboon 512	NPCR	99.608044	99.555897	99.556959
		UACI	33.457006	33.457980	33.436678
		HD	0.499965	0.500007	0.499669
	Boat 512	NPCR	99.611649	99.549033	99.551606
		UACI	33.465358	33.443964	33.456685
		HD	0.500025	0.499524	0.499530

Key sensitivity attack

As well as the changes of the input, any slight change in the secret key will produce a completely different ciphered image [54], on other words, that means that any cryptosystem has to be resistant to this attack. However, changing one bit in the key during decryption o the ciphered image will completely destroy the decryption process; the whole encryption process will fail.

The testing scenario of the key sensitivity is similar to the plaintext sensitivity attacks as well: we have one plaintext P and two secret keys with a

difference of one bit. First, P is encrypted using K_1 to obtain C_1. Then the same P is encrypted using K_2 to obtain C_2. Finally, NPCR and UACI are evaluated to calculate the key sensitivity attack of the proposed cryptosystem. As shown in Table 4.2, our proposed cryptosystem results indicate that the proposed cryptosystem is very sensitive to a one-bit change in the secret key.

Table 4.2: Key sensitivity tests for the proposed cryptosystem

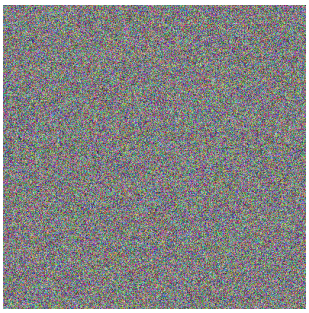
Test Name	**Image Name**		**Masuda**	**Farajallah**	**Qumsieh**
Key Sensitivity Attack	Lena 256	NPCR	99.613413	99.609350	99.608515
		UACI	33.462236	33.467554	33.449413
		HD	0.499990	0.499969	0.499957
	Lena 512	NPCR	99.607698	99.610329	99.611708
		UACI	33.460583	33.466205	33.456402
		HD	0.500048	0.500037	0.500021
	Lena 1024	NPCR	99.607817	99.604034	99.604988
		UACI	33.479417	33.450483	33.408832
		HD	0.499907	0.499670	0.499882
	Baboon 512	NPCR	99.606837	99.608943	99.610943
		UACI	33.457946	33.461276	33.462904
		HD	0.499954	0.499968	0.499973
	Boat 512	NPCR	99.608734	99.608728	99.606537
		UACI	33.462312	33.464436	33.463292
		HD	0.499945	0.500036	0.499959

Histogram analysis

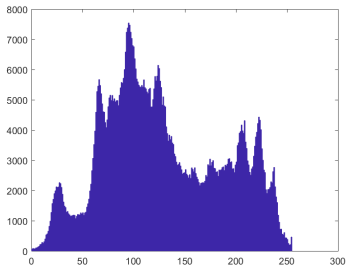
An image histogram is a graphical demonstration that shows a visual impression of the circulation of pixels through scheming the number of pixels

at each grayscale level. This graph shows the number of pixels in an image at each different intensity value and we call it the histogram. For encrypted images, the histogram should be uniformly distributed to be strong against the statistical attacks, where we can benefit from the most used bit in the image and its position to reveal some information about the key.

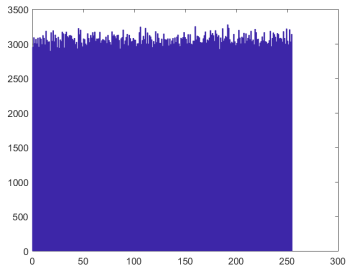
(a) Plain Lena Image



(b) Ciphered Lena Image



(c) Histogram-plain image



(d) Histogram-ciphered image

Figure 4.6: Lena image 512 plain and ciphered with their Histogram

The chi-square test's result ensures whether the ciphered image pixels are uniformly distributed or not, as shown in equation 4.8 :

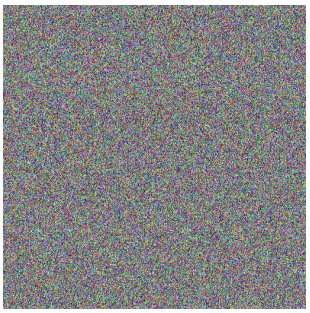
$$\chi^2_{exp} = \sum_{i=0}^{Q-1} \frac{(o_i - e_i)}{e_i} \tag{4.8}$$

where Q is the number of levels (in our model is 256), o_i is the observed occurrence frequencies for each level in the ciphered image and e_i is the expected one from the uniform distribution. In a secure cryptosystem, the

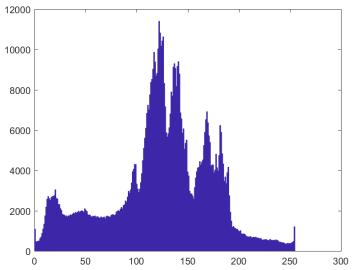
experimental chi-square value have to be less than the theoretical chi-square value, which is 293 in case of $\alpha = 0.05$ which is the level of significance and Q = 256 [101], as: $\chi^2_{exp} < \chi^2_{th}(255, 0.05) = 293$.

