

**Republic of Iraq
Ministry of Higher Education and Scientific Research
Diyala University
College of Engineering
Computer and Software Engineering Department**



Image Cryptography Based Chaotic System

By

Farah Najieb Ibrahim

Elaf Jassim Mohammed

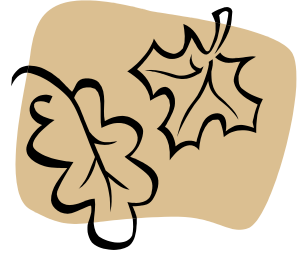
Deman Khalid Noori

Supervised By

Hussien Y. Radhi

May 2016

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



فَتَبَارَكَ الَّذِي فِي يَدَيْهِ الْمَصِيرُ
وَالَّذِي يُنَزِّلُ الْمَطَرُ
وَالَّذِي يُنْزِلُ مِنَ السَّمَاءِ مَاءً
فَيَخْرُجُ مِنْهُ شَجَرٌ يَخْرُجُ مِنْهُ
طَعَامٌ

فَتَبَارَكَ الَّذِي فِي يَدَيْهِ الْمَصِيرُ
وَالَّذِي يُنَزِّلُ الْمَطَرُ
وَالَّذِي يُنْزِلُ مِنَ السَّمَاءِ مَاءً
فَيَخْرُجُ مِنْهُ شَجَرٌ يَخْرُجُ مِنْهُ
طَعَامٌ

وَالَّذِي يُنَزِّلُ الْمَطَرُ
وَالَّذِي يُنْزِلُ مِنَ السَّمَاءِ مَاءً
فَيَخْرُجُ مِنْهُ شَجَرٌ يَخْرُجُ مِنْهُ
طَعَامٌ

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

سورة طه الآية (114)



الإهداء



جلأنا بأكرم زيد..... وقاسرنا أكثرهم زهم..... وعانينا الكثير من الصعوبات..... وهانحن اليوم والحمد لله

نطوي سهر الليالي..... وتعب الأيام..... وخلاصة مشوارنا بين دفتي هذا العمل المتواضع.....

إلى منارة العلم ولأمام المصطفى النبي الأمي..... السيد الخلق الرسول الكريم سيدنا محمد صلى الله عليه وآله

وسلم.....

إلى ينبوع الذي لا يمل العطاء..... إلى من حاك تسعادي بخيوط منسوجة من قلبها..... إلى والدي

العزيزة.....

إلى من سعى وشقى لأنعم بالراحة والهناء..... الذي لم يخل بشيء من أجل دفعي في طريق النجاح..... الذي علمني أن

أرتقي سلم الحياة بحكمة وصبر..... إلى والدي العزيز.....

إلى من ينهم بحري في عروقي..... ويلهج بذكرهم فؤادي..... إلى إخوتي.....

إلى من سبنا سويًا ونحن نشق الطريق معاً نحو النجاح والإبداع إلى زميلاتي وزملائي

إلى من علمونا حروفاً من ذهب وكلمات من دُرر وعبارات من أسمى وأجلى عبارات في العلم إلى من صاغوا

لنا علمهم حُروفاً ومن فكرهم منارة تُنيرُ لنا سيرة العلم والنجاح إلى أساتذتنا الكرام

الشكر والتقدير

بسم الله والصلاة والسلام على رسول الله وعلى آله وصحبه ومن والاه

الحمد والشكر لله العلي القدير الذي مكنتنا من انجاز هذا العمل المتواضع والذي نأمل ان ينال رضا واستحسان
القائمين والمشرفين عليه.

وشكر خاص للجميع اعضاء الهيئة التدريسية الكرام للجامعة ديا / كلية الهندسة / قسم هندسة الحاسبات
والبرامجيات لما افاضوا علينا من منهل علمهم الفياض.

وكذلك نعرب عن امتناننا الكبير لرئيس قسم هندسة الحاسبات والبرامجيات الاستاذ الدكتور علي جاسم عبود الذي
قدم لنا الدعم والتسهيلات اللازمة لانجاز هذا المشروع من خلال توفير المراجع والمختبرات.

والكلمات وحدها لا تكفي أن تعبر عن مدى شكرنا وامتناننا الكبيرين للاستاذ الدكتور حسين يوسف راضي

المشرف على المشروع، والذي لم يألوا جهدا في انجاح هذا المشروع وذلك من خلال توجيهاته واقتراحاته السديدة
وتشجيعه المستمر لنا .

وأخيرا، الشكر لكل من ساهم وساعد في انجاز هذا العمل والشكر للعائلة مع حبهم.

ABSTRACT

Because of a huge development in communication systems such as internet , mobile and satellite , etc . A large information is needed to be sent and received and some of this information is very important and must be secured therefore it must be encrypted to prevent the third party bit from listening or changing the sending data , the main idea of encryption technology comes out from the relation between the original information or data and the cipher one more strong encryption is obtain when there is no absolute relation between the cipher and the original data and it is possible to rebuild the original data in much easier way . The secret key is an important matter to encrypt and data such as text , image , audio and video , there are different techniques used to generate the key , In literature , the chaotic systems have got much attention because of their complex dynamic behaviors bifurcation and it is known to be more random and non predictable , it can be made utilized in achieving the encryption , the scrambling behavior can be obtained from the randomness property of chaos which can be better utilized in the techniques like transposition system . Therefore in recent years a large number of researches used this system to encrypt the data.

In this project the chaos system is used to obtain the key , two types of chaos system is used , Liu and Lorenz. The key stream generated is the key design issue of an encryption system , it directly determines the security and efficiency but most of the proposed key streams are binary valued and suffer from short period and limited key space , the cryptography of image is achieved by changing the position of the pixels in the original image and

changing the pixels valued depending on random numbers that generated by Liu and Lorenz systems and it is found that the generated key from these system is very secret from the obtained results it is found that the proposed system is effective and has high level security since it has high key space , high key sensitivity , high encrypt , low correlation and strong against different analysis and final very low time complexity.

CONTENTS

<i>Subjects</i>	<i>Pages</i>
Acknowledgement	i
Abstract	ii
Contents	iv
List of Figures	vi
List of Tables	Vii

Chapter One : Introduction

1.1 General eneral Consideration	1
1.2 Types of cryptography	2
1.3 Literature Survey.....	14
1.4 Aims of the Work.....	15
1.5 Thesis Organization.....	15

Chapter Two : Cryptography Based Chaotic System

2.1 Introduction	16
------------------------	----

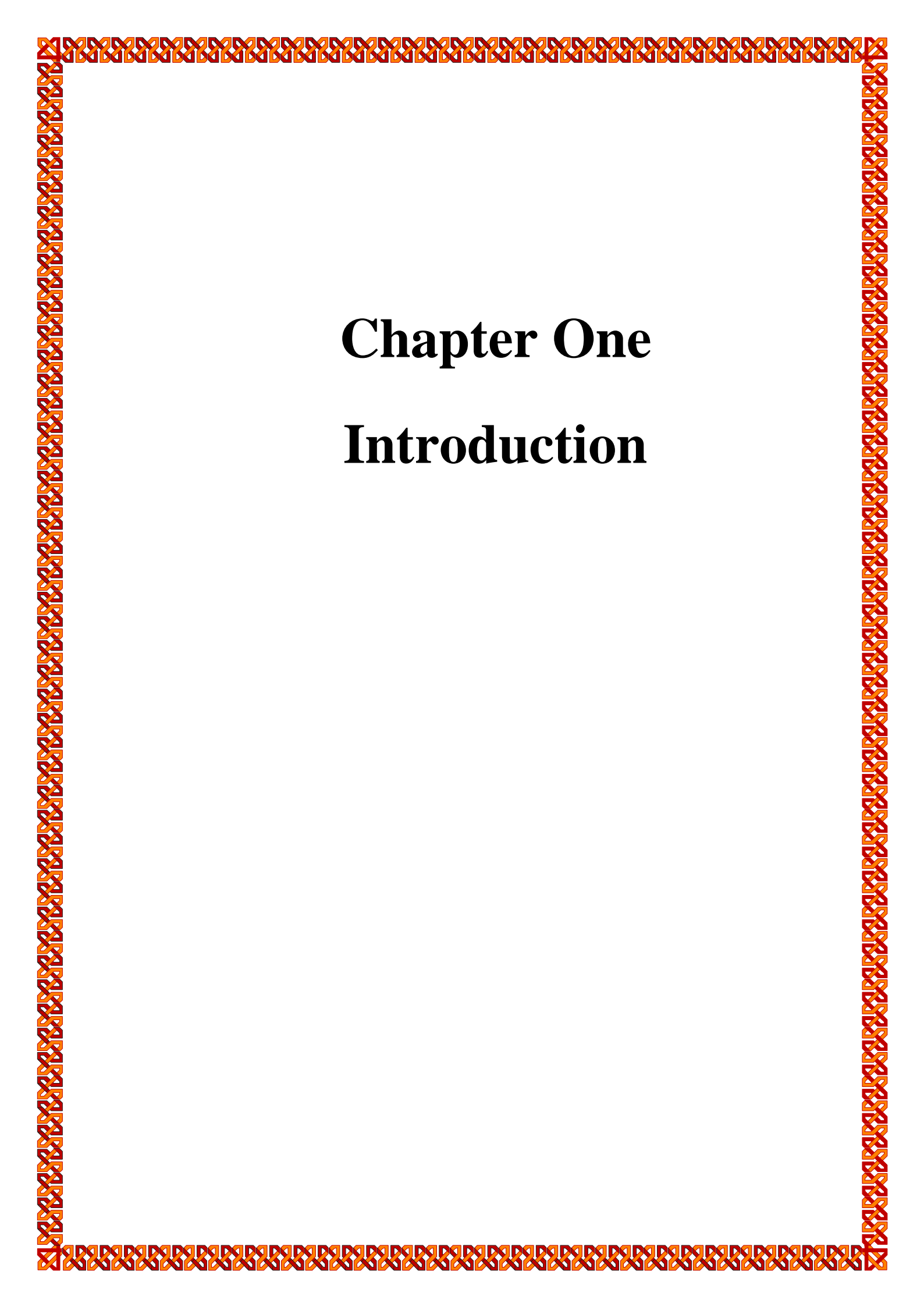
2.2 Cryptography	16
2.3 The Aims of Cryptography	17
2.4 Cryptography Terminology	17
2.5 Cryptanalysis	18
2.6 Classification Encryption.....	20
2.7 Chaos System	24
2.8 The Properties of Chaos	25
2.9 Principles of Chaos	26
2.10 Chaos-based Image Encryption	27
2.11 Propose system	32

Chapter Three : Simulation Results

3.1 Introduction	37
3.2 Results.....	37
3.3 Evaluation of Encryption Process	39

Chapter Four : Conclusion

4.1 Conclusions	50
4.2 Suggestions for Future Works	51



Chapter One

Introduction

CHAPTER ONE

Introduction

1.1 General consideration

A secure computing environment would not be complete without consideration of encryption technology. The term encryption refers to the practice of obscuring the meaning of a piece of information by encoding it in such a way that it can only be decoded, read and understood by people for whom the information is intended. It is the process of encoding data to prevent unauthorized parties from viewing or modifying it.

The use of simple codes to protect information can be traced back to the fifth century BC. As time has progressed, the methods by which information is protected have become more complex and more secure. Encryption can be used to provide high levels of security to network communication, e-mail, files stored on hard drives or floppy disks, and other information that requires protection.

Cryptography is used to hide information. It is not only use by spies but for phone, fax and e-mail communication, bank transactions, bank account security, PINs, passwords and credit card transactions on the web. It is also used for a variety of other information security issues including electronic signatures, which are used to prove who sent a message. we must know the A plaintext message, or simply a plaintext, is a message to be communicated. A disguised version of a plaintext message is a cipher text message or simply a cipher text. The process of creating a cipher text from a plaintext is called encryption. The process of turning a cipher text back into a plaintext is called decryption. Cryptosystems come in 3 kinds[1]:

1. Those that have been broken (most).
2. Those that have not yet been analyzed (because they are new and not yet widely used).
3. Those that have been analyzed but not broken. (RSA, Discrete log cryptosystems, Triple DES, AES).

There are important concepts you need to know on the subject of encryption:

1. Encryption and decryption should be easy for the proper users, Alice and Bob. Decryption should be hard for Eve. Computers are much better at handling discrete objects. Number theory is an excellent source of discrete (i.e. finite) problems with easy and hard aspects.
2. Security and practicality of a successful cryptosystem are almost always tradeoffs. Practicality issues: time, storage, co-presence.
3. Must assume that the enemy will find out about the nature of a cryptosystem and will only be missing a key .

1.2 Types of cryptography

1.1.2 Historical cryptography

The historical types are [1]:

- *Ancient Egypt*

The earliest known text containing components of cryptography originates in the Egyptian town Menet Khufu on the tomb of nobleman Khnumhotep II nearly 4,000 years ago. In about 1900 B.C. Khnumhotep's scribe drew his master's life in his tomb. As he drew the hieroglyphics he used a number of unusual symbols to obscure the meaning of the inscriptions. This method of encryption is an example of a substitution cipher, which is an cipher system which substitutes one symbol or character for another.



