ROBUST IMAGE ENCRYPTION METHOD WITH CIPHER STREAM CHAINING PROCESS

SOVAN TEP

A THESIS REPORT SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF ENGINEERING IN COMPUTING IN ENGINEERING SYSTEM
INTERNATIONAL COLLEGE
KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG
ACADEMIC YEAR 2018
KMITL-2018-IC-M-11-06

ROBUST IMAGE ENCRYPTION METHOD WITH CIPHER STREAM CHAINING PROCESS

SOVAN TEP

A THESIS REPORT SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF ENGINEERING IN COMPUTING IN ENGINEERING SYSTEM
INTERNATIONAL COLLEGE
KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG
ACADEMIC YEAR 2018
KMITL-2018-IC-M-11-06

Thesis Title	Robust Image Encryption Method with Cipher Stream Chaining Process
Student	Sovan TEP
Student ID	60610023
Degree	Master of Engineering
Program	Computational Intelligent System
Advisor	Dr. Isara Anantavrasilp

ABSTRACT

Security of multimedia data during the transmission is one of the main concern of vulnerable connection. In order to protect the data, cryptography has been employed by many techniques to hide the real information. An image encryption algorithm that uses one dimensional logistic map combined with perceptron model is proposed. The algorithm uses logistic map to produce pseudo random sequences, which are used as sequences of keys to specify the weights of the perceptron. The perceptron is then used to encrypt the pixels of the image. The approach is also equipped with the novel process called Cipher Stream Chaining Process (CSCP), making it highly sensitive to given image. Our work is evaluated against histogram analysis, information entropy, key sensitivity analysis. Experiment results show that, the cipher image does not give out any information on the plain image and the algorithm is highly sensitive to plain image and key. The results of the Number of Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI) are also better comparing to the algorithm without CSCP.

Acknowledgments

This work would have been impossible, if there is no the treasured contributions and support from the following people. First and foremost, I would like to express all my gratitude and thank to both my advisor Dr. Isara Anantavrasilp of International College for his valued supervision, encouragement and suggestion to win all the problems and obstacles since the first day of my project until the last day of my study here. Additionally, I also would like to thank all lecturers and staff of KMITL who have provided the proper knowledge and services to fulfill my research and work with their worth contributions and time. Furthermore, I also need to show my gratitude to AUN Seed Net scholarship and staff for providing the big opportunity for me to conduct my master degree here with an appropriate financial support and help for this whole two years. Finally, is for my family and friends for their power of love and taking care to rich my motivation through these years. Because of these people above, my best achievement has brighten my educational life.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Background

Today, the Internet is used, not only for legacy services such as email, chat or file transfer, but also social interaction, multimedia, games and other entertainment. Countless amount of non-textual data such as images, video and audio are being shared and transferred every day. This raises privacy and security concerns, especially for personal multimedia data. In order to protect such information, one traditional way is to encrypt the content of the data before transmission. This kind of techniques is called Cryptography. In cryptography, the original message may contain all kind of information including images. The original message is transformed into a cipher message that is hard to decipher.

Several data encryption standards such as DES, triple DES, AES have been introduced. However, such algorithms may only be suitable to encrypt textual data [1], but not multimedia one. The reason is that multimedia data especially images and videos may be highly redundant (adjacent pixels may contain the same color). Thus, human may still be able to perceive the original image from the cipher image [2]. Multimedia data are also much larger than textual ones.

1.2 Problem Descriptions

Recently, the encryption scheme based on the chaotic map has been employed to encrypt the image due to its nonlinear behavior [3]. The word chaotic mean the state of disorder. This kind of

techniques are very sensitive to the initial condition. A slightly change in the initial point can lead to two different divergence outcomes. Logistic map is one of the chaos map. Advantages of using the logistic map to encrypt the image is because it is simple in implementation [4]. In [5], they proposed new way to scramble the image pixel using perceptron model. In the experimental result, their proposed method yield better than using XOR operation in term of encrypting the image value. However, their algorithms encrypt the image separately. As the result, the output image pixel values are not depend on each other. Thus, they are not sensitive to plain image. That is, if some parts of the plain image are change, only some part of cipher image change accordingly. Therefore, the algorithm are vulnerable to the differential analysis attack. To be resistant to differential analysis attack analysis, a good cryptography algorithms should be sensitive with respect to the given key and plain image. It mean that if the input key of algorithms is changed, the output of the encryption must also change. Also, if the plain image is change, the cipher image must be different [6]. Therefore, in this thesis we are trying to proposed the algorithm which is highly secure especially resistant to the differential analysis attack.

1.3 Research Objectives

In this research work, the aim is to design and implement new algorithms for image encryption. The algorithm must be able to produce the cipher image which is not understandable. And the key generator of the algorithm must be highly secure. That mean even if a slightly change to the key, the original image can not be retrieved back. Moreover, the algorithm must achieve the sensitivity with respect to the plain image. Therefore, it is strong against differential analysis attack.

Chapter 2

Literature Review

This chapter discusses background study and some of the related works. we also discuss about the weakness of the related works.

2.1 Research Background

Basing on the information security, the science of cryptology functions is the main solution to hide the originated information. Cryptology consists of two are cryptography and cryptanalysis [7]. Both of them are the study of creating and solving the problems including encryption and decryption.

Figure 2.1: Cryptology

1. Cryptography is the study of making a cryptosystem that is capable of providing information security [8]. Cryptography deals with the actual securing of digital data. It refers to the design of mechanisms. Such techniques are generally based on math algorithms that provide fundamental information security services.

2. The fields of researches trying to break the cipher text is known as cryptanalysis [9]. Cryptanalysis is the sister branch of cryptography and they both co-exist. The cryptographic process results in the cipher text for transmission or storage. Cryptanalysis involves the study of cryptographic mechanisms with the intention to break them. Cryptanalysis is also used during the design of the new cryptographic techniques to test their security strengths.

   In summary, Cryptography concerns with the design of cryptosystems, while cryptanalysis studies the breaking of cryptosystems.

Cryptosystem is the the technique to provide confidentiality of the information[10]. It is also known as the cryptographic algorithms. It is the study to create pair of algorithms call encryption and decryption . In the following section of the chapter, cryptosystem and related study will be described in detail.

2.1.1 Cryptosystem

A cryptosystem is an implementation of cryptographic techniques. A cryptosystem is also referred to as a cipher system. There are several important components in this process such as:

1. plaint text: It is the original information to be sent by the sender.

2. Cipher text: Cipher text is the scramble version of the plain text produced by the encryption algorithm using the certain key.

3. Encryption algorithm: It is the process to produce cipher text for any given plain text. In the sender node, it takes the original information (plain text) and key as the input and product the cipher text as the output. The role of the encryption key is used to scramble the plain text.

4. Decryption algorithm: The decryption algorithms is the reverse process of the encryption algorithms. In the receiver node, the algorithm takes the cipher text as the input and convert

it to the original plain text as the output. The role of the decryption key is used to unsramble the cipher text back to the plain text.