The results in Figure 4.3.2, 4.3.2 shows that the tested histograms are uniform and do not reveal any useful information for the statistical analysis.

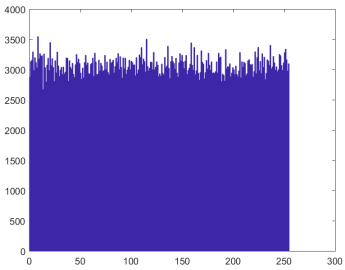
(a) Plain Boat Image



(b) Ciphered Boat Image



(c) Histogram-plain image



(d) Histogram-ciphered image

Figure 4.7: Boat image 512 plain and ciphered with their Histogram

Correlation analysis

Two neighboring pixels in a plain image are intensively corresponded in an extreme estimation of relationship coefficient of 1 and the base is 0 considered as the property of an image. On the other hand, the pixels in the encrypted image should have as low redundancy and correlation values as possible (closer to zero), even though the adjacent pixels in the plain images are very redundant and correlated [55].

To define the correlation in the encrypted images, we calculated the correlation coefficient (r_{xy}) between two horizontally, vertically and diagonally neighboring pixels [102] for 10000 randomly pairs (N) using the equation 4.9

$$r_{x,y} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{4.9}$$

where $cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}([x_i - E(x)]\,[y_i - E(y)])$, $D(x) = \frac{1}{N}\sum_{i=1}^{N}(x - i - E(x))^2$, $E(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i)$ and x,y are the pixel values of the two adjacent pixels in the tested image.

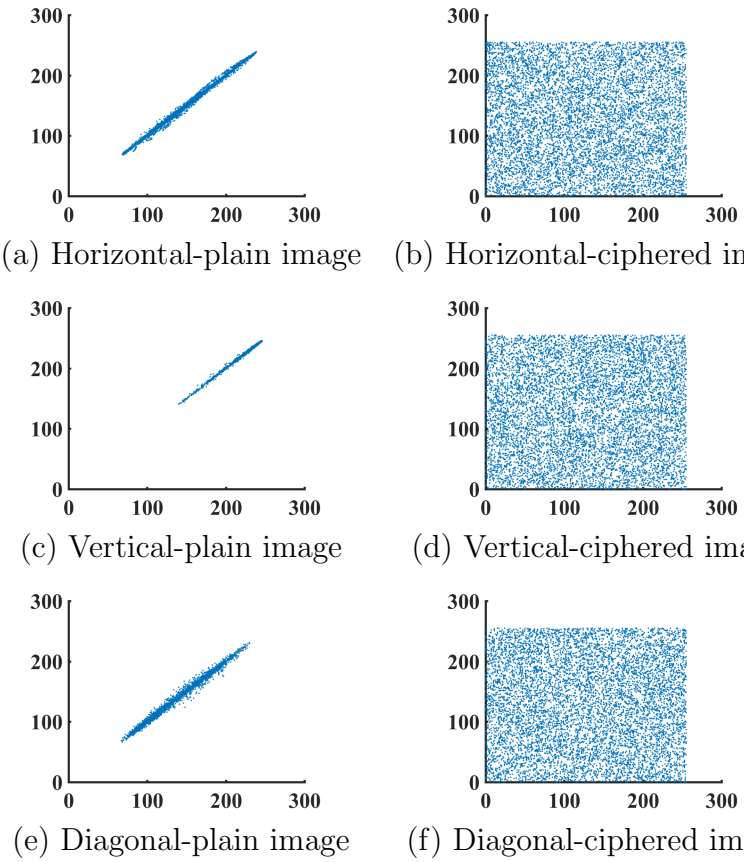
Table 4.3 & Figure 4.3.2 show the correlation results for the Lena image and its corresponding cipher image, which is encrypted by our proposed cryptosystem.

Table 4.3: Correlation analysis of the ciphered images

Test Name	**Image Name**		**Masuda**	**Farajallah**	**Qumsieh**
Correlation Analysis	Lena 256	Horizontal	0.001830	0.004250	0.009787
		Vertical	0.272201	0.342148	0.333790
		Diagonal	0.003502	0.005918	0.002495
	Lena 512	Horizontal	0.001000	0.015139	0.011517
		Vertical	0.054024	0.090599	0.105004
		Diagonal	0.004644	0.007350	0.013922
	Lena 1024	Horizontal	0.016281	0.002321	0.018429
		Vertical	0.014768	0.025720	0.035597
		Diagonal	0.012571	0.038604	0.004533
	Baboon 512	Horizontal	0.012609	0.000482	0.007449
		Vertical	0.041996	0.108608	0.101798
		Diagonal	0.007462	0.014617	0.000394
	Boat 512	Horizontal	0.014435	0.008261	0.000345
		Vertical	0.048885	0.102851	0.124831
		Diagonal	0.004244	0.007714	0.026092