Fig 1.1. Symbol taken from the tomb of Khnumhotep II.

As the Egyptian culture evolved, hieroglyphic substitution became more common. This method of encryption was relatively easy to break for those who could read and write. There are several possibilities why the Egyptians would use the sacred nature of their religious rituals from common cryptography is that the scribes wanted to give a formal appearance to their writings. This seems to be very similar to formal complicated language used in any modern legal document. Egyptian cryptography could also have been a way for a scribe to impress others by showing that he could write at a higher level .

- *Greece*

In about 500 B.C. the Spartans developed a device called secret messages. The device was a cylinder message was then written length-wise on the parchment. Once it was unwound the message on the strip of parchment became unreadable. To receive the message an identical cylinder was needed. It was only then that the letters would line up resulting in the original message. The Scytale is an example of a transposition cipher, which is any cipher system that changes the order of the characters rather than changing the character be very easy to decipher, however, 2,500 years ago the percent of people would could read and write was relatively small. The Scytale provided the Spartans a secure method of communication.

- ***Rome***

The earliest recorded military use of cryptography comes from Julius Caesar 2,000 years ago. Caesar, being commander of the Roman army, solved the problem of secure communication with his troops . The problem was that messengers of secret military messages Caesar developed a substitution cipher method in which he would substitute letters for different letters. Only those who knew the substitution used messengers were overtaken the secret messages were not exposed. This gave the Roman army a huge advantage during war.



Fig 1.2. Example of a substitution

Unlike the example found in Figure 1.2, Caesar typically just shifted his letters by some predetermined number. This number was the cipher key of his algorithm. A randomized order of substitution yields a much larger amount of security due to the larger amount of possible orderings [1].

- ***Alberti-Vigenere Cipher***

During the mid-1400's a man named Leon Battista Alberti invented an encryption system using a cipher disk. This was a mechanical device with sliding disks that allowed for many different methods of substitution. This is

the base concept of a poly alphabetic cipher, which is an encryption method which switches through several substitution ciphers throughout encryption.

In the 1500's Blaise De Vigenere, following Alberti's poly alphabetic cipher style, created a cipher that came to be known as the Vigenere Cipher. The Vigenere Cipher works exactly like the Caesar except that it changes the key throughout the encryption process. The Vigenere Cipher uses a grid of letters that give the method of substitution. This grid is called a Vigenere Square or a Vigenere Table. The grid is made up of 26 alphabets offset from each other by one letter.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Fig 1.3. Vigenere

The method of changing from one key to another follows chosen as a special secret word. The first character of the plaintext can follow: The substituted letter for the first plaintext character on the x-axis and the first letter of the special secret word letter is then substituted for the plaintext character. This

method is repeated through all characters of the key word. After all characters of the key word are used, the word is just repeated.

For example, suppose that the plaintext to be encrypted is :

ATTACKATDAWN

The person encrypting the message chooses a key word and repeats it until its length matches the plaintext. For example "LEMON."

LEMONLEMONLE

The first letter of the plaintext is enciphered using the alphabet in row keyword. The substitution is made by finding the letter in row next letter, the substitution is made by finding the letter in row repeated until each plaintext character

Plaintext: **ATTACKATDAWN**

Keyword: **LEMONLEMONLE**

Ciphertext: **LXFOPVEFRNHR**

The decryption algorithm is the exact same except that the person finds the column that corresponds to the ciphertext's character in the keyword's row.

- ***Jefferson Wheel Cipher***

In the late 1700's, Thomas Jefferson came up with acipher system very similar to the Vigenere Cipher except with higher security. His invention was 26 wheels with the alphabet randomly scattered on each wheel. The wheels were numbered and ordered with a specified order. This order is the key to the encryption algorithm. To message to be encrypted is made on the wheels by lining up the wheels such that the message is present. The cipher text is any other line besides the line containing the original message. The person decrypting the cipher text must have the wheels in the proper order. As the cipher text is made on the wheels, the plaintext is lined up somewhere else on

the wheels. A visual scan can quickly result in finding the original text. There is an extremely small chance that two non-gibberish messages will emerge on the disk during decryption. Similar to Alberti, Jefferson never developed his encryption system. During the early 1900's, the United States Army reinvented Jefferson's Wheel Cipher without any knowledge about Jefferson's invention. Jefferson was over a hundred years before his time. The United States Army used this system from 1923 to 1942 (Thinkquest.org 1999).

2.1.2 Modern Encryption

These types are [1]

- *One-Time Pad*

The "one-time pad" encryption algorithm was invented in the early 1900's, and has since been proven as unbreakable. The one-time pad algorithm is derived from a previous cipher called Vernam Cipher, named after Gilbert Vernam. The Vernam Cipher was a cipher that combined a message with a key read from a paper tape or pad. The Vernam Cipher was not unbreakable until Joseph Mauborgne recognized that if the key was completely random the cryptanalytic difficulty would be equal to attempting every possible key (Kahn 1996). Even when trying every possible key, one would still have to review each attempt at decipherment to see if the proper key was used. The unbreakable aspect of the one-time pad comes from two assumptions: the key used is completely random; and the key cannot be used more than once. The security of the one-time pad relies on keeping the key 100% secret. The one-time pad is typically implemented by using a modular addition (XOR) to combine plaintext elements with key elements. An example of this is shown

in Fig 1.4. The key used for encryption is also used for decryption. Applying the same key to the ciphertext results back to the plaintext.

ENCRYPT	
\oplus	<div> 00110101 Plaintext 11100011 Secret Key <hr/> = 11010110 Ciphertext </div>
DECRYPT	
\oplus	<div> 11010110 Ciphertext 11100011 Secret Key <hr/> = 00110101 Plaintext </div>

Fig 1.4. Example of a One-Time Pad implementation using modular addition.

- ***Pseudo-Random Number Generator (PRNGS)***

If any non-randomness occurs in the key of a one-time pad, the security is decreased and thus no more unbreakable. Numerous attempts have been made to create seemingly random numbers from a designated key. These number generators are called Pseudo-Random Number Generators (PRNGs) because they cannot give a completely random number stream. Even though the security of a PRNG is not 100% unbreakable, it can provide sufficient security when implemented correctly. PRNGs that have been designated secure for cryptographic use are called Cryptographically Secure Pseudo-Random Number Generators (CSPRNGs). CSPRNGs have qualities that other PRNGs do not. CSPRNGs must pass the "next-bit test" in that given the first k bits, there is no polynomial-time algorithm that can predict the $(k+1)$ th bit with probability of success higher than 50% (Knuth 1981). CSPRNGs must also withstand "state compromises." In the event that part or all of its state is revealed, it should be impossible to reconstruct the stream of random numbers prior to the revelation.

- ***Symmetric Key Encryption (Private-Key)***

A symmetric key, sometimes called private-key, encryption cipher is any algorithm in which the key for encryption is trivially related to the key used for decryption. An analogy of this is a typical mechanical lock. The same key that engages the lock can disengage it. To protect anything valuable behind the lock, the key must be given to each member securely. If an unintended person obtains access to the key, he or she will have full access to what is being secured by the lock.

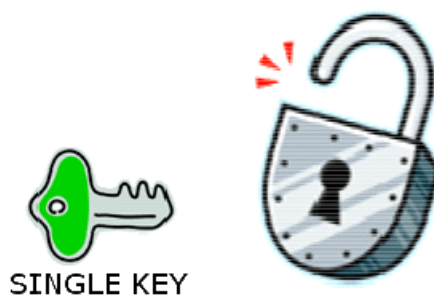


Fig 1.5. A lock that is engaged and disengaged by the same key.

- ***Implementations of Symmetric Key Encryption***

There are several modern algorithms that implement a symmetric key encrypt of symmetric key encryption is a stream cipher, where a stream of random, or pseudo are combined with the original message. Specific stream ciphers include: Feedback Shift Register (LFSR), Line and is used in Secure Socket Layer (SSL) and Wired Equivalent Privacy (WEP). Another method of symmetric key encryption is a block cipher, which operates on a fixed of bits. When encrypting, a block cipher takes a set amount of bits (i.e. 128 outputs a corresponding same size (i.e. 128 cipher is controlled by the encryption/decryption DES, and AES . AES is an encryption standard adopted by the U.S. government and has been approved by the National Security Agency (NSA) for encryption of "top secret" information. Many

current methods of symmetric key encryption employ both stream and block schemes .

- ***Asymmetric Key Encryption (Public-Key)***

The digital era of the 1970's caused a need for an encryption system that would rely on a predetermined key. Cryptographers of this era realized that in order to send a message securely without previously meeting with the recipient, they would need a system that uses a different key for encryption than it does for decryption. In comparison with symmetric key encryption, this system would compare to a lock that has one key for engaging the lock and a different key for disengaging the lock .

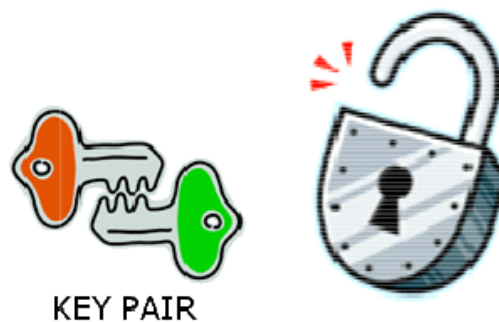


Fig 1.6. A lock that is engaged and disengaged by different keys.

- ***Diffie-Hellman Key Exchange***

The Diffie-Hellman Key Exchange is a cryptographic protocol that allows two parties with no prior knowledge of each other to establish a shared secret key, which typically **is used in a symmetric key** cipher. The Diffie- Hellman Key Exchange was first published by Whitfield Diffie and Martin Hellman in 1976. The GCHQ, the British signals intelligence, announced that this scheme had been invented by Malcolm Williamson years before Diffie and Hellman's publication, but was kept classified. The Diffie-Hellman Key

Exchange relies on exponential functions computing much faster than discrete logarithms. When used properly, the Diffie-Hellman key Exchange protocol gives two parties the same without actually transmitting it. The strength of this algorithm depends on the time it takes to compute a discrete logarithm of the public keys transmitted (Diffie, Hellman 1976).

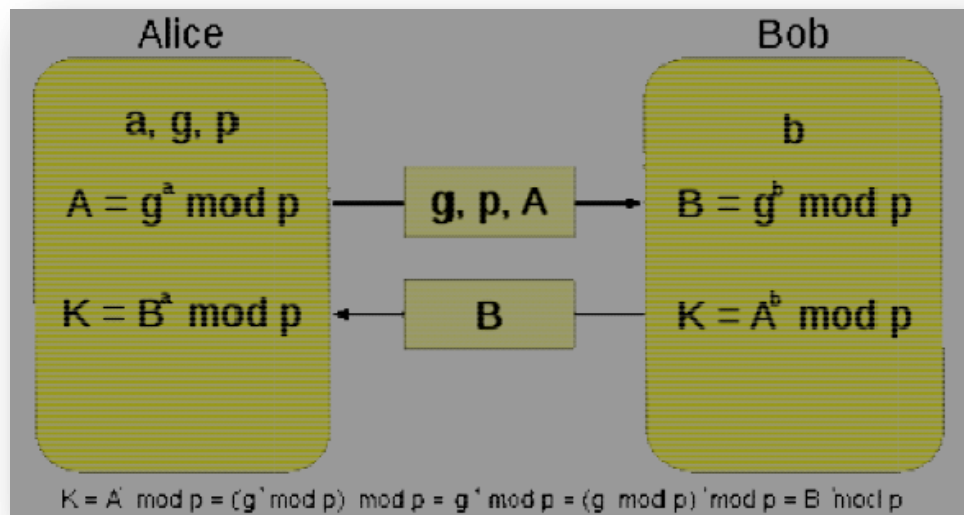


Fig 1.7. Diffie-Hellman Key Exchange protocol.

Figure 1.7 shows the steps for establishing a key through the Diffie-Hellman Key Exchange. Alice wanting to establish a key with Bob, first sets up the variables "a", "g", and "p." Bob decides "b". sending the public keys, or numbers, each party can compute "K." Notice that "K" is never sent through. The Diffie-Hellman Key Exchange is a cryptographic protocol that allows two parties with no prior is used in a symmetric key Hellman Key Exchange was first published by Whitfield Diffie and Martin Hellman in 1976. The GCHQ, the British signals intelligence, announced that this scheme had been invented by before Diffie and Hellman's publication, but was kept classified. Hellman Key Exchange relies on exponential functions computing much faster than discrete Hellman Key Exchange protocol gives two parties the same key without actually transmitting it. The strength of this

algorithm depends on the time it takes to Hellman Key Exchange. Alice, wanting to establish a key with Bob, After sending the public keys, or numbers, each party can compute "K." Notice that "K." is never sent through the medium. Also notice that "K" was not previously determined, rather it was a result to both Alice and Bob's computations. This allows each party access to the same key without ever having to see each other. A disadvantage of the Diffie-Hellman key exchange is that it does not contain the function of encryption. A predetermined message cannot be inserted into the algorithm. The transmitted number is simply the result of computation, of which is purposely hard to decompose. In order for "K" to be discovered by someone besides Alice and Bob, a logarithm of "A" or "B" must be computed. When extremely large numbers for "a", "b", and "p" are chosen, it could take billions of years to compute the logarithm of "A" or "B." .