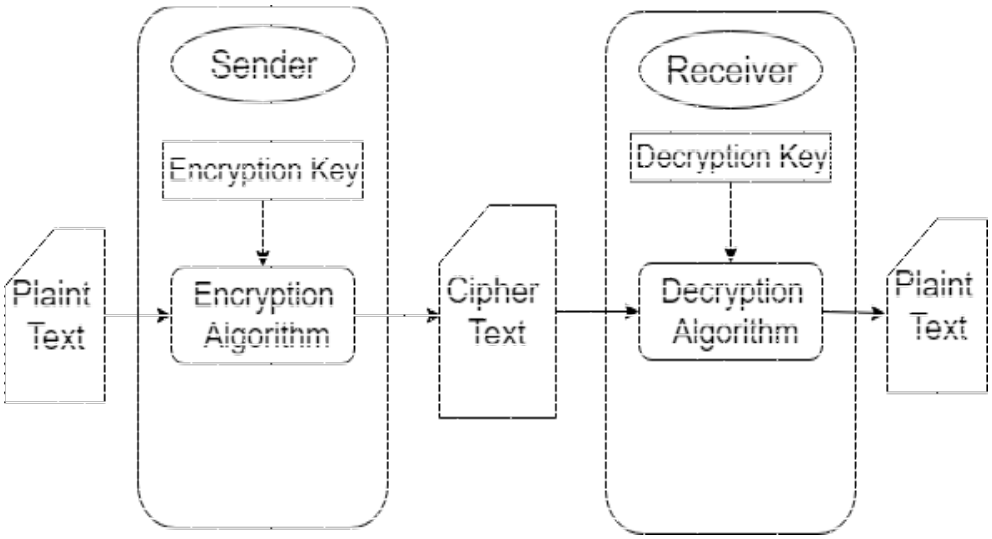


Figure 2.2: cryptosystem

In figure 2.2, it can be seen that the information sent by the sender is encrypted. Then, the message is decrypted back when it reaches the destination and is received by the receiver. In the end, only the sender and receiver could understand the content of the message. This to ensure the information is not leaked out to the third party.

2.1.2 Type of Cryptosystem

Generally, there are two main types of the cryptosystem which are symmetric key algorithm and asymmetric key algorithm.

1. Symmetric key: is a type of encryption where only one key is used at both the transmitter and receiver side [11]. The study of the symmetric cryptosystem is known as the symmetric cryptography. By using symmetric encryption algorithms, data is converted to a form that cannot be understood by anyone who does not possess the secret key to decrypt it. Once the intended receiver who possesses the key has the message, the algorithm reverses its action so that the message is returned to its original and understandable form. The secret key that the sender and receiver both use could be a specific password/code or it can be random string of letters or numbers that have been generated by a secure random number generator (RNG).

The flow or process of this symmetric cryptography is depicted in the figure 2.3 below:

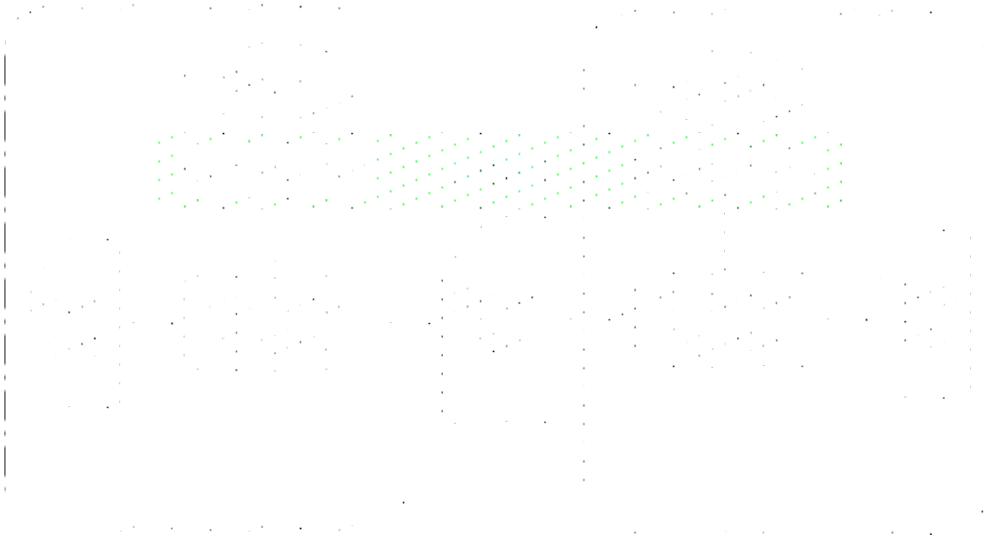


Figure 2.3: Cryptology

There are two different kinds of symmetric key algorithm are block encryption [12] and stream encryption [13]. In block encryption, a set of bits length are encrypted in blocks with the use of a specific secret key. As the data is being encrypted, the system holds the data in its memory as it waits for complete blocks. In stream encryption, data is encrypted bit by bit from the first to the end. In this case, the value no need to be retained in the system's memory. A few well-known examples of symmetric key encryption methods are:

(a) Data Encryption Standard (DES) [14]

(b) Triple DES (3DES) [15]

(c) Advance Encryption Standard (AES) [16]

(d) Rivest Cipher 4 (RC4) [17]

(e) Rivest Cipher 5 (RC5) [18]

(f) Rivest Cipher 6 (RC6) [19]

AES, DES, triple DES and RC5 are block ciphers and RC4 and RC6 is stream cipher.

(a) **Strength:** A symmetric cryptosystem is faster[20].It requires less computation power the create the keys. A system only which possesses the secret key can decrypt a message.

(b) **Weakness:** It has the problem with the key transportation [21].The secret key is to be transmitted to the receiving system before transferring the actual message. So the only secure way of exchanging keys would be exchanging them personally.

2. Asymmetric key: is a type of encryption where different keys are used for encrypting and decrypting the information [22]. The study of the asymmetric cryptosystem is known as the asymmetric cryptography. There are two keys used in this mode. One is called private key and another one is called public key. It is mentioned that these two keys are mathematically related even though they are different.

   The process of this asymmetric cryptography is depicted in the figure 2.4 below:

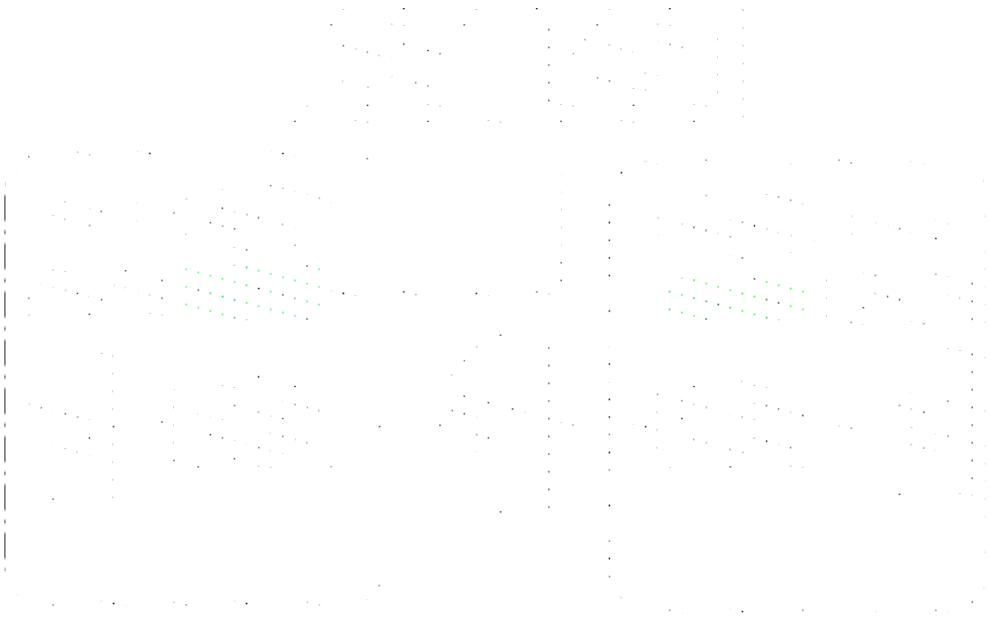


Figure 2.4: Cryptology

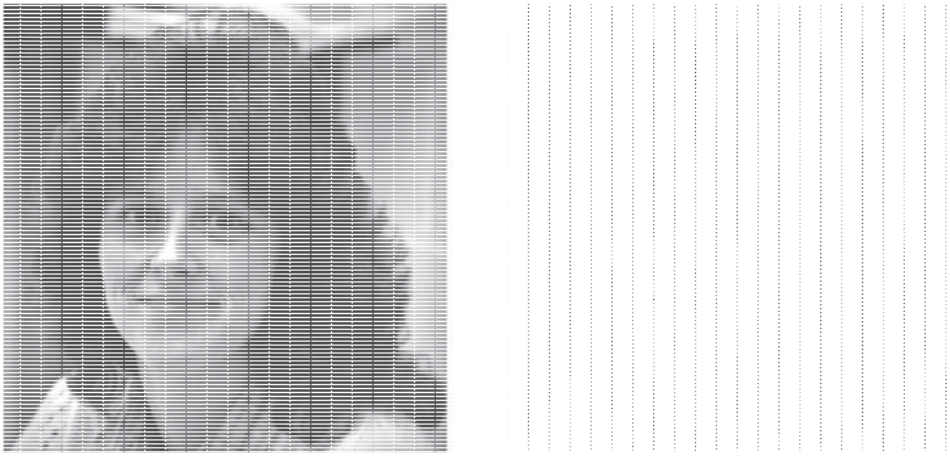
As shown in the figure, the public key is put freely available that everyone can reach. The sender is able to access the public key which represent receiver location. The public key is then used for encrypting the message. As the private/second key is kept secret within the receiver. In this case, no one can understand the message beside the intended person. The security over this mode is that a message that is encrypted using a public key can only be decrypted using a private key. Popular asymmetric key encryption algorithm includes RSA [23], DSA [24], Elliptic curve techniques [25].

(a) **Strength:** The primary advantage of public-key cryptography is increased security: the private keys do not ever need to be transmitted or revealed to anyone [21]. The unique private and public keys provided to each user allow them to conduct secure exchanges of information without any secret.

(b) **Weakness:** A disadvantage of using public-key cryptography for encryption is speed [20]. Asymmetric keys must be many times longer than keys in secret-cryptography in order to boast equivalent security.So, the computation become more intensive to generate the keys.

Even though there are many algorithms in the field, they still have the strength and the weakness. On the other hand, each of them can be used for a specific purposed toward the application since none among all of them could be recognized as the best one [26]. Thus, the good use of the cryptography method for the application is to choose the most suitable one, instead of choosing the best one. In this book, the cryptography algorithms based on the symmetric key is studied. The algorithms was implemented as an image-based encryption using cipher stream encryption.The detail of the algorithm is described in the chapter 3.

2.2 Related Studies



(a) Original image (b) Encrypted image

Figure 2.5: Image Encryption using AES

In the last decade, there are many algorithms have been proposed in cryptography. In symmetric cryptography, there are several conventional method such as DES, triple DES, AES used widely in today internet. Those standard methods are the block cipher algorithm. As its name suggested, they encrypted the information block by block. However, these type of algorithms are found as vulnerable algorithms for the large information like image or video [2], as seen in figure 2.5. This has lead to the rising of the stream cipher algorithms. Since the algorithms encrypt the data bit by bit, it is known as the effective way to encrypt the redundant pixels(adjacent pixel have similar color) of the image. Many algorithms using chaos-based application have been proposed. Hanchinamani and Kulkarn [27] proposed the image encryption based on the Peter de Jong chaotic map [28] and a RC4 stream cipher [29]. The algorithms involve with three steps:

1. **Permutation**: Scramble the position of the row and column along with the circular rotations in the alternative orientation. This is to decorrelate the adjacent pixels of the image based on the value obtained from chaotic map.

2. **Pixel value circular rotation**: Changing the value of the pixels.

3. **Diffusion**: Spreading the effectiveness of each pixel over the entire image. Thanks to their two rounds of encryption, the scheme is very sensitive the plain image. Hence, the algorithm is robust against differential attack.

Long and Tan [30] proposed multiple chaotic map for the digital image encryption. The algorithm consists of three chaotic maps: Chebyhev map [31], Nonlinear Chaotic Algorithm (NCA)[32] and Logistic map. The algorithm produces the keys of the encryption and decryption which are generated by the plaintext values and Chebyshev map. The keys are then fed into Logistic map and NCA for confusing and shuffling the plain image respectively.

Rohith et al. [4] proposed image encryption using 1-D logistic map because it is simple to implement but very efficient. The algorithm uses map function to generate pseudo-random sequence as the key streams. Then it applies XOR operation with a new sequence, generated from linear feedback shift register to produce another set of key streams. Finally, they use the last output key steams to confuse the image pixel by using XOR operation.

Wang et al. [5] proposed encryption algorithm based on Lorenz chaotic map without XOR operation, instead they introduce a new way to scramble the image pixel value using a perceptron

model. Due to the complex structure of the perceptron, it is a good approach for confusing and changing the pixel values of the image.

In [33], they proposed new image encryption method using double logistic map. The algorithm produces two sequence keys in two phase. First, an encryption key is generated through a process of K_1 being XORed with K_2 to create new key K_3. This new key K_4 is later XORed with the original image in the second phase. Finally, the result of the histogram show much flatter and result of the meas square error is better comparing to the images produced by one logistic map.

In [34], a new method is proposed using 2D cat map and shadow number. The algorithm based on the concept of scrambling the position of pixels, and changing the pixel intensity value. The algorithm based on two major step. The first one is scrambling image with the uniform distribution using two dimensional cat map. The second step is modifying a method of shadow process algorithm. This modification makes the shadow process suitable to work efficiently with image. The performance of the proposed algorithm give high uncorrelated between adjacent pixel in the encrypted image and with the high entropy.