Information entropy

In any image, the values of the pixels are ranging from 0 up to 255. To have a robust algorithm for encrypting, the occurrence probability of any pixel should be almost the same. Thus, the entropy information, which is



(a) Horizontal-plain image (b) Horizontal-ciphered image

(c) Vertical-plain image (d) Vertical-ciphered image

(e) Diagonal-plain image (f) Diagonal-ciphered image

Figure 4.8: Correlation analysis of the plain and ciphered Lena image 512.

calculated using equation 4.10, will evaluate the random behavior of the encrypted message.

$$H(C) = \sum_{i=0}^{Q-1} Pro(c_i) \times log_2 \frac{1}{Pro(c_i)} \tag{4.10}$$

where H(C) is the entropy of the ciphered image C, Pro(c_i) is the occurrence number of each level (i = 0, 1, 2 ... 255). In case of equal probability levels (Pro(c_i) = 2^{-8}), the information entropy is maximal, $H(C) = \sum_{i=0}^{256-1} 2^{-8} \times log_2(256) = 8$ according to the above equation 4.10. Lena image statistics in our cryptosystem, entropy of encrypted image using the proposed algorithm is 7.9996, which is very adjacent to the theoretical value of 8. This shows that the algorithm is secure against entropy attack.

Encryption quality

In cryptosystems, that encrypts images, pixels values as compared to the value of the same pixel before encryption, where those changes may be irregular [103]. Therefore, this means that the higher the change in the pixels values, the more effective will be the image encryption and the quality of the encryption.

Thus, the encryption quality can be defined as the total changes in pixels values between the original image and the encrypted image and the measure for the encryption quality can be the deviation between the original and encrypted image:

$$EQ = \frac{\sum_{i=1}^{N}(|o_i(P) - o_i(C)|)}{256} \tag{4.11}$$

where o_i(C) and o_i(P) are the observed occurrences for the byte level i in the ciphered image C and in the plain image P respectively. As a result, the larger the value of EQ, the higher the level of security of the cryptosystem.

For the need of comparison, it is necessary to estimate the optimal value of EQ. The maximal value of EQ denoted as EQmax [28], $EQ_{max} = \frac{510 \times L \times C}{256^2}$ where L and C are the line and the column of the gray image/frame, and depending on that the ideal encryption quality is 2040. Regarding the Table 4.4 and Figure 4.9, our cryptosystem has a better EQ than the algorithms proposed by [24, 28].

Table 4.4: Encryption Quality Analysis

Test Name	Image name	Masuda	Farajallah	Qumsieh
Encryption Quality	Lena 256	286	288	504
	Lena 512	1170	1178	2023
	Lena 1024	4597	4631	8060
	Baboon 512	1373	1381	2036
	Boat 512	1348	1355	2024

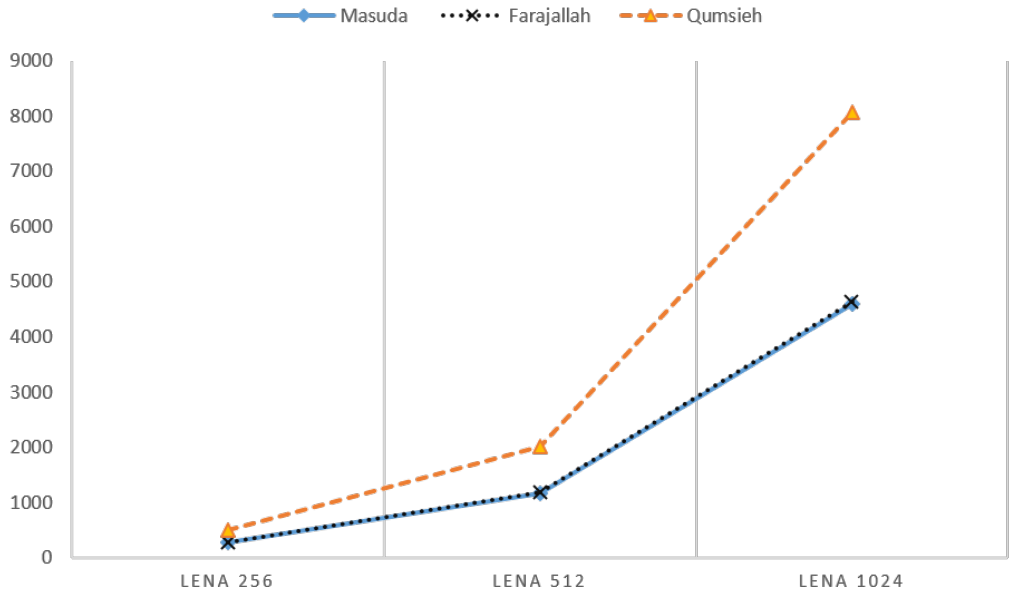


Figure 4.9: Encryption Quality Analysis

Complexity analysis

Calculating the complexity of the algorithm used in the cryptosystem is an important factor that determines the time of performance. On the other hand, the performance can be determined by the running speed of the algorithm or the Encryption Throughput (ET), and the number of cycles needed to encrypt one byte, which is the CPU speed in Hertz divided by the ET in

bytes.