- ***RSA Encryption***

Noticing the inability of the Diffie-Hellman Key Exchange to transmit a secret message, Ron Rivest , Adi Shamir, and Leonard Adleman developed a system similar to the Diffie-Hellman protocol except that a message could be embedded and transmitted.

RSA encryption, named for the surnames of the inventors, relies on multiplication and exponentiation being much faster than prime factorization. The entire protocol is built from two large prime numbers. These prime numbers are manipulated to give a public key and private key. Once these keys are generated they can be used many times. Typically one keeps the private key and publishes the public key. Anyone can then encrypt a message using the public key and sent it to the creator of the keys. This person then uses the private key to decrypt the message. Only the one possessing the private key can decrypt the message. One of the special numbers generated and used in RSA encryption is the modulus, which is the product of the two

large primes. In order to break this system, one must compute the prime factorization of the modulus, which results in the two primes. The strength of RSA encryption depends on the difficulty to produce this prime factorization. RSA Encryption is the most widely used asymmetric key encryption system used for electronic commerce protocols.

- ***Breaking RSA Keys***

The patent holder of RSA Encryption, RSA Security or RSA Laboratories, issued a challenge to encourage research into the practical difficulty of factorizing large integers. The motivation behind the challenge was to credit RSA Encryption to be a super power in the cryptography field. In 2007, RSA Laboratories ended the challenge stating: "Now that the industry has a considerably more advanced understanding of the cryptanalytic strength of common symmetric-key and public-key algorithms, these challenges are no longer active" (RSA Laboratories 2007).

During the activity of the RSA factoring challenge, RSA Laboratories published a list of semi-primes (numbers with exactly two prime factors) known as RSA numbers. Several of these numbers had cash prizes if they were successfully factored. Many of the smaller numbers were factored during the 1990's. During the early 2000's, a few decently large RSA numbers were factored, one of which took 80 computers 5 months to compute, and had a cash prize of \$20,000. Some of the numbers that were never factored were worth \$100,000 and \$200,000. These larger numbers are estimated to take billions of years to factor on a single computer. In contrast, they can be generated in less than a minute .

1-3 Literature Survey

To study and analyze more about the encryption techniques, the following literature survey has done and discussed in this chapter.

In [3], 2006, Gonzalo Alvarez¹ and Shujun Li², provided a common framework of basic guidelines that, if followed, every new cryptosystem would benefit from. The suggested guidelines address three main issues: implementation, key management, and security analysis, aiming at assisting designers of new cryptosystems to present their work in a more systematic and rigorous way to fulfill some basic cryptographic requirements. In [4], 2008, Yaron Rachlin and Dror Baron, considered secrecy in the context of an adversary that does not know the measurement matrix used to encrypt the signal. We demonstrate that compressed sensing based encryption does not achieve Shannon's definition of perfect secrecy, but can provide a computational guarantee of secrecy. In [5], 2011, Sundarapandian Vaidyanathan, derived new results for the hybrid synchronization of identical Liu systems, identical Lü systems, and non-identical Liu and Lü systems via adaptive control method. In [6], 2012, Priyanka Agrawal¹, Manisha Rajpoot², proposed a Partial Encryption Algorithm with Random Number Generator which encrypt the data partially but the condition is that when we apply this algorithm on the data, the order of bits should be determined randomly. In [7], 2014, Hayder Raheem Hashim^{a*}, Irtifaa Abd alkadum Neamaa^b, considered a particular public key cryptosystem called the ElGamal Cryptosystem is presented. In [8], Avi Kak introduced the rudiments of encryption/decryption vocabulary.

1-4 Aims of the Work

The main purposes of this work are:

1. To show the importance of encryption algorithms for the security of information
2. Provide more secret key by using more than one Chaotic systems with a large key space
3. Encrypt images using chaotic key
4. Detect the strength of proposed encryption algorithm such as correlation, entropy,... etc

1-5 Thesis Organization

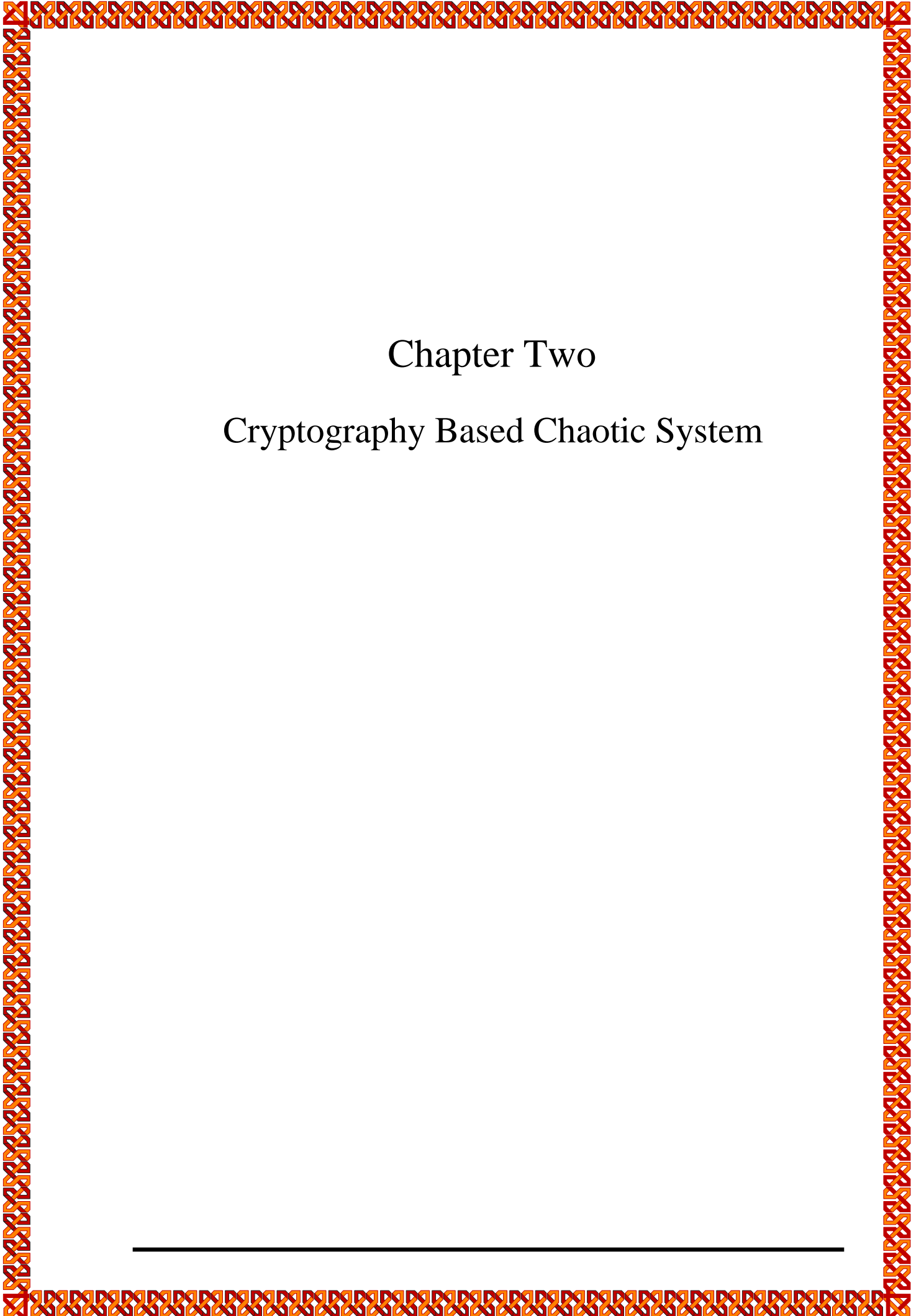
This thesis consists of four chapters, which can be briefly presented as:

Chapter One: Presents a general introduction and literature survey for the present work.

Chapter Two: this chapter shows the cryptography based on chaotic system and the proposed cryptography algorithm.

Chapter three: the simulation results and different analysis are illustrate this chapter.

Chapter four: the main conclusions that obtained from the project and the Future work is illustrated.



Chapter Two

Cryptography Based Chaotic System

CHAPTER Two

Cryptography Based Chaotic System

2.1 Introduction

In this chapter, the encryption , encryption types , and the proposed system are illustrated. The chaos systems that used to generate the cryptography key is illustrated analyzed .All stages of system in which the data passed is analyzed from the transmitter site to the receiver one to show the effect of the system can be done as compared with other works.

2.2 Cryptography

Cryptology can be divided into two areas; Cryptography and Cryptanalysis. Cryptography is the science or study of techniques of secret writing and message hiding. Cryptography is as broad as formal linguistics which obscure the meaning from those without formal training. It is also as specific as modern encryption algorithms used to secure transactions made across digital networks. Cryptography constitutes any method in which someone attempts to hide a message, or the meaning thereof, in some medium. [1]

Cryptanalysis is the branch of cryptology concerned with solving the cryptographic systems used by others. The objects of cryptanalysts are to read the text of encrypted messages and to recover the cryptographic systems used. The text is recovered for its potential intelligence value. The systems are recovered for application to future messages in the same or similar systems.[9]

2.3 The Aims of Cryptography

The cryptography is used to accomplish the following as [10] :-

- 1- Confidentiality** : Ensuring that no one can read the message except the intended receiver.
- 2- Data integrity** : Assuring the receiver that the received message has not been altered in any way from the original.
- 3- Authentication** :The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.)
- 4- Non-Repudiation** :A mechanism to prove that the sender really sent this message.

2.4 Cryptography Terminology

Cryptography Terminology is [11,8] :-

- 1- Plaintexts(the original message)**: the original data or message to be transmitted or stored.
- 2- Cipher texts (cipher message)**: the disguised message.
- 3- Encode** : to convert a message into a representation in a standard alphabet, such as to the alphabet {A, . . . , Z} or to numerical alphabet.
- 4- Decode** : to convert the encoded message back to its original alphabet and original form, the term plaintext will apply to either the original or the encoded form. The process of encoding a message is not an obscure process, and the result that we get can be considered equivalent to the plaintext message.

5- Encryption and Decryption transformation: a map from a space of plaintext to a space of cipher text . Decryption to convert plaintext into cipher text.

The following flow chart in Figure (2.1) shows the image Encryption and Decryption process [7] :

6- key space: The total number of all possible keys that can be used in a cryptographic system. For example, DES uses a 56-bit key. So the key space is of size 2^{56} . [12]

2.5 Cryptanalysis

The cryptanalysis Means “breaking the code”. Cryptanalysis relies on a knowledge of the encryption algorithm (that for civilian applications should be in the public domain) and some knowledge of the possible structure of the plaintext (such as the structure of a typical inter-bank financial transaction) for a partial or full reconstruction of the plaintext from cipher-text. Additionally, the goal is to also infer the key for decryption of future messages. The precise methods used for cryptanalysis depend on whether the “attacker” has just a piece of cipher-text, or pairs of plaintext and cipher-text, how much structure is possessed by the plaintext, and how much of that structure is known to the attacker. All forms of cryptanalysis for classical encryption exploit the fact that some aspect of the structure of plaintext may survive in the Cipher- text.[12]

There are many ways that used by cryptanalyst as [12, 3, 13]:

- brute-force attack:

When encryption and decryption algorithms are publicly available, as they generally are, a brute-force attack means trying every possible key on a piece of cipher- text until an intelligible translation into plaintext is obtained.

- codebook attack:

The attacker tries to acquire as many as possible of the mappings between the plaintext words and the corresponding cipher-text words. In some cases, such a table, referred to as the codebook, can be used to speed up the brute-force search for the encryption key. As a trivial example, consider an 8-bit block cipher. If we can construct a codebook with 256 rows in it, that would break the cipher.

- algebraic attack:

in this type the plaintext-to-cipher-text relationship can be expressed as a system of equations. Given a set of (plaintext, cipher-text) pairs, you try to solve the equations for the encryption key. As you will see, encryption algorithms involve nonlinearities. In algebraic attacks, one attempts to introduce additional variables into the system of equations and make nonlinear equations look linear.

- time-memory tradeoff in attacking ciphers:

The brute-force and the codebook attacks represent two opposite cases in terms of time versus memory needs of the algorithms. Pure brute-force attacks have very little memory needs, but can require inordinately long times to scan through all possible keys. On the other hand, codebook attacks can in principle yield results instantaneously, but their memory needs can be humongously large. Just imagine a codebook for a 64-bit block cipher; it may need as many as 2^{64} rows in it. In some cases, by trading off memory for time, it is possible to devise more effective attacks that are sometimes referred to as time-memory tradeoff attacks.