In [35], an improved diffusion strategy is proposed to promote the efficiency of the most widely investigated permutation-diffusion type of the image cipher. By using the novel bidirectional diffusion strategy, the spreading process is significantly accelerated and hence the same level of security can be achieved with fewer overall encryption round. Moreover, to further enhance the security of the cryptosystem, a plain-text related chaotic orbit turbulence mechanism is introduced in diffusion procedure by perturbing the control parameter of the employed chaotic system according to the cipher-pixel. Result of the analysis indicated that the new scheme has a satisfactory security level with a low computational complexity.

To be resistant to differential analysis attack, a good cryptosystem should be sensitive with respect to the given key and plain image. Even just one bit of the key is flipped, it should yield two completely different cipher images when applied to an identical plain image. Also, using the same key, even just one bit in plain image is flipped, it should produce completely different cipher images [6]. In our work, the combination logistic map and perceptron-model approach is used to encrypt pixel values. More importantly, linear feedback shift register, which improves the encryption statistic, is deployed into the cipher stream chaining process. Such approach allows for image-wide pixel-dependent encryption.

Chapter 3

Methodology

This chapter introduces about the background information of the method in use. The proposed process and its algorithm are described in detail.

3.1 Chaotic System

Nearly all nontrivial real-world systems are nonlinear dynamical systems. Chaos describes certain nonlinear dynamical systems that have a very sensitive dependence on initial conditions. Chaotic systems are always deterministic and may be very simple, yet they produce completely unpredictable and divergent behavior. Systems of nonlinear equations are difficult to solve analytically, and scientists have relied heavily on visual and qualitative approaches to discover and analyze the dynamics of non-linearity.

In this section, one of the famous chaotic map called Logistic map will be presented. This Logistic map will be critically analyzed by using the visualization method to understand the behaviour of this nonlinear dynamical systems.

3.1.1 Logistic Map

Logistic map is the one-dimensional chaotic system [36]. This model is based on the common s-curve logistic function that shows how a population territory grows slowly, then rapidly, before tapering off as it reaches its carrying capacity. The logistic map uses a nonlinear difference equation

to look at discrete time steps. It's called the logistic map because it maps the population value at any time step to its value at the next time step. The following equation is the Logistic map formula 3.1:

$$X_{i+1} = r \times X_i \times (1 - X_i) \tag{3.1}$$

This equation defines the rules, or dynamics, of our system: r represents the growth rate and X_i denotes the population at a given index i. In other words, the population level at any given time is a function of the growth rate parameter and the previous time step's population level. If the growth rate is set too low, the population will die out and go extinct. Higher growth rates might settle toward a stable value or fluctuate across a series of population booms and busts. The distribution graph of the growing population X_i with respect to r from 0 to 4 is illustrated in the bifurcation diagram in Fig 3.1.

Figure 3.1: Logistic Map behavior

As we can see in the Fig 3.1, the population X of 100 generations toward the 1,000 discrete values of growth parameter r is plotted. At r < 1.0, the system population are always almost zero. Between 1.0 and 3.0, the population starts to settle into the exact point for each generation. From 3.0, the population is bifurcated into two different path and bifurcated into four different paths after

the growth rate is set to 3.4. However, after r > 3.6, the system begins to oscillate into two then four, eight, sixteen and so on follow 2n formula. At r = 3.9, it has bifurcated so many times that the system populations jump randomly in between all the paths.

3.2 Proposed Algorithm

In the proposed algorithms, the behavior of the Logistic map is used. The employment of the map, in term of cryptography, can be used to generated the sequence of keys. To encrypt the pixel individually, the perceptron model introduced by [5], is used. This method is very suitable for image encryption due to the complex relationship between the input and the output of the model. In the end, the value of the encrypted pixel have higher randomness and unpredictable beacause the usage the key sequence generated from the logistic map. However, the encryption is done on each pixel separately, making the approach vulnerable to differential analysis attack. To overcome this problem, a new encryption/decryption algorithm called Cipher Stream Chaining Process (CSCP) is introduced.

3.2.1 Cipher Stream Chaining Process

Cipher Stream Chaining Process (CSCP) is a symmetrickey encryption and decryption method that perform XOR cipher, adding previous cipher pixel to the key that is used in the current pixel. In turn, the encryption result of each pixel depends on the previous pixel, creating a chain of encryptions.

To be more precise, after a pixel is encrypted, Linear Feedback Shift Register (LFSR) [4] is applied to the cipher pixel. Then it is XORed with the key used to encrypt the next pixel. This novel approach ensures that the pixels are chained to each other, making highly sensitive to given plain image. Figure 3.3 shows the encryption process. Decrypting an image is simply reversing the encryption process. LFSR is applied to the cipher image. Then the result is XORed with the key.(See in Figure 3.4)

Our method is a symmetric-key method such that, different pixels being encrypted and decrypted with the different keys. Corresponding plain and cipher pixels use the same key to encrypt and decrypt respectively. Detail of the encryption and decryption processes are described in the following sections.

3.2.2 Encryption Algorithms

Image encryption process is as follows:

1. Given an 8-bit grayscale image of size $M \times N$ pixels, the image can be represented as a one-dimensional vector $\boldsymbol{P} =< P_1, P_2, ..., P_i, ..., P_n >$, where P_i, $1 \leq i \leq n$, $n = M \times N$, denotes values of the i^{th} pixel of the image. The value of a pixel is the 8-bit binary number corresponding to intensity of that pixel.

2. Set X_0 to any value within the range of $[0, 1]$ and r to any value between [3.99,4] as the initial parameters of the logistic map.

3. Calculate the Eq. 3.1 with the assigned value of X_0 and r, $2 \times n$ times to produce a sequence of population $\boldsymbol{X} =< X_1, X_2, ..., X_{2n} >$.

4. Convert each value X_i, $1 \leq i \leq 2n$, to 8-bit binary representation using the following steps:

   - Transform the value of X_i into unsigned integer in the range of [0, 255] by multiplying with 255:

   $$X_i = X_i \times 255 \tag{3.2}$$

   - Use round function to the sequence elements for converting them into their nearest decimal value:

   $$X_i = Round(X_i) \tag{3.3}$$

   - Convert each rounded X_i into 8-bits binary representation. This 8-bit representation will be used as encryption keys.

   After repeating Step 4 for all elements in $\boldsymbol{X}$, the vector of the keys $\boldsymbol{K} =< K_1, K_2, ..., K_{2n} >$, where K_i is an 8-bit representation of rounded X_i is obtained.