$$ET = \frac{Image_{size}(Byte)}{Encryption_{time}(second)} \tag{4.12}$$

$$Number\ of\ cycles\ per\ byte = \frac{CPUSpeed_{Herts}}{ET_{Byte}} \tag{4.13}$$

The results for the encryption and decryption processes of our proposed cryptosystem are carried out using the Code::Blocks compiler of C programming on a laptop with 2.70 GHz processor Intel $Core^{TM}$ i7-7500U CPU, 8GB RAM, and Windows 10, 64-bit operation system. Lena image colored with 3 different sizes ($(256 \times 256 \times 3$ bytes), $(512 \times 512 \times 3$ byte) and$(1024 \times 1024 \times 3$ byte)), Baboon and Boat images with the size $(512 \times 512 \times 3$ byte) are the image under test. Later, the results were tested again using MATLAB R2017a.

Table 4.5 presents the running speed of the algorithm (encryption time) in milliseconds, compared with the fastest chaos-based cryptosystems.

Table 4.5: Encryption time of different algorithms in millisecond

	Lena 256	Lena 512	Lena 1024
Proposed (Qumsieh)	4.60	18.06	54.35
Zhang 1[104]	7.5	30	120
Zhang 2[104]	7.5	30	120
Wang[105]	7.79	31.16	124.64
Akhshani [106]	14.4	57.6	230.4
Wong[107]	15.59	62.37	249.48
Kanso[108]	97.15	388	1554
Pareek[82]	160	920	5650
Farajallah[109]	6	24	96

To calculate the time performance, we calculated the average execution time for the test image after encrypting them using 1000 different secret keys. Table 4.6 presents the running speed of the algorithm (throughput) in megabyte per second (MBps) and the number of cycles required to encrypt or decrypt one byte. The results are compared to the fastest chaos-based cryptosystems in the literature. Through those calculations, the number of encryption rounds is identified by the required security level.

Table 4.6: Encryption throughput and the number of cycles for each encrypted byte - Lena image 512

	ET in MBps	Number of cycles per byte
Proposed (Qumsieh)	41.52	62
Zhang 1[104]	25	122.07
Zhang 2[104]	25	122.07
Wang[105]	24.06	122.85
Akhshani[106]	13.02	194.83
Wong[107]	12.03	245.7
Kanso [108]	1.93	1121
Pareek [82]	0.39	2445
Farajallah[109]	31.25	94.60

Chapter 5

Conclusion and Future Work

In recent decades, the most important communication is happening through wireless techniques using the internet to transfer data, and the main concerns remain in the subject of the security. Encryption is a unique way to guarantee the security of data.

Various important encryption techniques are presented in the thesis, the outcomes of every algorithm have advantages and disadvantages based on their techniques, which are being practiced on images. In this thesis, we studied the problem of achieving the confidentiality of transmitted images over public channels, by using chaos-based cryptosystems. A STM model was improved in this thesis to be used as the core structure on the proposed cryptosystem that was designed and implemented for real-time applications with a high-security level. A hybrid encryption scheme that has both block and stream cipher algorithms was proposed. This combination achieved a faster cryptosystem than the existing ones in the literature, in addition, it preserves the required security level.

The block cipher is used to encrypt the odd plain text blocks which are implemented by a substitution layer from the R_Q-FSTM and a permutation

layer that is achieved by using the same map as a generator. On the other hand, the stream cipher level is applied by a selective cryptosystem to encrypt the most two significant bits (MSB) of each byte in the even plain text blocks.

Our modified version of the STM used a novel method designed with a confusion and a diffusion layer in order to be simple, fast and robust against theoretical and statistical attacks.

The selective encryption of the MSB requires a better improvement in future work in order to increase the security level of our model while constantly increasing the encryption time, in addition to encrypt the MSB as static or access time without mathematical operations.

Bibliography

[1] Sharkovskiĭ. Coexistence of cycles of a continuous map of the line into itself.

[2] Yoshitsugu Oono. Period= 2^ n implies chaos. *Progress of theoretical physics*, 59(3):1028–1030, 1978.

[3] David Ruelle. What is a strange attractor. *Notices of the AMS*, 53(7):764–765, 2006.

[4] Otto E Rössler. An equation for continuous chaos. *Physics Letters A*, 57(5):397–398, 1976.

[5] Robert M May. Simple mathematical models with very complicated dynamics. *Nature*, 261(5560):459–467, 1976.

[6] AN Zaikin and AM Zhabotinsky. Concentration wave propagation in two-dimensional liquid-phase self-oscillating system. *Nature*, 225(5232):535–537, 1970.

[7] EN Lorenz. Essence of chaos. florence, ky, 1995.

[8] Christos K Volos and Antonios S Andreatos. Secure text encryption based on hardware chaotic noise generator. *Journal of Applied Mathematics and Bioinformatics*, 5(3):15, 2015.