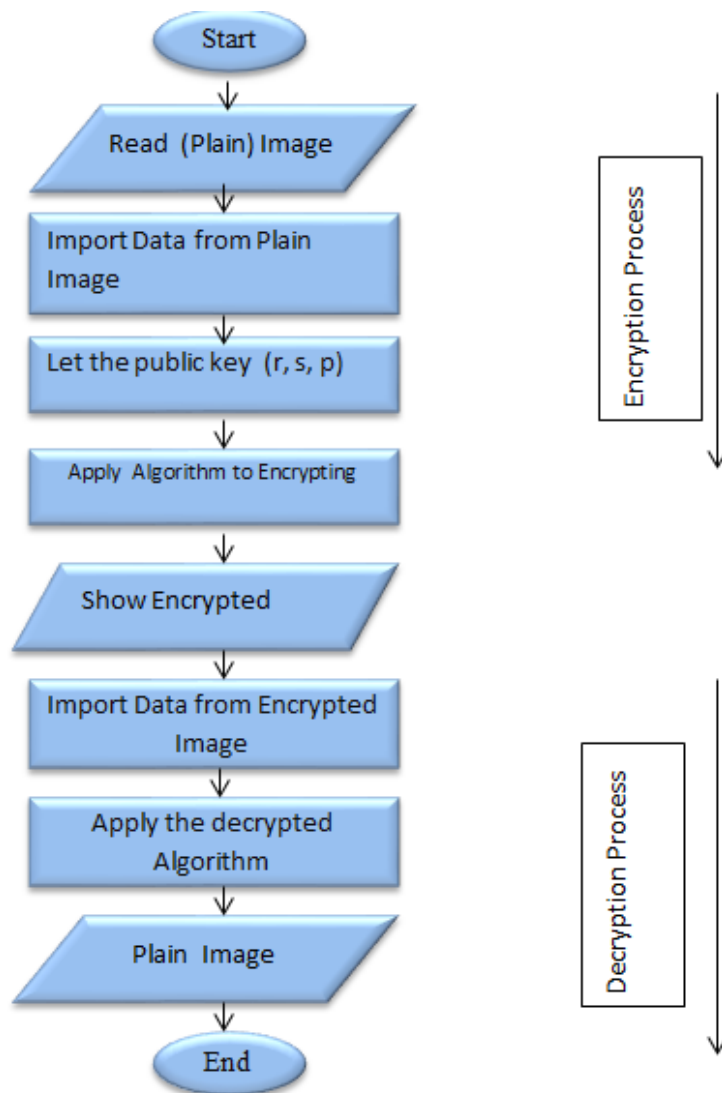


Fig 2.1 Image Encryption and Decryption process

2.6 Classification of Encryption

Encryption algorithms can be classified in different ways as [15] :-

2.6.1 According to the Structures of cryptography algorithm

The main types of this classification is illustrated in Figure(2.2).

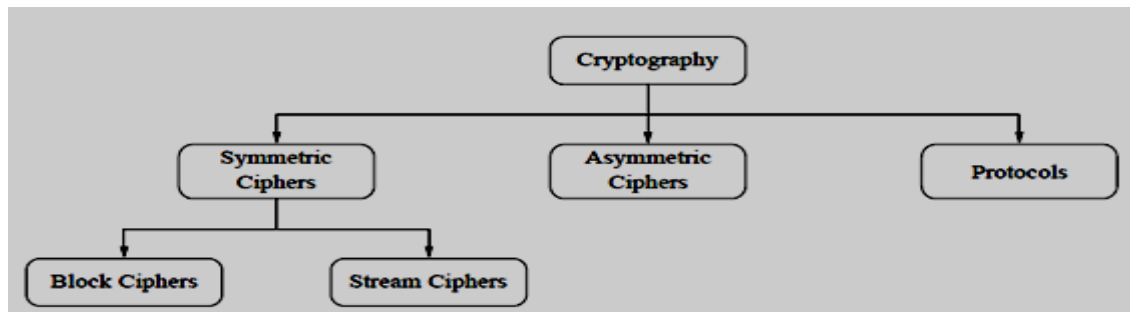


Fig 2.2 Structure Classification

(i) A stream Cipher

Encrypt bits individually. This is achieved by adding a bit from a key stream to a plaintext bit. There are synchronous stream ciphers where the key stream depends only on the key, and asynchronous ones where the key stream also depends on the cipher text. If the dotted line in Fig. 2.3 is present, the stream cipher is an asynchronous one.

(ii) A Block Cipher

Encrypt an entire block of plaintext bits at a time with the same key. This means that the encryption of any plaintext bit in a given block depends on every other plaintext bit in the same block. In practice, the vast majority of block ciphers either have a block length of 128 bits (16 bytes) such as the advanced encryption standard (AES), or a block length of 64 bits (8 bytes) such as the data encryption standard (DES) or triple DES (3DES) algorithm.

2.6.2 According to Keys

In this case the cryptography algorithm can be classified as [a8]:

(i) Symmetric (Private) Key Cryptosystems

A symmetric cryptosystem (or private key cryptosystem) uses only one key for both encryption and decryption of the data. The key used for encryption and decryption is called the private key and only people who are

authorized for the encryption/decryption would know it. In a symmetric cryptosystem, the encrypted message is sent over without any public keys attached to it.

(ii)Asymmetric (Public) Key

In an asymmetric cryptosystem (or public key cryptosystem), there are two different keys used for the encryption and decryption of data. The key used for encryption is kept public and so as called public key, and the decryption key is kept secret and called private key. The keys are generated in such a way that it is impossible to derive the private key from the public key. The transmitter and the receiver both have two keys in an asymmetric system. However, the private key is kept private and not sent over with the message to the receiver, although the public key is.

Public-key cryptography provides a radical departure from all that has gone before. For one thing, public-key algorithms are based on mathematical functions rather than on substitution and permutation. More important, public-key cryptography is asymmetric, involving the use of two separate keys, in contrast to symmetric encryption, which uses only one key. The use of two keys has profound consequences in the areas of confidentiality, key distribution, and authentication.

As with symmetric encryption, a public-key encryption scheme is vulnerable to a brute-force attack. The countermeasure is the same: Use large keys. However, there is a tradeoff to be considered. Public-key systems depend on the use of some sort of invertible mathematical function. The complexity of calculating these functions may not scale linearly with the number of bits in the key but grow more rapidly than that. Thus, the key size must be large enough to make brute-force attack impractical but small enough for practical encryption and decryption. In practice, the key sizes that have been proposed do make brute-force attack impractical but result in encryption/decryption

speeds that are too slow for general-purpose use. Instead, as was mentioned earlier, public-key encryption is currently confined to key management and signature applications. Another form of attack is to find some way to compute the private key given the public key. To date, it has not been mathematically proven that this form of attack is infeasible for a particular public-key algorithm. Thus, any given algorithm, including the widely used RSA algorithm, is suspect. The history of cryptanalysis shows that a problem that seems insoluble from one perspective can be found to have a solution if looked at in an entirely different way. Finally, there is a form of attack that is peculiar to public-key systems. This is, in essence, a probable-message attack. Suppose, for example, that a message were to be sent that consisted solely of a 56-bit DES key. An adversary could encrypt all possible 56-bit DES keys using the public key and could discover the encrypted key by matching the transmitted cipher-text. Thus, no matter how large the key size of the public-key scheme, the attack is reduced to a brute-force attack on a 56-bit key. This attack can be thwarted by appending some random bits to such simple messages.[17]

2.6.3 According to The Percentage of The Data Encryption

This classification include the following two category such as [6]:

(i)Full Encryption :

In the full encryption scheme, images as binary large objects or pixels are encrypted in their entirety. Full encryption can offer a high level of security, effectively prevent unauthorized access, and is often operated without any compression process

(ii) Partial Encryption :

This type is also called (selective encryption) which only encrypts part of the data ,a partial encryption algorithm which uses the advantages of randomization method aiming to obtain sufficient uncertainties in the selection of the bit positions of a multimedia message. During the process of sending messages, the sender will randomly select the bit positions of the multimedia message after conversion of the message in binary form . The bits on selected positions will be encrypted and transmitted along with the remaining bits over the transmission channels to the receiver. Figure(2.3) shows partial encryption type.

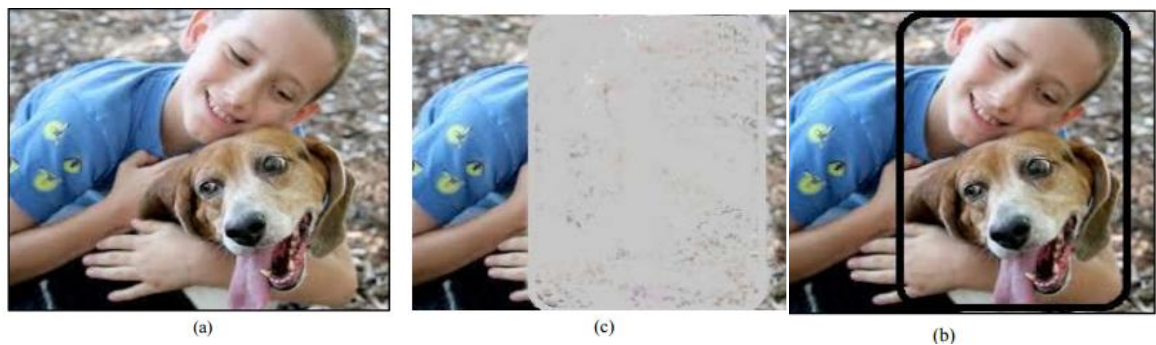


Fig 2.3. Partial Encryption

2.7 Chaos System

Chaos is the science of surprises, of the nonlinear and the unpredictable. It teaches us to expect the unexpected. While most traditional science deals with supposedly predictable phenomena like gravity, electricity, or chemical reactions, Chaos Theory deals with nonlinear things that are effectively impossible to predict or control, like turbulence, weather, the stock market, our brain states, and so on. These phenomena are often described by fractal mathematics, which captures the infinite complexity of nature. Many natural objects exhibit fractal properties, including landscapes, clouds, trees, organs,

rivers etc, and many of the systems in which we live exhibit complex, chaotic behavior. Recognizing the chaotic, fractal nature of our world can give us new insight, power, and wisdom. For example, by understanding the complex, chaotic dynamics of the atmosphere, a balloon pilot can “steer” a balloon to a desired location. By understanding that the proposed ecosystems ,the proposed social systems, and the proposed economic systems are interconnected, we can hope to avoid actions which may end up being detrimental to our long-term well-being [2].

There are different types of chaos systems such as Lorenz system ,Rossler ,Chen ,Liu ,Chue ,Henon ,etc... .In this work ,two types of chaotic system are used in such a way to provide the proposed key.

2.8 The Properties of Chaos

The basic properties of chaotic systems are :-

- **Deterministic**:-means that chaotic systems have some determining mathematical equations ruling their behavior.
- **The sensitivity to initial conditions**:- means that, when a chaotic system is iteratively applied to two initially close points, the iterations quickly diverge, and become uncorrelated in the long term.
- **Sensitivity to parameters**:-causes the properties of the map change quickly, when slightly perturbing the parameters, on which the map depends. Hence, a chaotic system can be used as a pseudorandom number generator.
- **Topological transitivity**:- is the tendency of the system to quickly scramble up small portions of the state space into an intricate network of filaments. Local, correlated information becomes scattered all over the state space.

- **The ergodicity property of a chaotic systems:-** means that if partitioning the state space into a finite number of regions, no matter how many, any orbit of the map will pass through all these regions. The ergodicity of a chaotic system is ensured by the topological transitivity property[1, 4, 3].

2.9 Principles of Chaos

Principles of Chaos are [2]:

- **The Butterfly Effect:**

This effect grants the power to cause a hurricane in China to a butterfly flapping its wings in New Mexico. It may take a very long time, but the connection is real. If the butterfly had not flapped its wings at just the right point in space/time, the hurricane would not have happened. A more rigorous way to express this is that small changes in the initial conditions lead to drastic changes in the results. Our lives are an ongoing demonstration of this principle.

- **Unpredictability:**

Because we can never know all the initial conditions of a complex system in sufficient (i.e. perfect) detail, we cannot hope to predict the ultimate fate of a complex system. Even slight errors in measuring the state of a system will be amplified dramatically, rendering any prediction useless. Since it is impossible to measure the effects of all the butterflies (etc) in the World, accurate long-range weather prediction will always remain impossible.

- **Order / Disorder Chaos:**

is not simply disorder. Chaos explores the transitions between order and disorder, which often occur in surprising ways.

- Mixing:

Turbulence ensures that two adjacent points in a complex system will eventually end up in very different positions after some time has elapsed. Examples: Two neighboring water molecules may end up in different parts of the ocean or even in different oceans. A group of helium balloons that launch together will eventually land in drastically different places. Mixing is thorough because turbulence occurs at all scales. It is also nonlinear: fluids cannot be unmixed.

- Feedback:

Systems often become chaotic when there is feedback present. A good example is the behavior of the stock market. As the value of a stock rises or falls, people are inclined to buy or sell that stock. This in turn further affects the price of the stock, causing it to rise or fall chaotically.

- Fractals:

A fractal is a never-ending pattern. Fractals are infinitely complex patterns that are self-similar across different scales. They are created by repeating a simple process over and over in an ongoing feedback loop. Driven by recursion, fractals are images of dynamic systems – the pictures of Chaos. Geometrically, they exist in between our familiar dimensions. Fractal patterns are extremely familiar, since nature is full of fractals. For instance: trees, rivers, coastlines, mountains, clouds, seashells, hurricanes, etc.