5. To encrypt each pixel P_i in image $\boldsymbol{P} =< P_1, P_2, ..., P_i, ..., P_n >$, two keys in K, K_{2i-1}, K_{2i}, are required. Both keys are fed into the structure of perceptron to generate the values of weight and threshold for the neuron net. The algorithm for producing the perceptron model

is well explained in [5]. The overview process of encrypting the plain pixel into a cipher pixel is described in equation below.

$$C_i = NeuronNet(P_i, (K_{2i-1}, K_{2i})) \tag{3.4}$$

where C_i, P_i, $K_{2i-1}$and K_{2i} denote the i^{th} cipher pixel, the i^{th} plain pixel and encryption keys at index $2i-1$ and $2i$, $1 \leq i \leq n$, respectively. *NeuronNet()* is the function to encrypt the pixel using perceptron model. It was introduce by [5], and is described as follow:

Figure 3.2: NeuronNet()

In this method, 8 neurons are required to scramble one gray scale image pixel because each particular neuron is used to encrypt one bit. Inside each neuron, 4 parameters are required which are $W_{1,k}$, $W_{2,j}$, Z_j, and θ_j where $W_{1,j}$, $W_{2,j}$ are the weights of the neuron, Z_j is additional input, θ_j is the threshold value and $1 \leq j \leq 8$. To retrieve all these values,the keys K_{2i-1}, K_{2i} obtained from the logistic map are used. Supposed that K_1 and K_2 are the keys used for encrypting one gray scale image pixel. Generally, their values are 8-bits representation. $K_{1,j}$ and $K_{2,j}$ denote the j^{th} bit of K_1 and K_2, respectively, $1 \leq j \leq 8$. The following transformation are used to obtained the value of parameters $W_{1,k}$, $W_{2,j}$, Z_j, and θ_j:

$$W_{1,j} = \begin{cases} 1 & \text{if } K_{1,j} = 1 \\ -1 & \text{if } K_{1,j} = 0 \end{cases} \tag{3.5}$$

$$W_{2,j} = \begin{cases} 1 & \text{if } K_{2,j} = 1 \\ -1 & \text{if } K_{2,j} = 0 \end{cases} \tag{3.6}$$

$$Z_j = \begin{cases} 1 & \text{if } K_{1,j} = 1 \\ 0 & \text{if } K_{1,j} = 0 \end{cases} \tag{3.7}$$

$$\theta_i = K_{1,j} \oplus K_{2,j}, where 1 \leq j \leq 8 \tag{3.8}$$

After retrieving all the required parameter value from the key, using stream cipher strategy to encrypt the image. Taking one pixel P from image. b_j denotes the j^{th} bit of pixel P. After encryption, the cipher pixel value is C, and b'_j denote the j^{th} bit of pixel C, $1 \leq j \leq 8$.

$$b'_j = \begin{cases} f(W_{1,j} \times b_j + W_{2,j} \times Z_j - \theta_j) & \text{if } K_{1,j} = 1 \\ f(W_{1,j} \times b_j - W_{2,j} \times Z_j + \theta_j) & \text{if } K_{1,j} = 0 \end{cases} \tag{3.9}$$

$$where, f(x) = \begin{cases} 1 & \text{if } x \geq 1 \\ 0 & \text{if } x < 0 \end{cases} \tag{3.10}$$

6. To make our method more robust to differential analysis attack, pixel-chaining process is employed. For the first plain pixel, we encrypt it using perceptron model directly. The cipher pixel is then applied by LFSR process. Next, it is XORed with the corresponding key. The process is repeated until the last pixel is encrypted. Chaining the pixel create better chaos to the cipher image, and thus more prone to differential analysis attack. The encryption algorithm is described below.

Algorithm 1 Encryption

for (i from 1 to n) **do**

if ($i == 1$) **then**

C_i = *NeuronNet*$(P_i, (K_{2i-1}, K_{2i}))$

else

$C'_{i-1} =$ *LSFR*(C_{i-1})

$K'_{2i-1} = K_{2i-1} \oplus C'_{i-1}$

$K'_{2i} = K_{2i} \oplus C'_{i-1}$

$C_i =$ *NeuronNet* $(P_i, (K'_{2i-1}, K'_{2i}))$

end if

end for

7. After finishing the Step 6, the vector of cipher pixels $\boldsymbol{C} =< C_1, C_2, ..., C_n >$ is generated. Then, the vector is converted back into 8-bits grayscale cipher image. The encryption process is illustrated in Fig 3.3.

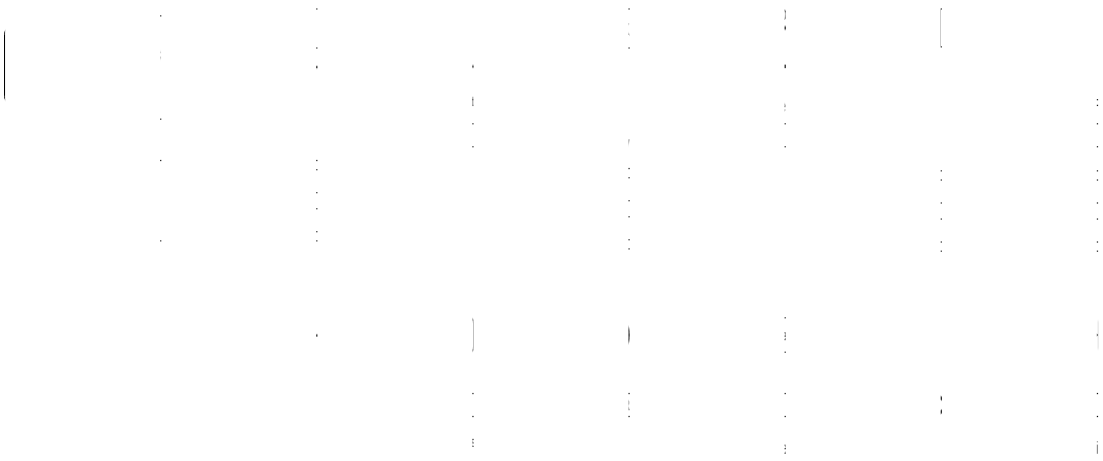


Figure 3.3: Flow of Encryption

3.2.3 Decryption Algorithms

In the decryption process, the cipher image is received. The procedure of the proposed image decryption process is described as follow:

1. An 8-bit grayscale of the cipher image of size $M \times N$ is obtained. It is then converted into vector of ciper pixels $\boldsymbol{C} =< C_1, C_2, ..., C_n >$, where $n = M \times N$ and the value of a pixel is the 8-bit binary number corresponding to intensity of that pixel.

2. As the proposed method is symetric-key algorithm, the same key is used for both encryption and decryption process. Thus, the values of X_0 and r are chosen the same as Step 2 of the encryption process.

3. The value of X_0 and r obtained from Step 2 are used to generated the sequence of population $\boldsymbol{X} =< X_1, X_2, ..., X_{2n} >$ using Eq. 3.1. Since the initial values of this logistic map is deterministic. The sequence of vector $\boldsymbol{X}$ will be exactly the same as we obtain from the encryption step.

4. Convert each value of $X_i, 1 \leq i \leq 2n$, to 8-bit binary representation as described in Step 4 of the encryption process.

5. The perceptron model which is used for decrypting the pixel is the same as the encryption [5]. Thus, the agorithm of decrypting the a cipher pixel into a plain pixel can be expressed as in Eq (3.4)

6. To decrypt the image, the reverse of CSCP is employed. (See in algorithm below)

Algorithm 2 Decryption

for (i from 1 to n) **do**
  if $(i == 1)$ **then**
    P_i = *NeuronNet*$(C_i, (K_{2i-1}, K_{2i}))$
  else
    C'_{i-1} = LSFR(C_{i-1})
    $K'_{2i-1} = K_{2i-1} \oplus C'_{i-1}$
    $K'_{2i} = K_{2i} \oplus C'_{i-1}$
    $P_i =$ *NeuronNet*$(C_i, (K'_{2i-1}, K'_{2i}))$
  end if
end for

7. After finishing the Step 6, the process of decryption as shown in Figure 3.4 was taken until the last pixel of the image is reached. Then, the vector of plain pixels $\boldsymbol{P} =< P_1, P_2, ..., P_n >$ is generated from the decryption process. Finally, it is converted back into 8-bits grayscale plain image.