[9] Edward N Lorenz. Deterministic nonperiodic flow. *Journal of the atmospheric sciences*, 20(2):130–141, 1963.

[10] Jiri Fridrich. Symmetric ciphers based on two-dimensional chaotic maps. *International Journal of Bifurcation and chaos*, 8(06):1259–1284, 1998.

[11] Ljupco Kocarev, Goce Jakimoski, Toni Stojanovski, and Ulrich Parlitz. From chaotic maps to encryption schemes. In *Circuits and Systems, 1998. ISCAS'98. Proceedings of the 1998 IEEE International Symposium on*, volume 4, pages 514–517. IEEE, 1998.

[12] Marco Gotz, Kristina Kelber, and Wolfgang Schwarz. Discrete-time chaotic encryption systems. i. statistical design approach. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 44(10):963–970, 1997.

[13] Claude E Shannon. Communication theory of secrecy systems. *Bell Labs Technical Journal*, 28(4):656–715, 1949.

[14] Shu-Jun Li. *Analyses and new designs of digital chaotic ciphers*. PhD thesis, Xi'an Jiaotong University, 2003.

[15] Li Shujuna, Mou Xuanqinb, and Cai Yuanlongc. Pseudo-random bit generator based on couple chaotic systems and its applications in stream-cipher cryptography. In *International Conference on Cryptology in India (INDOCRYPT*, volume 16, page 20, 2001.

[16] Yvo G Desmedt. *Advances in CryptologyCRYPTO94: 14th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21–25, 1994. Proceedings*, volume 839. Springer, 2003.

[17] Robert Matthews. On the derivation of a chaotic encryption algorithm. *Cryptologia*, 13(1):29–42, 1989.

[18] Daniel D Wheeler. Problems with chaotic cryptosystems. *Cryptologia*, 13(3):243–250, 1989.

[19] Toshiki Habutsu, Yoshifumi Nishio, Iwao Sasase, and Shinsaku Mori. A secret key cryptosystem using a chaotic map. *IEICE TRANSACTIONS (1976-1990)*, 73(7):1041–1044, 1990.

[20] Toshiki Habutsu, Yoshifumi Nishio, Iwao Sasase, and Shinsaku Mori. A secret key cryptosystem by iterating a chaotic map. In *Eurocrypt*, volume 91, pages 127–136. Springer, 1991.

[21] Shujun Li, Qi Li, Wenmin Li, Xuanqin Mou, and Yuanlong Cai. Statistical properties of digital piecewise linear chaotic maps and their roles in cryptography and pseudo-random coding. *Lecture notes in computer science*, 2260:205–221, 2001.

[22] Vladimir A Protopopescu, Robert T Santoro, and Johnny S Tolliver. Fast and secure encryption-decryption method based on chaotic dynamics, December 26 1995. US Patent 5,479,513.

[23] Sang Tao, Wang Ruli, and Yan Yixun. Perturbance-based algorithm to expand cycle length of chaotic key stream. *Electronics Letters*, 34(9):873–874, 1998.

[24] Naoki Masuda and Kazuyuki Aihara. Cryptosystems with discretized chaotic maps. *Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions on*, 49(1):28–40, 2002.

[25] Mieczysław Jessa. Data encryption algorithms using one-dimensional chaotic maps. In *Circuits and Systems, 2000. Proceedings. ISCAS 2000 Geneva. The 2000 IEEE International Symposium on*, volume 1, pages 711–714. IEEE, 2000.

[26] Kenji Yano and Kiyoshi Tanaka. Image encryption scheme based on a truncated baker transformation. *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*, 85(9):2025–2035, 2002.

[27] Roy Tenny and Lev S Tsimring. Additive mixing modulation for public key encryption based on distributed dynamics. *IEEE transactions on circuits and systems I: regular papers*, 52(3):672–679, 2005.

[28] Mousa Farajallah. *Chaos-based crypto and joint crypto-compression systems for images and videos.* PhD thesis, UNIVERSITE DE NANTES, 2015.

[29] Don Coppersmith. The data encryption standard (des) and its strength against attacks. *IBM journal of research and development*, 38(3):243–250, 1994.

[30] Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson. *The Twofish encryption algorithm: a 128-bit block cipher.* John Wiley & Sons, Inc., 1999.

[31] Eli Biham, Ross Anderson, and Lars Knudsen. Serpent: A new block cipher proposal. In *Fast Software Encryption*, pages 222–238. Springer, 1998.

[32] Pete Chown. Advanced encryption standard (aes) ciphersuites for transport layer security (tls). Technical report, 2002.

[33] Goutam Paul and Subhamoy Maitra. *RC4 stream cipher and its variants.* CRC press, 2011.

[34] Philip Hawkes and G Rose. Primitive specification for sober-128. iacr eprint archive, 2003.

[35] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[36] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE transactions on information theory*, 31(4):469–472, 1985.

[37] Mousa Farajallah, Rawan Qumsieh, and Samer Isayed. " selective hybrid chaotic-based cipher for real-time image application. The Tenth International Conference on Emerging Security Information, Systems and Technologies–SECURWARE 2016, 2016.