2.10 Chaos-based Image Encryption

There are a number of encryption algorithms available such as **DES** (**D**ata **E**ncryption **S**tandard), **AES** (**A**dvanced **E**ncryption **S**tandard), **IDEA** (**I**nternational **D**ata **E**ncryption **A**lgorithm), **RSA** (**R**ivest, **S**hamir and **A**dleman) these traditional encryption algorithms which are used for text or binary data, do not appear as ideal for multimedia applications (especially

image) and the basic reasons are; huge in size and bulk capacity, high redundancy and a high correlation between pixels. Traditional encryption methods are difficult to apply and slow in process, on the other hand digital image encryption needs to have :-

1. The computational complexity of encryption and decryption processes should be as slow as possible.
2. The encryption procedure should not significantly decrease the compression efficiency if encryption is done first.
3. The encryption should be relatively robust against other common image processing techniques [18, 19, 3].

For all the above reasons, to encrypt image one needs robust method.

Recently, paying attention has been devoted to the use of chaos theory to implement the encryption process. Although much of chaos-based image encryption schemes have been proposed, the class of cryptosystem uses the confusion-diffusion architecture proposed by Fridrich [7]. She suggested that, a chaos-based image encryption scheme should compose the iterations of two processes:-

confusion and **diffusion**. This confusion–diffusion architecture forms the basis of a class of chaos-based image ciphers proposed subsequently. **Confusion** refers to the process of substitution. The confusion (substitution) is intended to make the relationship between the key and the cipher text as complex as possible. **Diffusion** refers to the process of rearranging or spreading out the bit of the message so that redundancy in the plaintext is spread out over the complete cipher-text[18, 13].

The main advantage of these encryptions lies in the observation that, a chaotic signal looks like noise for non-authorized users ignoring the mechanism of generating it. Secondly, time evolution of the chaotic signal strongly depends on the initial conditions and the control parameters of the generating functions then slight variations in these quantities yield quite different time evolutions. In other words, this means that, initial states and control parameters can be efficiently used as keys (with very large key space) in an encryption system. What's more, generating of chaotic signal is often of low cost, which makes it suitable for the encryption of large bulky data[3, 21]. From all the above, chaos-based image encryption appears as a good combination of speed, security and flexibility either a chaotic block cipher or chaotic stream cipher, then both chaotic block or chaotic stream cipher can achieve very good overall performance [4, 19].

2.10.1 Lorenz System

This paper proposes a 3-D Lorenz system based image encryption scheme, which improves the security and performance of the encryption system over conventional simple chaos system based ones. The balance and correlation properties of the analog sequences generated by Lorenz system are analyzed and a pre-process method is proposed, which makes the key stream have good statistical properties. Three initial parameters of Lorenz system are

combined together as one key, which greatly enlarges the key space under precision restricted condition. The encryption speed is also improved since the position permutation and grayscale substitution of a pixel can be done by one iteration operation. Besides, the encryption system is strong against adaptive parameter synchronous attack since it has more complicated structure than simple chaos system based ones.

The dynamic equations of Lorenz system are:

$$\frac{\partial X}{\partial t} = a(Y - X)$$

$$\frac{\partial y}{\partial t} = Bx - ZX - Y$$

$$\frac{\partial Z}{\partial t} = XY - cZ$$

The experimental results indicate that the algorithm is more secure and efficient than conventional algorithms ,the performance and this chaotic system is given in Fig (2.4):-

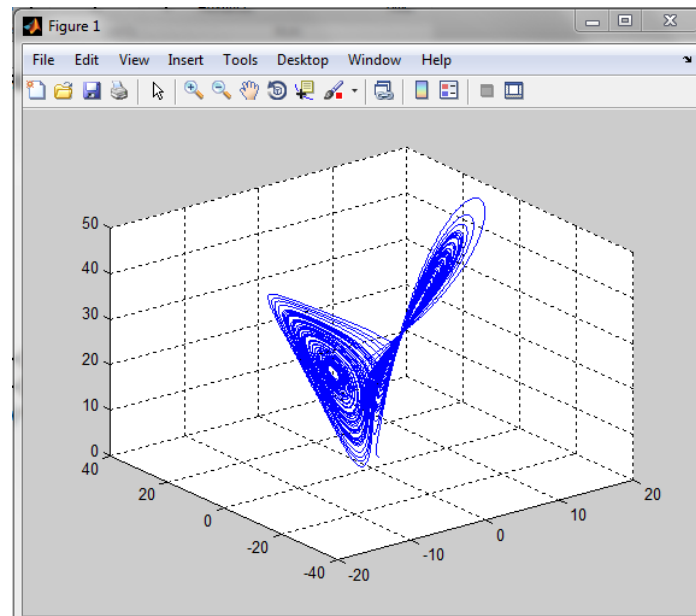


Fig 2.4. Lorenz system

2.10.2 Liu System

Liu system is one of the most important models of recently discovered hyper chaotic systems.

The Liu system (5) is described by the Liu dynamics

$$\dot{x}_1 = a(x_2 - x_1)$$

$$\dot{x}_2 = bx_1 - x_1x_3$$

$$\dot{x}_3 = -cx_3 + dx_1^2$$

where x_1 , x_2 , x_3 are the state variables and a , b , c , d are positive, constant parameters of the system

The Liu system (1) is chaotic when the parameter values are taken as

$$a = 10, b = 40, c = 2.5 \text{ and } d = 4$$

The state orbits of the Liu chaotic system (1) are shown in Figure (2.5).

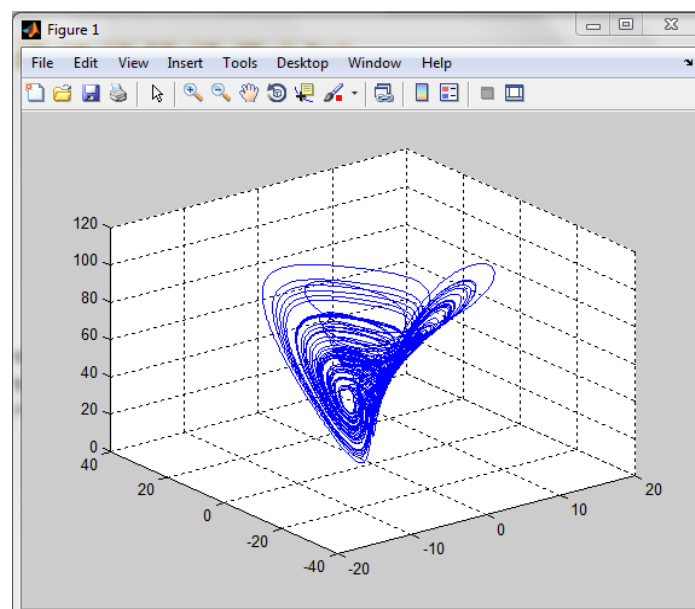


Fig 2.5. Liu System

2.11 Propose system

The proposed system from the transmitter side to the receiver is given in Figure(2.6)

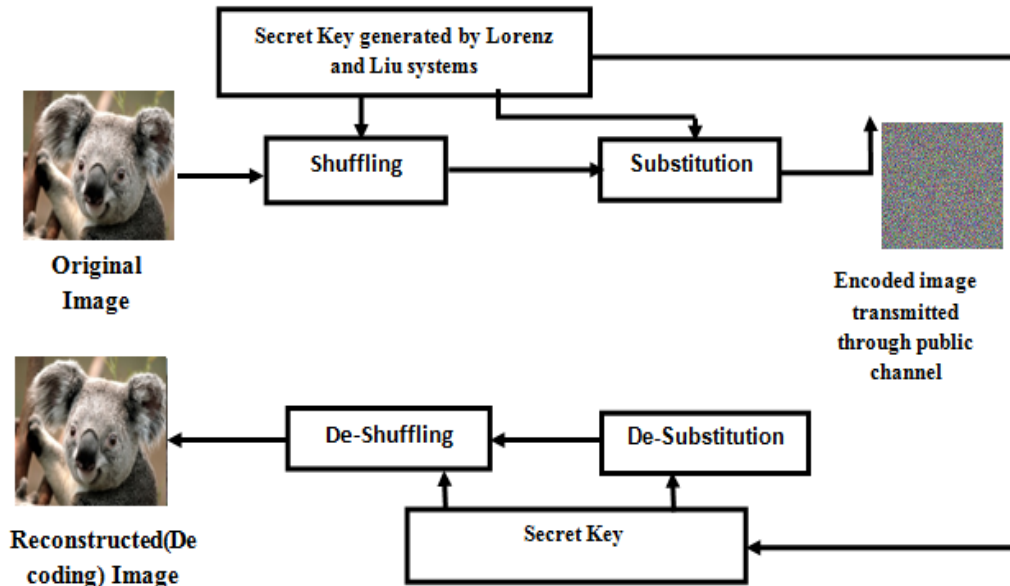


Fig 2.6. Proposed System

2.11.1 Confusion

Refers to the process of substitution. The confusion (substitution) is intended to make the relationship between the key and the cipher text as complex as possible.

2.11.2 Diffusion

Refers to the process of rearranging or spreading out the bit of the message so that redundancy in the plaintext is spread out over the complete cipher text.

The trajectory of both Lorenz and Liu systems can be obtained by the fourth-order Runge-Kutta algorithm with step=0.001. The sixth discrete variables of Chen and Liu systems are adopted to Cryptography the text and the image. The optimization model of Chen system and Liu system are:-

$$X^*(i) = \text{floor}(X(i) \times 10^m)$$

$$Y^*(i) = \text{floor}(Y(i) \times 10^m) \dots \dots \dots (3)$$

$$Z^*(i) = \text{floor}(Z(i) \times 10^m)$$

Where X^* , Y^* and Z^* , are the random number sequences generated by the optimization model of Chen and Liu systems, and $\text{floor}()$ is a rounded down function. One or more of the sequences can be used in the process of cryptography.

2.11.3 Encoding System

The proposed cryptographic algorithm here are applied to the text first separately and then the color image. To apply the algorithm on color image; the first is to divide the color image (24bit/pixels) into three original colors (red (R), green (G) and blue (B) (each color have 8 bits/pixel) and then start proposed algorithm for encoding. Three main algorithms in encoding system:-

2.11.4 Shuffling Algorithm (1-D)

The shuffling algorithm is using the 3-D (3- dimensions) Chen system and 3-D Liu system to generate new key according to propose key schedule:-

$$x_3 = \text{bitxor}(x_1, y_2)$$

$$y_3 = \text{bitxor}(y_1, z_2) \dots \dots \dots (4)$$

$$z_3 = \text{bitxor}(z_1, x_2)$$

From this step gets a new key and makes the work more strength. The (x_3, y_3, z_3) is using to generate the new random numbers sequences and then rearrange this numbers in descending order.

After dividing the color image ($3 \times (M \times N)$) into three color channels (R ($M \times N$), G($M \times N$) and B($M \times N$)) where M is the number of row in image and

N number of column then it is converted each channel from 2-D into 1-D (one row $((M \times N) \times 1)$) and use the indexed position of each element in the descending sequence of the new key to rearrange channel, using sort of X_3 to rearrange R-channel, X_3 to rearrange G-channel and X_3 to rearrange B-channel. Taking into consideration that in each case their own initial conditions but same parameters. In shuffling text is used X_3 once because a text originally (1-D (8 bits/character)).

2.11.5 Substitution of Pixels Value

The keys schedule for this step as shown:-

$$E = \text{bitxor}(x_3, x_2)$$

$$E_1 = \text{bitxor}(y_3, y_2) \dots \dots \dots (5)$$

$$E_2 = \text{bitxor}(z_3, z_2)$$

$$E_3 = \text{bitxor}(\text{bitxor}(E, E_1), E_2)$$

It is easy to suffer chosen-plaintext attack if just shuffling pixels position. The attacker can get the corresponding relationship of pixel's position change by choosing a single pixel change, which is avoidable by the introduction of substitution mechanism [4].

The method is realized by using the random sequences generated by new key schedule as XOR with pixel value in each channel to get new value for each pixel in the color image. The details are as follows:

a) Transform the keys schedule sequence to eight unsigned integer as XOR operand.

$$E4 = \text{mod}(E3, 256) \dots \dots \dots (6)$$

b) Changing the pixel value in each channel (R , G , and B) in the color image.

The resulting image of the shuffling process (1-D for each channel) is used in the process of changing pixels value are as follows (for R-channel and the same steps for both G and B-channel but with different initial conditions):-

New R =bitxor(E3, old R)..... This step for first pixel only.

New R =bitxor(E3,bitxor(new R, old R))..... The new value depending in both old value for pixel and new value for pixel before it.

After the completion of this step is returned to the (2-D) image for each channel.