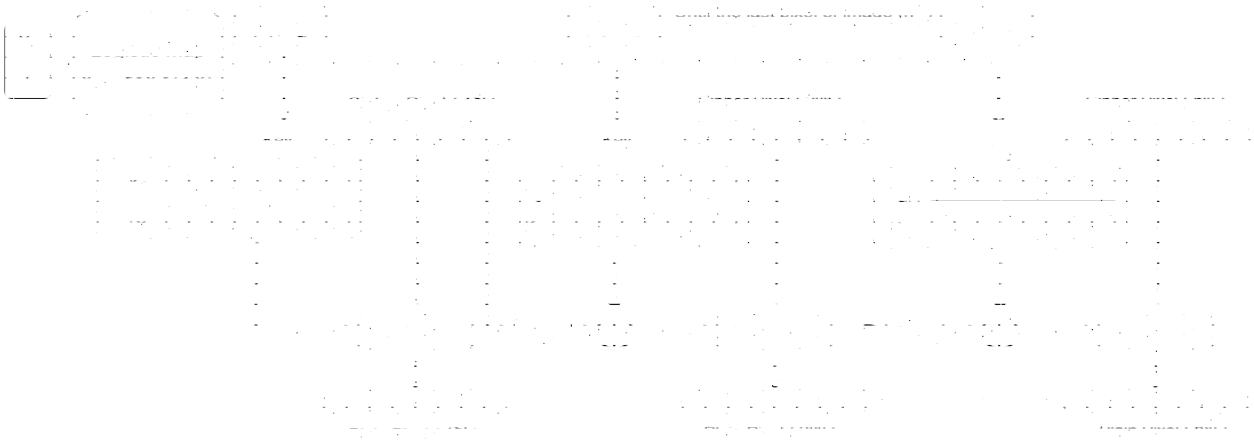


Figure 3.4: Flow of Decryption

Chapter 4

Experimentation and Results

In cryptography, security confirmation is the main issue for encryption algorithms. It is used to ensure that an encryption method is strong enough against any attack from the third party. Good encryption algorithm must be resistant to various attacks such as brute force, plain text, statistic analysis attack. The experimental set up and the usage of the security confirmation will be discussed in the below sections:

4.1 Experimental Setup

In this section, there are two set up types which are the data used for the experiment and the software used for the experiment.The experiment was done using MATLAB to explore the efficiency of the proposed image encryption method. Our proposed method is used for the image-based encryption. Various type of images such as gray scale images, color images is used.

4.2 Security Confirmation

Security confirmation is used in response to the cryptanalysis to evaluate the protection level of the cryptography algorithms. To confirm the strength of the proposed method, there are different ways to test with respect to different attack. Firstly, brute force attack is an automated software used to generate a large number of consecutive data to find the desired value (key value). Exhaustive key Search and Key sensitivity are used to analyse the brute force attack. Secondly, the cryptanalysis

based on the probability distribution has recently attracted a lots of attention in the analysis of the image encryption. Thus, the Histogram Analysis and the Information Entropy Analysis are used. Thirdly, differential attack is the branch of study on cryptography that compares the way differences or the correlation of the two cipher image if change in the plaint image. To evaluate this kind of attack, Number of Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI) are used. Lastly, Peak Signal-to-Noise Ratio, in term of cryptography, is used to confirm how different between the original image and the encrypted image. Each of the security analysis mention above will be described in detail in the following section.

4.2.1 Exhaustive Key Search

One aspect of the strength of encryption algorithm is the size of the key space or the amount of all possible key values. It is used to ensure the security of the algorithms toward the brute force attack. Normally, the information which are send through the network can be easily captured. It is somehow exhausted with all the possible keys to retrieve the original message back by the third party. Therefore, the larger the key space, the lower the chance to find the correct key. Thus, the encryption algorithm must be designed with key space as big as possible. In logistic map, number of possible values of both X_0 and r are 10^{16} [37]. The key space of the algorithm is, therefore, $10^{16} \times 10^{16} = 10^{32}$. In Table 4.1 show the key space of the proposed algorithms comparing with the conventional method.

Table 4.1: key space of the proposed system comparing with the conventional method

Algorithms	**Key space**
DES	7.4×10^{16}
Logistic Map	10^{32}
Triple DES	3.7×10^{50}
AES	6.2×10^{57}

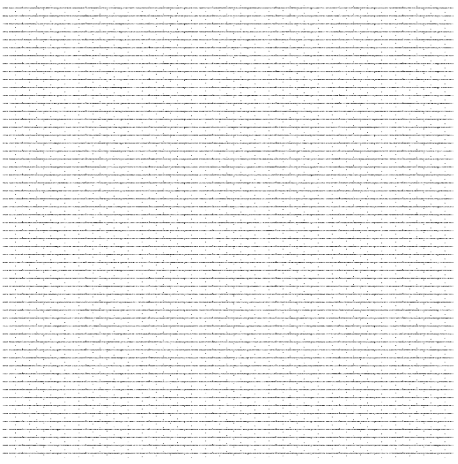
4.2.2 Key Sensitivity Analysis

Sensitivity of the key is an important feature in cryptography algorithms. It shows how sensitive of the key toward the output of the encryption method. Sensitive is mean that when a change is made to the key, the output of the encryption must be different. Therefore, A perfect one should produce two completely cipher images even a single bit change of the key. The experiment of the key sensitivity is described as follow:

In the experiment, the value of initial parameters were chosen with $X_0 = 0.1$ and $r = 3.99$. In this case, the experiment will be conducted in two ways. First, the value of the X_0 will be changed as the value of parameter r will remain the same. Second, the value of the parameter r will be changed by keeping the value of X_0 the same. These two processes was to ensure that the keys (X_1 and r) of the system are very sensitive to the algorithms. The original information can not be retrieved back when the value of X_1 or r is different.

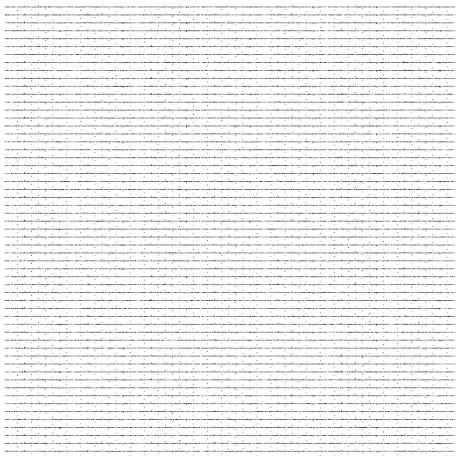
As shown in the figure 4.2, decrypted image with the wrong key can not be reversed back to the original image. The value of $X_0 = 0.1000000000000001$ and $r = 3.99$ are chosen for the Figure 4.2a, and the $X_0 = 0.1$ and $r = 3.9900000000000001$ are chosen for the Figure 4.2b. Similarly, the original Baboon image can not be retrieved when using different value of keys, as show in Figure 4.4.