[38] Douglas R Stinson. *Cryptography: theory and practice*. CRC press, 2005.

[39] Zbigniew Kotulski and Janusz Szczepański. Discrete chaotic cryptography. *Annalen der Physik*, 509(5):381–394, 1997.

[40] Mina Mishra and Vijay H Mankar. Chaotic encryption scheme using 1-d chaotic map. *arXiv preprint arXiv:1312.4042*, 2013.

[41] J Daemen. " aes proposal: Rijndael," aes algorithm submission. *http://csrc. nist. gov/encryption/aes/Rijndael. pdf*, 1999.

[42] Medien Zeghid, Mohsen Machhout, Lazhar Khriji, Adel Baganne, and Rached Tourki. A modified aes based algorithm for image encryption. *International Journal of Computer Science and Engineering*, 1(1):70–75, 2007.

[43] B Subramanyan, Vivek M Chhabria, and TG Sankar Babu. Image encryption based on aes key expansion. In *Emerging Applications of Information Technology (EAIT), 2011 Second International Conference on*, pages 217–220. IEEE, 2011.

[44] Qian Gong-bin, Jiang Qing-feng, and Qiu Shui-sheng. A new image encryption scheme based on des algorithm and chua's circuit. In *Imaging Systems and Techniques, 2009. IST'09. IEEE International Workshop on*, pages 168–172. IEEE, 2009.

[45] Whitfield Diffie and Martin Hellman. New directions in cryptography. *IEEE transactions on Information Theory*, 22(6):644–654, 1976.

[46] Kamlesh Gupta, Sanjay Silakari, Ranu Gupta, and Suhel A Khan. An ethical way of image encryption using ecc. In *Computational Intelligence, Communication Systems and Networks, 2009. CICSYN'09. First International Conference on*, pages 342–345. IEEE, 2009.

[47] George Anastasios Spanos and Tracy Bradley Maples. Performance study of a selective encryption scheme for the security of networked, real-time video. In *Computer Communications and Networks, 1995. Proceedings., Fourth International Conference on*, pages 2–10. IEEE, 1995.

[48] Kwangjin Hong and Keechul Jung. Partial encryption of digital contents using face detection algorithm. *PRICAI 2006: Trends in Artificial Intelligence*, pages 632–640, 2006.

[49] E Lorenz. The essence of chaosuniversity of washington press. *Seattle, WA*, 1993.

[50] Stephen H Kellert. *In the wake of chaos: Unpredictable order in dynamical systems*. University of Chicago press, 1994.

[51] Ljupco Kocarev. Chaos-based cryptography: a brief overview. *IEEE Circuits and Systems Magazine*, 1(3):6–21, 2001.

[52] Guanrong Chen, Yaobin Mao, and Charles K Chui. A symmetric image encryption scheme based on 3d chaotic cat maps. *Chaos, Solitons & Fractals*, 21(3):749–761, 2004.

[53] Jung-Sik Cho, Sang-Soo Yeo, and Sung Kwon Kim. Securing against brute-force attack: A hash-based rfid mutual authentication protocol using a secret value. *Computer Communications*, 34(3):391–397, 2011.

[54] J-R Ohm, Gary J Sullivan, Heiko Schwarz, Thiow Keng Tan, and Thomas Wiegand. Comparison of the coding efficiency of video coding standardsincluding high efficiency video coding (hevc). *IEEE Transactions on circuits and systems for video technology*, 22(12):1669–1684, 2012.

[55] Jacob Cohen, Patricia Cohen, Stephen G West, and Leona S Aiken. *Applied multiple regression/correlation analysis for the behavioral sciences*. Routledge, 2013.

[56] Heinz Georg Schuster and Wolfram Just. *Deterministic chaos: an introduction*. John Wiley & Sons, 2006.

[57] K Boguta. Sensitivity to peturbation in elementary cellular automata, from the wolfram demonstrations project http://demonstrations. wolfram. com, 2011.

[58] A Zech, JF Donges, N Marwan, and J Kurths. Frequency distribution of the logistic map, from the wolfram demonstrations project, 2011.

[59] E Mahieu. Bifurcation diagram of the hénon map from the wolfram demonstrations project http://demonstrations. wolfram. com, 2011.

[60] Kathleen T Alligood, Tim D Sauer, James A Yorke, and JD Crawford. Chaos: an introduction to dynamical systems. *Physics Today*, 50:67, 1997.

[61] Pellicer-Lostao Carmen and López-Ruiz Ricardo. Notions of chaotic cryptography: sketch of a chaos based cryptosystem. In *Applied Cryptography and Network Security*. InTech, 2012.

[62] C Fabre. Chaos game 2d/3d, from the wolfram demonstrations project http://demonstrations. wolfram. com, 2011.

[63] Michael A Bernhard. Introduction to chaotic dynamical systems. Technical report, NAVAL POSTGRADUATE SCHOOL MONTEREY CA, 1992.