2.11.6 SHUFFLING ALGORITHM (2-D)

The last step in the encoding process is the process of shuffling 2-D color image. Using the indexed position of each element in the descending sequence of the new key (y3 and z3)to rearrange channels as shown in figure below (for R-channel):

Table (1) Shuffling Algorithm (2-D)

R-channel from image				Sort of y3	Sort of z3	New position of pixel in R-channel according (y3,z3)			
(1,1)	(1,2)	(1,3)	(1,4)	4	2	(4,2)	(4,1)	(4,4)	(4,3)

(2,1)	(2,2)	(2,3)	(2,4)	2	1	(2,2)	(2,1)	(2,4)	(2,3)
(3,1)	(3,2)	(3,3)	(3,4)	1	4	(1,2)	(1,1)	(1,4)	(1,3)
(4,1)	(4,2)	(4,3)	(4,4)	3	3	(3,2)	(3,1)	(3,4)	(3,3)

From table above can see row in R-channel in image rearrange according the sort of secret key y3 and column according the sort of secret key z3, in the same manner both G and B channel rearrangement only different using different initial conditions in each state.

2.11.7 Decoding System

In order to decode the original image you should generate the same key in the same way used in encoding and is used the same relations, but in reverse to get the original image.



Chapter Three

Simulation Results

CHAPTER THREE

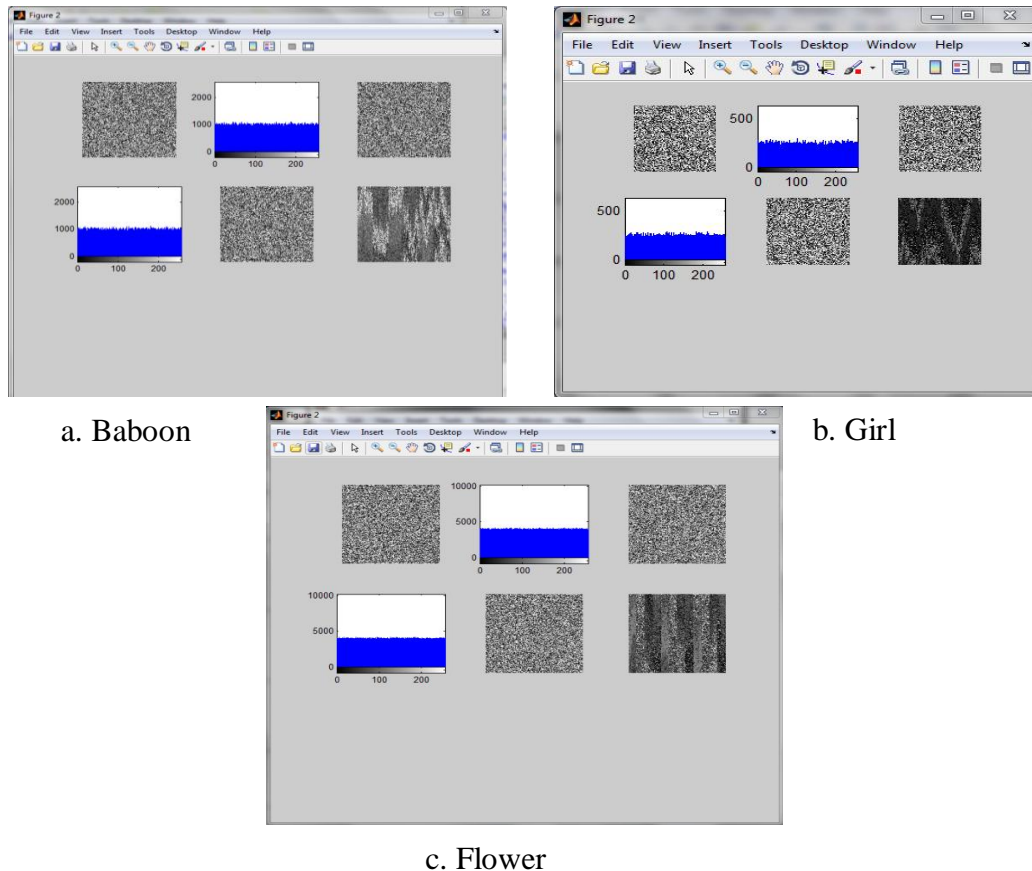
Simulation Results

3.1 Introduction

In this chapter the simulation results of this project are illustrated and discussed, the tests that used to explain the strength of the work are illustrated to.

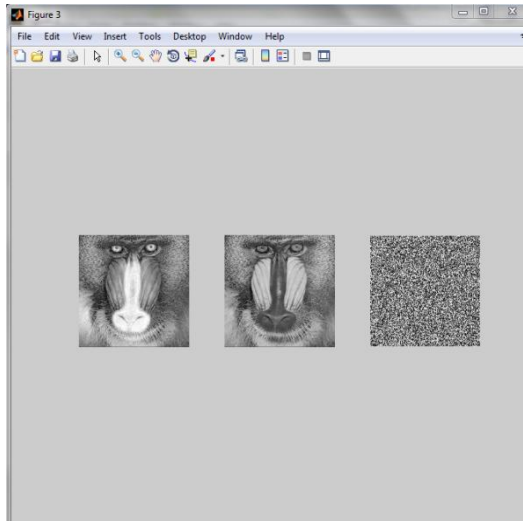
3.2 Results

Figure 3.1 illustrates the encryption of the original images and the histograms of the (Baboon, Girl, Flower).

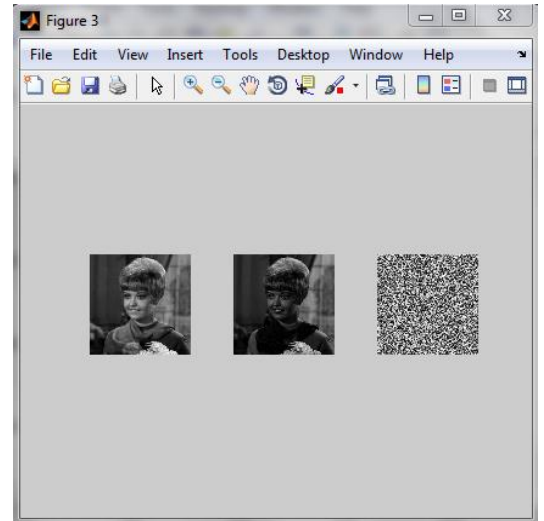


c. Flower
Fig 3.1

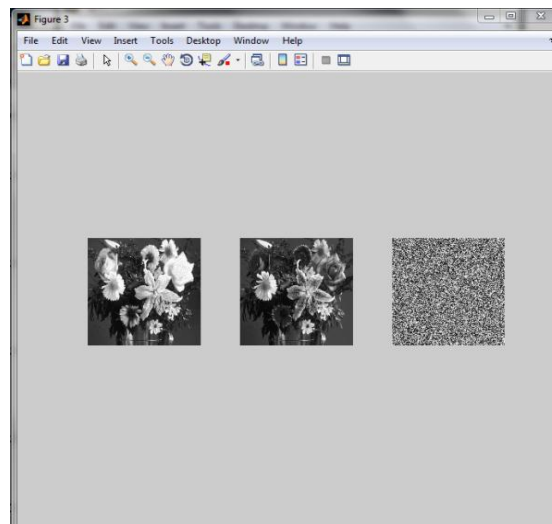
In Figure 3.2, the encryption of the three images is illustrated



a. Baboon



b. Girl



c. Flower

Fig 3.2

3.3 Evaluation of Encryption Process

3.3.1 Statistical Analysis

Shannon said ,in his masterpiece, "It is possible to solve many kinds of ciphers by statistical analysis" and ; therefore , he suggested to methods of diffusion and confusion for frustrating the powerful statistical analysis. Then, many ciphers have been successfully analyzed with the help of statistical analysis and several statistical attacks have been devised on them. Therefore, and ideal cipher should be robust against any statistical attack.

So, this work performs statistical analysis by calculating the histograms and correlations of two adjacent pixels in the plaintext/cipher text. To frustrate the statistical analysis attack, the encrypted image should be characterized by uniform histogram and low correlation between two adjacent pixels.

- **Correlation Coefficients Analysis:-**

Correlation coefficient is the measure of the extent and direction of linear combination of two random variables. If two variables are closely related with stronger association, the correlation coefficient is close to the value 1. On the other hand, if the coefficient is close to 0, the two variables are not related and cannot predict each other. This metric can be calculated, as follows:-

$$\text{Corr}_{xy} = \frac{|\text{cov}(x,y)|}{\sqrt{D(x)} \times \sqrt{D(y)}} \quad 3.1$$

Where:-

x and y are the gray-scale values of two pixels at the same indices in the plain and cipher images, while $\text{cov}(.,.)$ and $D(.)$ are computed, as follows:-

$$E(x) = \frac{1}{N} \sum_{i=1}^N x_i \quad 3.2$$

$$D(X) = \frac{1}{D} \sum_{i=1}^N (x_i - E(x))^2 \quad 3.3$$

$$\text{cov}(x, y) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))(y_i - E(y)) \quad 3.4$$

To test the correlation between two vertically adjacent pixels, two horizontally adjacent pixels, and two diagonally adjacent pixels in an original image/cipher image, are used respectively.

First, randomly select 2000 pairs of adjacent pixels (Horizontal, Vertical, Diagonal) from image (original image and then encrypted image). Then, calculated the correlation coefficient of each pair by using the formulas(3.1, 3.2, 3-3 and 3.4).

Table 1 Correlation Coefficient Values			
Original and encrypted images	Correlation coefficient values		
	Horizontal	Vertical	Diagonal
Original images	0.9798	0.9755	0.9613
Proposed method	3.589×10^{-4}	1.8838×10^{-4}	8.2914×10^{-4}

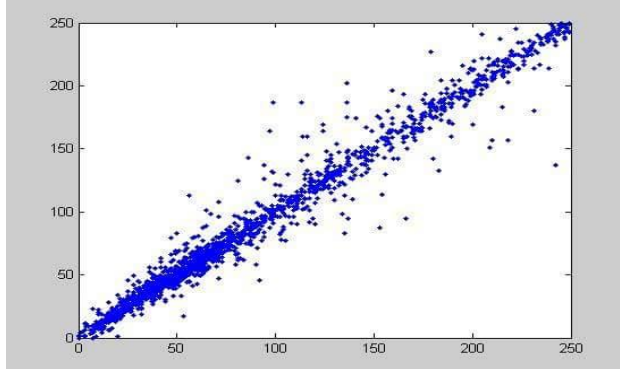
The simulation results shown in Table(1) show the correlation of two adjacent pixels in the plain image and in the cipher image. The correlation coefficient of two horizontal adjacent pixels (girl image) are 0.9798 for original image and 3.589×10^{-4} for cipher image, where similar results for diagonal and vertical directions are obtained. The closer this value is to zero,

the less correlation exists between two adjacent pixels. The results show that, the correlation coefficient is very close to zero in cipher image, and thus the proposed encryption algorithm is less predictable and more secure.

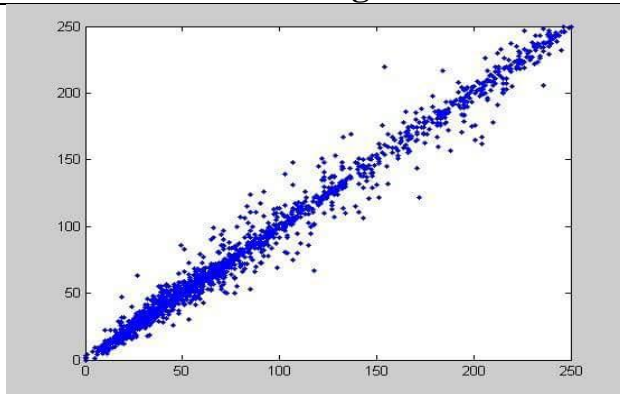
- **Correlation Distribution of Adjacent Pixels**

In the case of correlation distribution of pixels, it should be mentioned that, the closer they are to the main diagonal of the image matrix, the more correlated they are, In cryptography, methods that reduce this similarity to its minimum value in the ciphered image are needed. Then, there will be a very little chance for others to reach the original image by comparing these similarities between pixels. The correlation distribution tests for horizontal, vertical, and diagonal adjacent pixels have been performed for the proposed encryption algorithm and the results are gathered in Figure (3.3).