(a) Original Lena
Size: 512*512

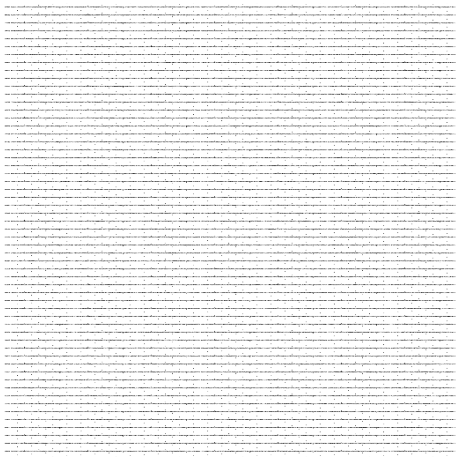


(b) Encrypted Lena
($X_0 = 0.1, r = 3.99$)

Figure 4.1: Gray Scale Lena and encrypted image of Lena

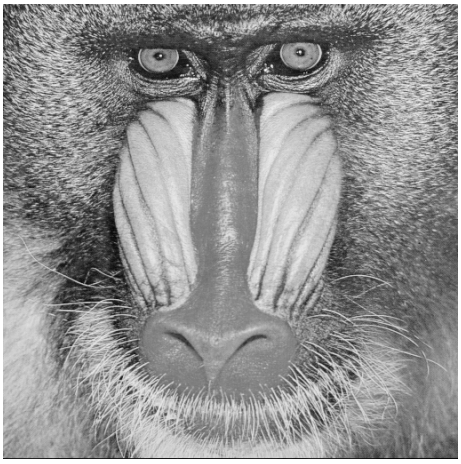


(a) Decrypted image with wrong parameter X_0 ($X_0 = 0.1000000000000001, r = 3.99$)

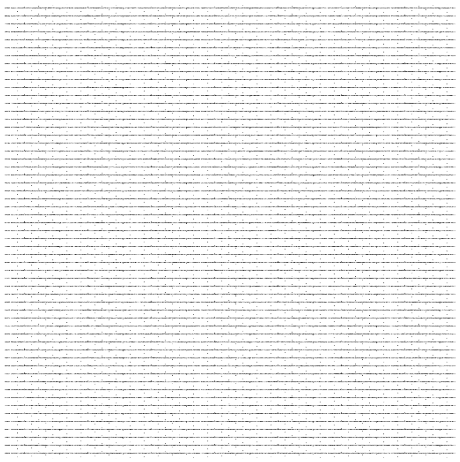


(b) Decrypted image with wrong parameter r ($X_0 = 0.1, r = 3.990000000000001$)

Figure 4.2: Decrypted images of Lena with wrong key

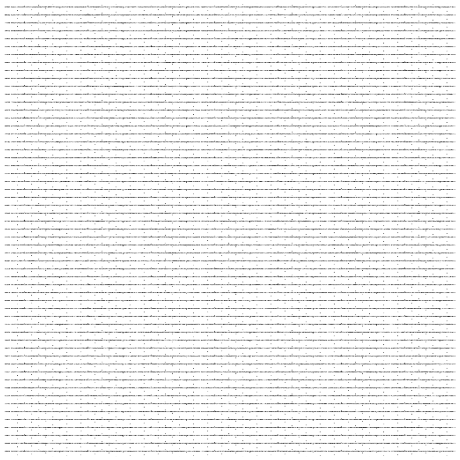


(a) Original Baboon
Size: 512*512

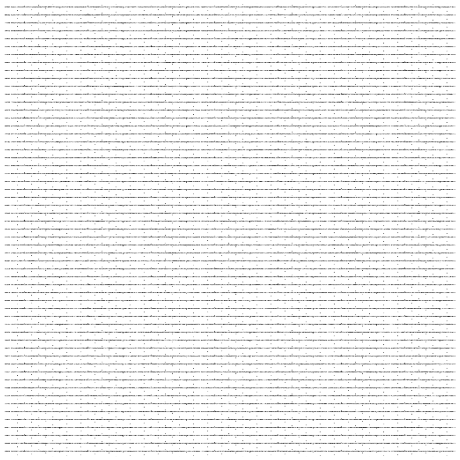


(b) Encrypted Baboon
($X_0 = 0.1, r = 3.99$)

Figure 4.3: Gray Scale Baboon and encrypted image of Baboon



(a) Decrypted image with wrong key
($X_0 = 0.1000000000000001, r = 3.99$)

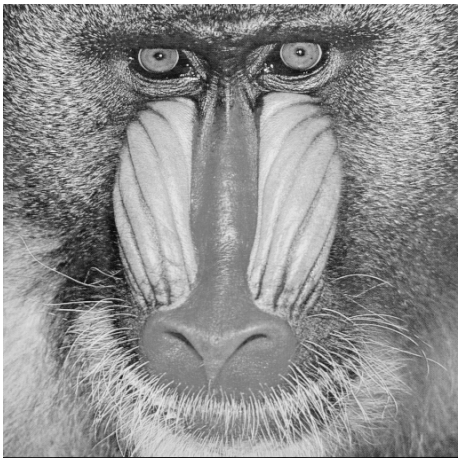


(b) Decrypted image with wrong key
($X_0 = 0.1, r = 3.990000000000001$)

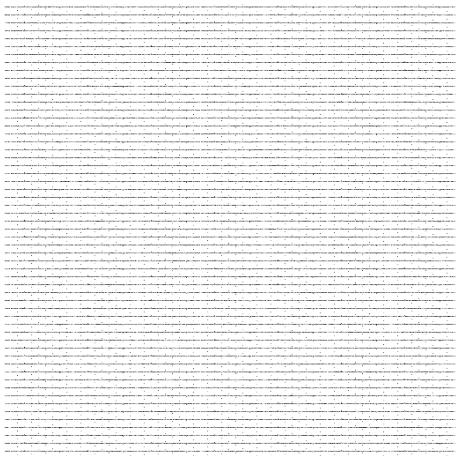
Figure 4.4: Decrypted images of Baboon with wrong key

4.2.3 Histogram Analysis

Histogram is generally used to describe frequency distribution of image intensity values. Good image encryption algorithm should produce the cipher image whose intensities cannot be used to predict the original image. This make it more complicated to obtain or guess the original image from the cipher image. Thus, an ideal cipher image should have the uniform or flat distribution which represent higher randomness of the pixel values. It is shown that the histogram of the encrypted image in Figure 4.5d is flat and does not resemble the histogram of the original image shown in Figure 4.5c.