[64] Gonzalo Alvarez and Shujun Li. Some basic cryptographic requirements for chaos-based cryptosystems. *International Journal of Bifurcation and Chaos*, 16(08):2129–2151, 2006.

[65] MS Baptista. Cryptography with chaos. *Physics Letters A*, 240(1-2):50–54, 1998.

[66] Chen Guan Rong and Dong Xiao Ning. *From chaos to order: methodologies, perspectives and applications*. World Scientific, 1998.

[67] William Stallings and Mohit P Tahiliani. *Cryptography and network security: principles and practice*, volume 6. Pearson London, 2014.

[68] Jiun-In Guo et al. A new chaotic key-based design for image encryption and decryption. In *Circuits and Systems, 2000. Proceedings. ISCAS 2000 Geneva. The 2000 IEEE International Symposium on*, volume 4, pages 49–52. IEEE, 2000.

[69] Goce Jakimoski and Ljupčo Kocarev. Analysis of some recently proposed chaos-based encryption algorithms. *Physics Letters A*, 291(6):381–384, 2001.

[70] Monisha Sharma and Manoj Kumar Kowar. Image encryption techniques using chaotic schemes: a review. 2010.

[71] Jiri Fridrich. Image encryption based on chaotic maps. In *Systems, Man, and Cybernetics, 1997. Computational Cybernetics and Simulation., 1997 IEEE International Conference on*, volume 2, pages 1105–1110. IEEE, 1997.

[72] Jiri Fridrich. Secure image ciphering based on chaos. *Final report (April, 1997)*, 1997.

[73] Fethi Belkhouche and Uvais Qidwai. Binary image encoding using 1d chaotic maps. In *IEEE Region 5, 2003 Annual Technical Conference*, pages 39–43. IEEE, 2003.

[74] Zhang Han, Wang Xiu Feng, Li Zhao Hui, Liu Da Hai, and Lin You Chou. A new image encryption algorithm based on chaos system. In *Robotics, intelligent systems and signal processing, 2003. Proceedings. 2003 IEEE international conference on*, volume 2, pages 778–782. IEEE, 2003.

[75] Musheer Ahmad and M Shamsher Alam. A new algorithm of encryption and decryption of images using chaotic mapping. *International Journal on computer science and engineering*, 2(1):46–50, 2009.

[76] G Srividya and P Nandakumar. A triple-key chaotic image encryption method. In *Communications and Signal Processing (ICCSP), 2011 International Conference on*, pages 266–270. IEEE, 2011.

[77] Narendra K Pareek, Vinod Patidar, and Krishan K Sud. Image encryption using chaotic logistic map. *Image and vision computing*, 24(9):926–934, 2006.

[78] Bruce Schneier. Description of a new variable-length key, 64-bit block cipher (blowfish). In *International Workshop on Fast Software Encryption*, pages 191–204. Springer, 1993.

[79] CK Huang and HH Nien. Multi chaotic systems based pixel shuffle for image encryption. *Optics Communications*, 282(11):2123–2127, 2009.

[80] Shubo Liu, Jing Sun, and Zhengquan Xu. An improved image encryption algorithm based on chaotic system. *JCP*, 4(11):1091–1100, 2009.

[81] Ercan Solak, Cahit Çokal, Olcay Taner Yildiz, and TÜRKER BIYIKOĞLU. Cryptanalysis of fridrich's chaotic image encryption. *International Journal of Bifurcation and Chaos*, 20(05):1405–1413, 2010.

[82] NK Pareek, Vinod Patidar, and KK Sud. Cryptography using multiple one-dimensional chaotic maps. *Communications in Nonlinear Science and Numerical Simulation*, 10(7):715–723, 2005.

[83] Rashidah Kadir, Rosdiana Shahril, and Mohd Aizaini Maarof. A modified image encryption scheme based on 2d chaotic map. In *Computer and Communication Engineering (ICCCE), 2010 International Conference on*, pages 1–5. IEEE, 2010.

[84] Yunpeng Zhang, Jing Xie, Peng Sun, and Lifu Huang. A new image encryption algorithm based on arnold and coupled chaos maps. In *Computer and Communication Technologies in Agriculture Engineering (CCTAE), 2010 International Conference On*, volume 1, pages 308–311. IEEE, 2010.

[85] GA Sathishkumar, Dr N Sriraam, et al. Image encryption based on diffusion and multiple chaotic maps. *arXiv preprint arXiv:1103.3792*, 2011.

[86] Komal D Patel and Sonal Belani. Image encryption using different techniques: A review. *International Journal of Emerging Technology and Advanced Engineering*, 1(1):30–34, 2011.

[87] Chenghang Yu, Baojun Zhang, and Xiang Ruan. The chaotic feature of trigonometric function and its use for image encryption. In *Fuzzy Systems and Knowledge Discovery (FSKD), 2011 Eighth International Conference on*, volume 1, pages 390–395. IEEE, 2011.