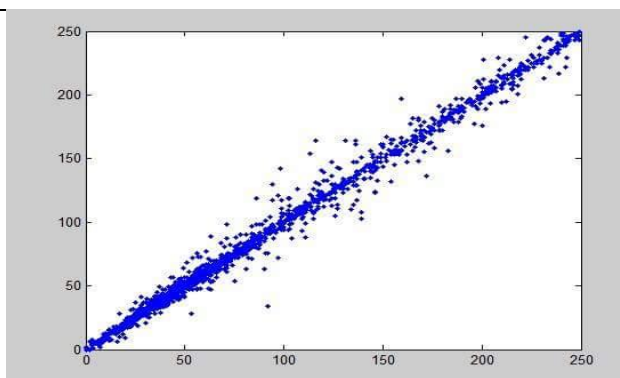
(a)Original images



Pixel gray value on location (X,Y)
Flower diagonal

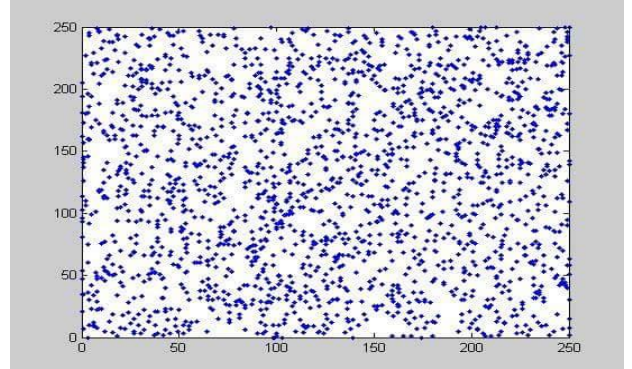


Pixel gray value on location (X,Y)
Flower horizontal

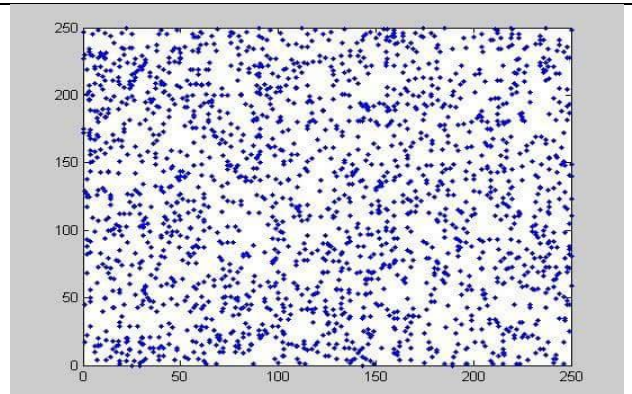


Pixel gray value on location (X,Y)
Flower vertical

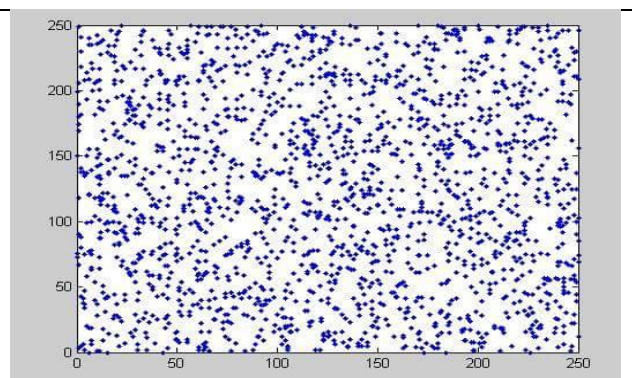
(b)Encryption images



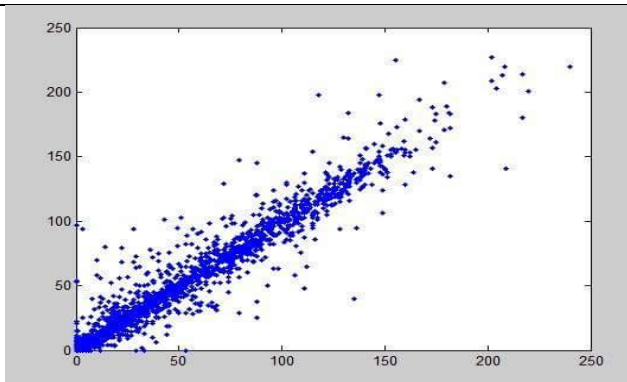
Pixel gray value on location (X,Y)



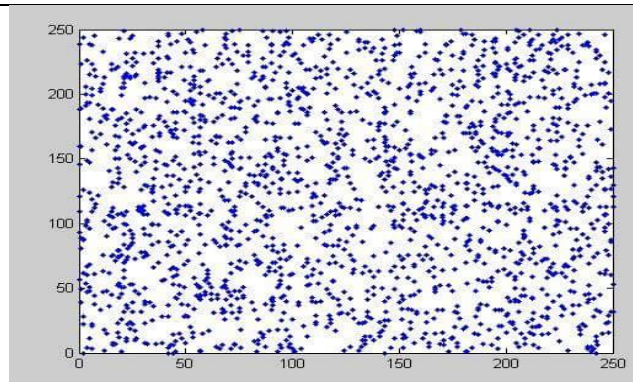
Pixel gray value on location (X,Y)



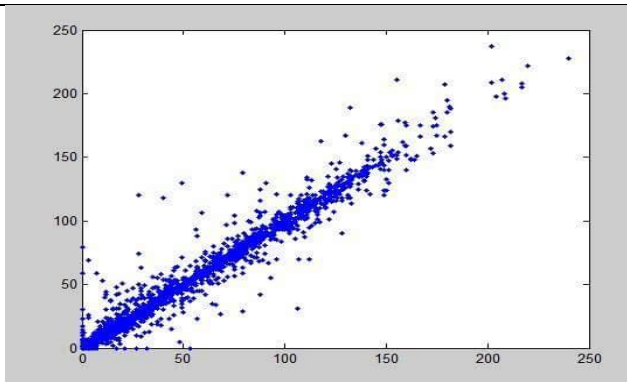
Pixel gray value on location (X,Y)



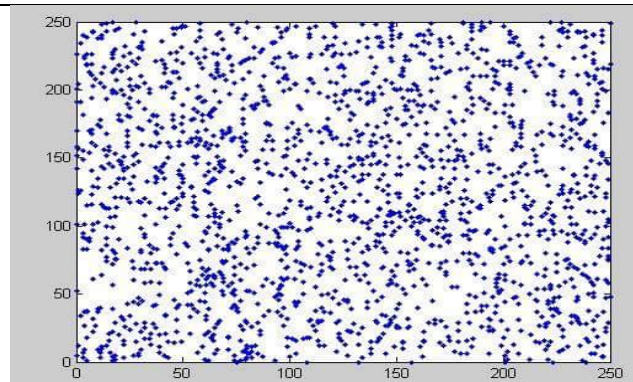
Pixel gray value on location (X,Y)
Baboon diagonal



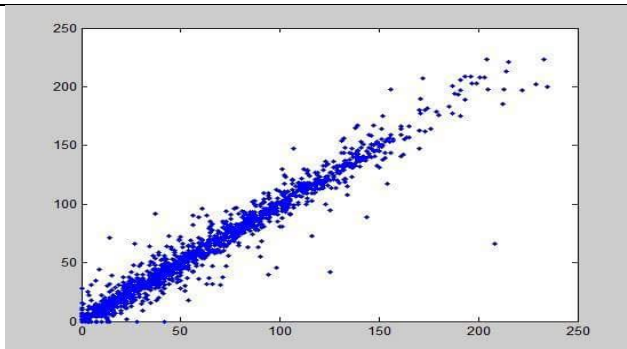
Pixel gray value on location (X,Y)



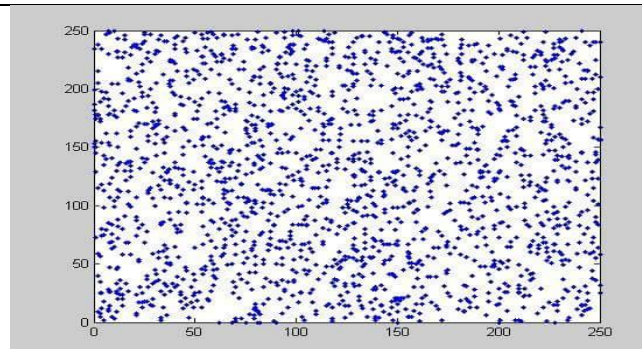
Pixel gray value on location (X,Y)
Baboon horizontal



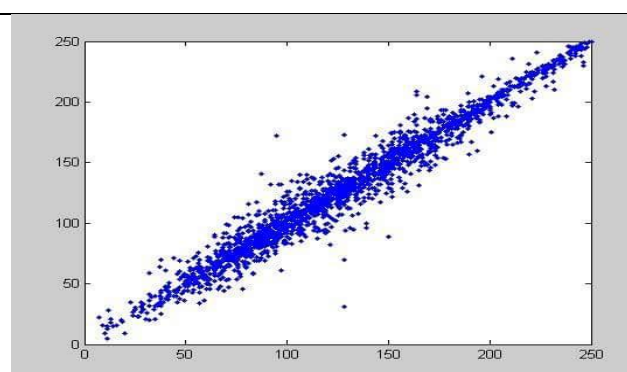
Pixel gray value on location (X,Y)



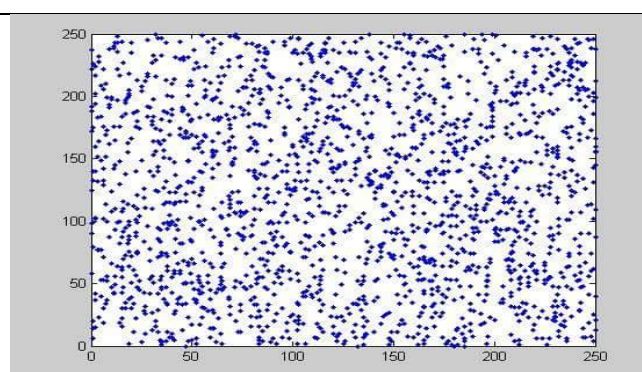
Pixel gray value on location (X,Y)
Baboon vertical



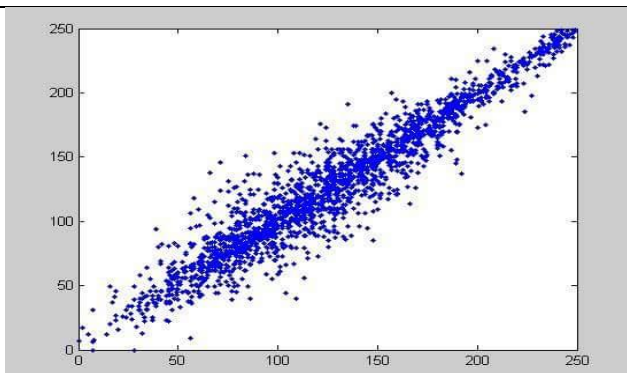
Pixel gray value on location (X,Y)



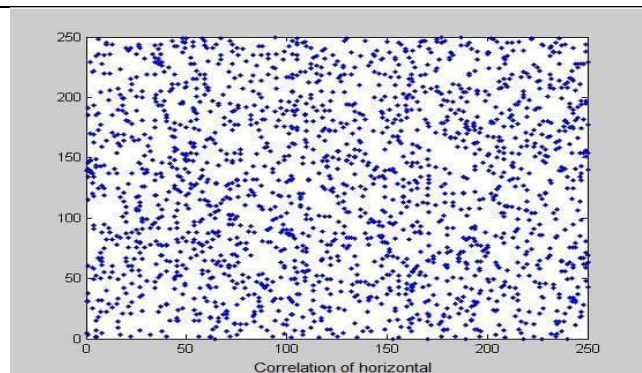
Pixel gray value on location (X,Y)
Girl diagonal



Pixel gray value on location (X,Y)



Pixel gray value on location (X,Y)
Girl horizontal



Pixel gray value on location (X,Y)

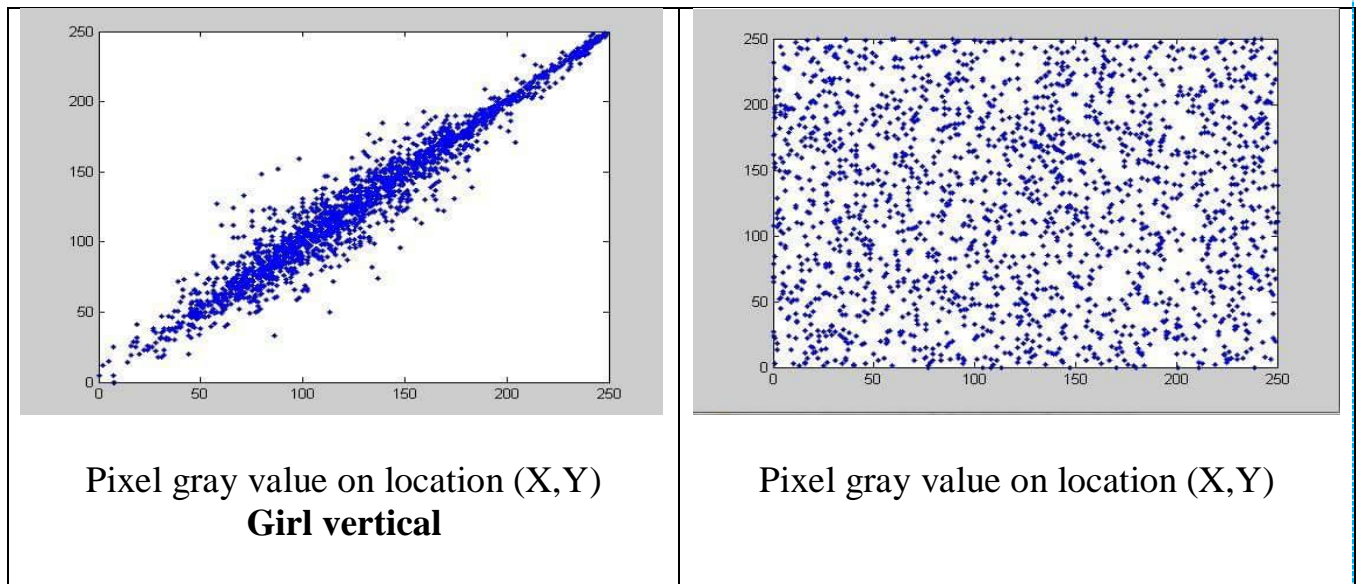


Figure 3.3 Correlation Distribution Test the First Column Shows the Test Result of Original Images. The Second Column Shows the Test Results of Encrypted Images Obtained from the Chaos Encryption

• Histogram Analysis

To prevent the leakage of information to an opponent, it is also advantageous if the cipher image bears little or no statistical similarity to the plain image. An image-histogram illustrates how pixels in an image are distributed by graphing the number of pixels at each color intensity level. A histogram uses a bar graph to profile the occurrence of each gray level of the image. The horizontal axis represents the gray level value. It begins at zero and goes to the number of gray levels. Each vertical bar represents the number of times of corresponding gray level occurs in the image. For image encryption algorithms, the histogram of the encrypted image should have two properties:-

1. It must be totally different from the histogram of the original image.
2. It must have a uniform distribution, which means that the probability of existence of any gray scale value is the same, and it is totally random.