[88] XiaoJun Tong, Yang Liu, Miao Zhang, and Zhu Wang. A novel image encryption scheme based on dynamical multiple chaos and baker map. In *Distributed Computing and Applications to Business, Engineering & Science (DCABES), 2012 11th International Symposium on*, pages 285–289. IEEE, 2012.

[89] Lei Li-Hong, Bai Feng-Ming, and Han Xue-Hui. New image encryption algorithm based on logistic map and hyper-chaos. In *Computational and Information Sciences (ICCIS), 2013 Fifth International Conference on*, pages 713–716. IEEE, 2013.

[90] Rajinder Kaur and Er Kanwalprit Singh. Image encryption techniques: A selected review. *Journal of Computer Engineering (IOSRJCE)*, 9(6):80–83, 2013.

[91] S Hraoui, F Gmira, AO Jarar, Khalid Satori, and Abderrahim Saaidi. Benchmarking aes and chaos based logistic map for image encryption. In *Computer Systems and Applications (AICCSA), 2013 ACS International Conference on*, pages 1–4. IEEE, 2013.

[92] MA Murillo-Escobar, F Abundiz-Pérez, C Cruz-Hernández, and RM López-Gutiérrez. A novel symmetric text encryption algorithm based on logistic map. In *Proceedings of the International Conference on Communications, Signal Processing and Computers (ICNC14)*, 2014.

[93] MA Murillo-Escobar, César Cruz-Hernández, F Abundiz-Pérez, RM López-Gutiérrez, and OR Acosta Del Campo. A rgb image encryption algorithm based on total plain image characteristics and chaos. *Signal Processing*, 109:119–131, 2015.

[94] Xiuli Chai, Yiran Chen, and Lucie Broyde. A novel chaos-based image encryption algorithm using dna sequence operations. *Optics and Lasers in Engineering*, 88:197–213, 2017.

[95] Naoki Masuda, Goce Jakimoski, Kazuyuki Aihara, and Ljupco Kocarev. Chaotic block ciphers: from theory to practical algorithms. *Circuits and Systems I: Regular Papers, IEEE Transactions on*, 53(6):1341–1352, 2006.

[96] W Steven Brown. On euclid's algorithm and the computation of polynomial greatest common divisors. *Journal of the ACM (JACM)*, 18(4):478–504, 1971.

[97] Stallings William. Cryptography and network security: principles and practice. *Prentice-Hall, Inc*, pages 23–50, 1999.

[98] William F Ehrsam, Carl HW Meyer, John L Smith, and Walter L Tuchman. Message verification and transmission error detection by block chaining, February 14 1978. US Patent 4,074,066.

[99] Yue Wu, Joseph P Noonan, and Sos Agaian. Npcr and uaci randomness tests for image encryption. *Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT)*, pages 31–38, 2011.

[100] Farhad Maleki, Ali Mohades, S Mehdi Hashemi, and Mohammad Ebrahim Shiri. An image encryption system by cellular automata with memory. In *Availability, Reliability and Security, 2008. ARES 08. Third International Conference on*, pages 1266–1271. IEEE, 2008.

[101] Michael Lewis-Beck. *Data analysis: An introduction*. Number 103. Sage, 1995.

[102] Rinaldi Munir. Security analysis of selective image encryption algorithm based on chaos and cbc-like mode. In *Telecommunication Systems, Services, and Applications (TSSA), 2012 7th International Conference on*, pages 142–146. IEEE, 2012.

[103] Hossam El-din H Ahmed, Hamdy M Kalash, and OS Farag Allah. Encryption efficiency analysis and security evaluation of rc6 block cipher for digital images. In *Electrical Engineering, 2007. ICEE'07. International Conference on*, pages 1–7. IEEE, 2007.

[104] Wei Zhang, Kwok-wo Wong, Hai Yu, and Zhi-liang Zhu. An image encryption scheme using reverse 2-dimensional chaotic map and dependent diffusion. *Communications in Nonlinear Science and Numerical Simulation*, 18(8):2066–2080, 2013.

[105] Yong Wang, Kwok-Wo Wong, Xiaofeng Liao, and Guanrong Chen. A new chaos-based fast image encryption algorithm. *Applied soft computing*, 11(1):514–522, 2011.

[106] A Akhshani, A Akhavan, S-C Lim, and Z Hassan. An image encryption scheme based on quantum logistic map. *Communications in Nonlinear Science and Numerical Simulation*, 17(12):4653–4661, 2012.

[107] Kwok-Wo Wong, Bernie Sin-Hung Kwok, and Wing-Shing Law. A fast image encryption scheme based on chaotic standard map. *Physics Letters A*, 372(15):2645–2652, 2008.

[108] A Kanso and M Ghebleh. A novel image encryption algorithm based on a 3d chaotic map. *Communications in Nonlinear Science and Numerical Simulation*, 17(7):2943–2959, 2012.

[109] Mousa Farajallah, Zeinab Fawaz, Safwan El Assad, and Olivier Déforges. Efficient image encryption and authentication scheme based on chaotic sequences. In *The 7th International Conference on Emerging Security Information, Systems and Technologies*, pages 150–155, 2013.