The histogram is illustrated in figure 3.2

3.3.2 Differential Analysis

To test the influence of one pixel change on the whole cipher -image, two most common measures **NPCR**(Number of **P**ixel **C**hange **R**ate; means the change rate of the number of pixel of ciphered image while one pixel of original image is change) and **UACI** (**U**nified **A**verage **C**hanging **I**ntensity; measures the average intensity of the differences between the original and ciphered image) are used. Let the two cipher images be C1 and C2, whose corresponding plain images have only one pixel difference. Label the gray values of the pixels at grid (i, j) in C1 and C2 by C1(i, j) and C2(i, j), respectively. Define a bipolar array D with the same size as image C1 or C2, namely, if C1(i, j) =C2(i, j) then D(i, j) =0, otherwise D(i, j) =1. The NPCR and UACI are defined by:-

$$\text{NPCR} = \frac{\sum_{i,j} D(i,j)}{2M \times N} \times 100\% \quad 3.5$$

$$\text{UACI} = \frac{1}{2M \times N} \left[\sum_{i,j} \frac{|c_1(i,j) - c_2(i,j)|}{255} \right] \times 100\% \quad 3.6$$

Where :- 2M: height of the cipher image, N: width of the cipher image. The higher the values of NPCR and UACI are the better the encryption. The results of these two tests are shown in Table2 (a & b).

a. NPCR Results		
Image name	Color	Proposed Encrypted Image
Girl	R	99.66
	G	99.60
	B	99.62
Baboon	R	99.60
	G	99.60
	B	99.62
Flower	R	99.60
	G	99.61
	B	99.62

b. UASI Results		
Image Name	color	Proposed Encrypted Image
Girl	R	33.46
	G	33.49
	B	33.57

Baboon	R	33.44
	G	33.43
	B	33.50
Flower	R	33.47
	G	33.49
	B	33.48

3.3.3 Information Entropy

Entropy (E) is one of the most outstanding features that makes the images have a random-like behavior. Information entropy can be used to characterize the confusion, and is calculated by :-

$$E(C) = \sum P(C_{i,j}) \log_2(1/P(C_{i,j})) \quad 3.7$$

Where:- $P(c_{i,j})$ represents the probability of symbol $c_{i,j}$ for a grayscale image, if $2^8 = 256$ intensities appear with equal probability, the entropy $E(C)$ reaches the maximum value of 8.

Table3 Entropy Values for Red , Green, and Blue colors				
Image	color	Girl	Mandrill	Flower
Original Image	R	7.2711	7.6515	7.4815
	G	7.0319	7.3488	7.2924

	B	6.8594	7.6692	7.5072
Proposed Image	R	7.9970	7.9993	7.9998
	G	7.9972	7.9993	7.9998
	B	7.9974	7.9994	7.9998

It is observed from Table (3) that, the proposed method achieves outstanding confusion , and outperforms the CS-based methods , in the sense that the corresponding entropy $E(C)$ is more close to the maximum value of 8.



CHAPTER FOUR

Conclusions and Suggestions for Future Works

CHAPTER FOUR

Conclusions and Suggestions for Future Works

4.1 Conclusions

In this work, the cryptography using a secret key that implemented by two chaotic systems CHEN and LIU is performed for three different images and an important tests was illustrates the strength of the this works is performed too.

The main conclusions are:

- 1- Using of two chaotic system to generate the secret key can provide large key space and more secret system which prevent cryptanalyst from listen or take the transmitted message.
- 2- Chaos technique improve the performance of the cryptography system as compared with other traditional systems such as Advantage Encryption standard 9AES) Data Encryption Standard (DES) and others.
- 3- It can be found that the proposed algorithm provides very powerful and secret cryptography method.
- 4- The analysis of the system performances shows that the proposed system has a large key space to resist brute-force attacks, high key sensitivity.
- 5- The system is strong against differential attack, achieve good randomness, high security against statistical attacks, the execution time is very small and final simple of the system design.

6- In this system, the calculation of the entropy of proposed images with different initial conditions is done. Results show that all values are very close to 8, with an average of 7.99.

7- From the results that was obtained, it is found that the original images can be retuned at the receiver which means that the errors is very small.

4.2 Suggestions for Future Works

More than two chaotic system can be used to generate the secret key to provide more security and prevent the cryptanalyst from listening or received information, this system can be used to encrypt video by dividing it to many frames and encrypt them.



REFERENCES

REFERENCES

- [1] Nicholas G. McDonald **“PAST, PRESENT, AND FUTURE METHODS OF CRYPTOGRAPHY AND DATA ENCRYPTIONDigital Image Encryption”**
Department of Electrical and Computer Engineering University of Utah.
 - [2] Sreedhanya **“What is Chaos Theory”**, *Computing and communications,2006 .*
 - [3] Gonzalo Alvarez¹ and Shujun Li² **“Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems** *Department of Electronic and Information Engineering, Hong Kong Polytechnic University,Hung Hom, Kowloon, Hong Kong SAR, China.2006.*
 - [4] Yaron Rachlin and Dror Baron **“The Secrecy of Compressed Sensing Measurements”**, *2008.*
 - [5] Sundarapandian Vaidyanathan **“HYBRID SYNCHRONIZATION OF LIU AND LÜ CHAOTIC SYSTEMS VIA ADAPTIVE CONTROL”** *2011.*
 - [6] ¹Priyanka Agrawal, ²Manisha Rajpoot **“Partial Encryption Algorithm for Secure Transmission of Multimedia Messages”**, *1,2Dept. of CSE, RCET, Bhilai, CG, india .2012.*
 - [7] Hayder Raheem Hashima, Irtifaa Abdalkadum Neamaab **“Image Encryption and Decryption in A Modification of ElGamal Cryptosystem in MATLAB”**, *a Department of Mathematics, Faculty of Computer Science and Mathematics, University of Kufa, Najaf, Iraq hayderr.almuswi@uokufa.edu.iq b Department of Mathematics, Faculty of Computer Science and Mathematics, University of Kufa, Najaf.*
-

- [8] Avi Kak **“Classical Encryption Techniques”**, *Avinash Kak, Purdue University 2016.*
 - [9] K. Klomkam, A. Jansri &P. Sooraksa **“TERMINOLOGY AND SYSTEM TYPES”**,2004.
 - [10] Gary C. Kessler **“An Overview of Cryptography”** ,2006.
 - [11] H. H. Nien, S. K. Changchien, S. Y. Wu & C. K. Huang **“Math3024 Elementary Cryptography and Protocols”**, *The University of Sydney.*
 - [12] A. Orsdemir, H. Oktay Altun, G. Sharma &Mark F. Bocko **“On The Security and Robustness of Encryption via Compressed Sensing”**, *IEEE Military Communications Conference(MILCOM),pp. 1-7, 2008, .*
 - [13] Pianhui Wu **“Research on Digital Image Watermark Encryption Based on Hyperchaos”**, 2013.
 - [14] Afnan Sameer Yaseen Al-Ali **“Chaos Encryption Methods for Partial Encryption of Wavelet-based Images”**, *Submitted to the Council of the College of Engineering, University of Basrah in Partial Fulfillment of the Requirements for the Degree of Master of Science in Computer Engineering, 2008.*
 - [15] A. A. Kumar &A. Makur **“Stream Ciphers”**, *TENCON IEEE Region 10 Conference, 2009.*
 - [16] W. Yu, C. Chi, X. Wei& X. Yang **“Advantages and Disadvantages of Asymmetric and Symmetric Cryptosystems”**, *IEEE Intelligent Control and Information Processing (ICICIP),International Conference, Dalian, China, pp. 463 – 467,2010,*
-

- [17] William Stallings **“CRYPTOGRAPHY AND NETWORK SECURITY PRINCIPLES AND PRACTICE”**, *Boston Columbus Indianapolis New York San Francisco Upper Saddle River Amsterdam Cape Town Dubai London Madrid Milan Munich Paris Montreal Toronto Delhi Mexico City Sao Paulo Sydney Hong Kong Seoul Singapore Taipei Tokyo*, 2011.
 - [18] H. NYQUIST¹ **“Certain Topics in Telegraph Transmission Theor-y”**, *Member, A. I. E. E.*, 2008.
 - [19] Zhaopin Su, Guofu Zhang and Jianguo Jiang **“Multimedia Security: A Survey of Chaos-Based Encryption Technology”**, *School of Computer and Information, Hefei University of Technology China*.
 - [20] JIRI FRIDRICH **“SYMMETRIC CIPHERS BASED ON TWO DIMENSIONAL CHAOTIC MAPS”**, *Center for Intelligent Systems, Department of Systems Science and Industrial Engineering, SUNY Binghamton, Binghamton, NY 13902-6000, USA Received July 1, 1997; Revised December 8, 1997*.
 - [21] CLYDE-EMMANUEL ESTORNINHO MEADOR **“NUMERICAL CALCULATION OF LYAPUNOV EXPONENTS FOR THREE-DIMENSIONAL SYSTEMS OF ORDINARY DIFFERENTIAL EQUATIONS”**, *A Thesis submitted to the Graduate College of Marshall University, Marshall University*, 2011.
 - [22] Yaobin Mao¹ and Guanrong Chen² **“Chaos-Based Image Encryption”**, *1Nanjing University of Science and Technology maoyaobin@163.com ,2 City University of Hong Kong gchen@ee.cityu.edu.hk*.
-

الملخص

بسبب التطور الكبير في أنظمة الاتصالات مثل الإنترنت والجوال والقنوات الفضائية، الخ. وهناك معلومات كبيرة يتم إرسالها واستقبالها وبعض هذه المعلومات مهم جداً ويجب أن يكون في غاية السرية ولذلك يجب أن تكون مشفرة لمنع الشخص المتطفل أو ما يسمى بالشخص الثالث من الاستماع للبيانات المرسلّة أو تغييرها، والفكرة الرئيسية لتقنية التشفير يخرج من العلاقة بين المعلومات الأصلية أو البيانات والشفرات والتشفير. ويمكن الحصول على تشفير قوي عندما لا يكون هناك علاقة مطلقة بين الشفرات والبيانات الأصلية وأنه من الممكن لإعادة بناء البيانات الأصلية بأسهل الطرق. المفتاح السري مهم جداً لتشفير البيانات مثل النص والصورة والصوت والفيديو، وهناك تقنيات مختلفة تستخدم لتوليد مفتاح، وقد حازت طريقة توليد المفتاح باستخدام النظام الفوضوي اهتماماً كبيراً لما لها من التعقيد وكذا تشعب السلوكيات ومن المعروف أنها أكثر عشوائية وغير قابلة للتنبؤ، فإنه يمكن أن يتم الاستفادة منه في تحقيق التشفير. لذلك في الأعوام اهتم عدد كبير من الأبحاث في استخدام هذا النظام لتشفير البيانات.

في هذا المشروع يتم استخدام نظام الفوضى للحصول على المفتاح، حيث تم استخدام نوعين من نظام الفوضى هما (ليو، لورنز). مفتاح التشفير الذي تم إنشاؤه هو الجزء المهم لتصميم نظام التشفير، فإنه يحدد بشكل مباشر أمن وكفاءة نظام التشفير ولكن معظم المفاتيح الرئيسية المقترحة هي استخدام النظام الثنائي وتعاني من استخدام مفتاح ذا طول قليل وفضاء المفتاح قليل ومحدد، يتحقق تشفير الصورة عن طريق تغيير موقع البكسلات في الصورة الأصلية وتغيير قيمتها أيضاً بالاعتماد على المفتاح الذي تم إنشاؤه من قبل أنظمة ليو ولورينز وقد تبين من النتائج المتحصل عليها أن المفاتيح المتولدة من هذه النظام سرية وفعالة بشكل كبير جداً وبالتالي أن النظام المقترح مؤمن بشكل جيد لأنه لديه مساحة عالية رئيسي، حساسية عالية للشروط الابتدائية، تشفير مؤمن بشكل جيد، وانخفاض التتابع بين البكسلات المتجاورة وبالتالي قوي ضد طرق التحليل المختلفة من قبل الشخص الثالث وأخيراً وقت انجاز العملية قليل.