(a) Original Baboon



(b) Encrypted Baboon
($X_0 = 0.1, r = 3.99$)

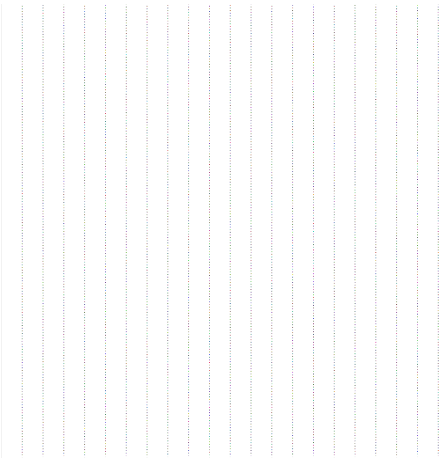
(c) Histogram of Original Baboon

(d) Histogram of Encrypted Baboon

Figure 4.5: Gray Scale and Color image of Baboon

For color images, the appearance of the cipher images is scramble similar to the grey scale image. Moreover, each pixels is consist of three combination values which are Red, Green and Blue channels. In Figure 4.6, show the encrypted image of the RGB version of Baboon. The histogram of the original and cipher images are shown in Figure 4.7 and Figure 4.8.

(a) Original Baboon (RGB)



(b) Encrypted Baboon (RGB)

Figure 4.6: Color image of Baboon

Figure 4.7: Histogram of Baboon (RGB)

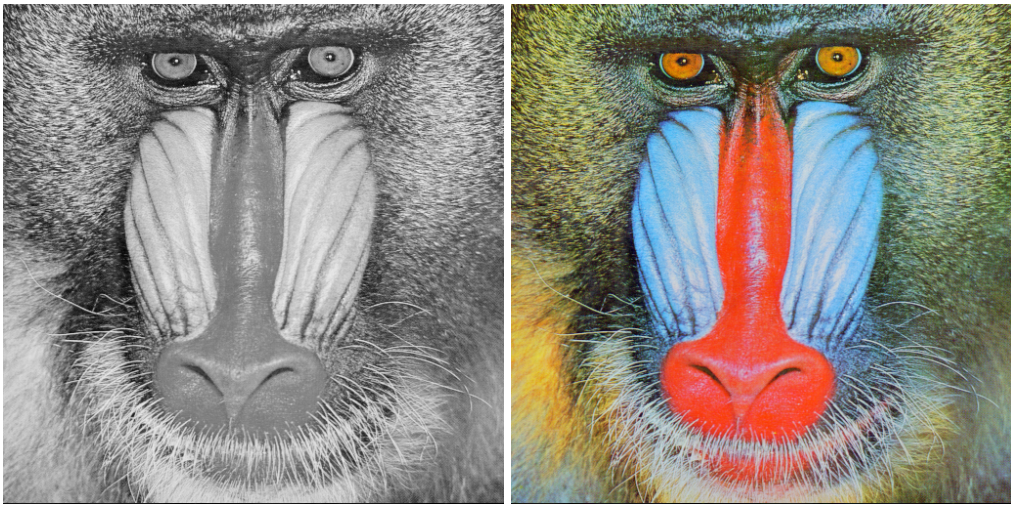
Figure 4.8: Histogram of Encrypted Baboon (RGB)

4.2.4 Information Entropy Analysis

Information Entropy, introduce by shanon in 1993 [38], is the important concept to study about the characteristic of the given information. It is used to measure the randomness of the signal source. Below is the equation to calculate the entropy of the information.

$$\mathbf{H}(\mathbf{m}) = \sum_{i=0}^{L-1} p(m_i) \log_2 \frac{1}{p(m_i)} \tag{4.1}$$

where L is the total number of the pixel intensity (normally $L = 256$ for the 8-bit grayscale image), m_i denotes each of the pixel intensity values and $p(m_i)$ is the probability of m_i. According to the equation, the optimal value of the entropy is 8, which means that each pixel intensity has the same probability .Table 4.2 shows the result of the image entropy of the proposed scheme. As shown in the table, entropies of cipher images of using the proposed algorithm are almost 8.



(a) Gray Scale Baboon
Size: 512*512

(b) color Baboon
size: 512*512

Figure 4.10: Gray Scale and Color image of Baboon

(a) Gray Scale Lena
Size: 512*512

(b) color Lena
size: 512*512

Figure 4.9: Gray Scale and Color image of Lena

Table 4.2: Entropy of the Encrypted Image

Image	Logistic Map with CSCP	[4]	[5]
Gray Scale Lena	7.9992	7.9993	7.6514
Gray Scale Baboon	7.9991	7.9993	7.6880
Color Lena	7.9992	7.9992	6.6130
Color Baboon	7.9993	7.9992	7.7960

4.2.5 Plain Text sensitivity Analysis

Strong cryptography algorithms should be sensitive to the plaintext attack or differential analysis attack where the algorithms produce two different cipher images from two plain images with a small difference. Let C_1 and C_2 be the cipher images which are corresponding to the original image P_1 and P_2 with only one-pixel difference, respectively. Number of Pixels Change Rate (NPCR) can be used to calculate the percentage of different pixel between C_1 and C_2 and the Unified Average Changing Intensity (UACI) can be used to measure the average differences of pixel intensity between C_1 and C_2[39]. NPCR and UACI are defined as follows:

$$\textbf{NPCR} = \frac{1}{n \times m} \sum_{i=1}^{M} \sum_{i=1}^{N} D\left(i, j\right) \times 100 \tag{4.2}$$

$$\textbf{UACI} = \frac{1}{n \times m} \sum_{i=1}^{M} \sum_{i=1}^{N} \frac{\left|C_1\left(i, j\right) - C_2\left(i, j\right)\right|}{255} \times 100 \tag{4.3}$$

where M and N are the width and height of the image, respectively, $C_1\left(i, j\right)$ and $C_2\left(i, j\right)$ are the intensity values of the two cipher images at position (i, j) and $D\left(i, j\right)$ is defined in Eq. 4.4

$$\mathbf{D}\left(\mathbf{i}, \mathbf{j}\right) = \begin{cases} 1 & \text{if } C_1\left(i, j\right) = C_2\left(i, j\right) \\ 0 & \text{if } C_1\left(i, j\right) \neq C_2\left(i, j\right) \end{cases} \tag{4.4}$$

The results of NPCR and UCAI evaluations based on the grey scale images and the color images are shown in table 4.4

Table 4.3: Number of Pixels Change Rate (NPCR)

Image	Logistic Map with CSCP	[4]	[5]
Gray Scale Lena	100	0.00038	0.00038
Gray Scale Baboon	100	0.00038	0.00038
Color Lena	100	0.00038	0.00038
Color Baboon	100	0.00038	0.00038

Table 4.4: Unified Average Changing Intensity (UACI)

Image	Logistic Map with CSCP	[4]	[5]
Gray Scale Lena	33.56779	0.000034	0.000032
Gray Scale Baboon	33.60931	0.000065	0.000014
Color Lena	33.59605	0.000143	0.000027
Color Baboon	33.59417	0.000033	0.000033

4.2.6 Peak Signal to Noise Ratio Analysis

To measure the ratio of mean square difference between the original image the encrypted image, Peak Signal-toNoise Ratio (PSNR) [40] is used. In this case, the original image and the cipher image are considered as the signal and noise, respectively. The formula is defined as below:

$$\textbf{PSNR} = 10 \times log_{10} \frac{255^2}{MSE} \tag{4.5}$$

where MSE is the mean square error between two images and computed as follow.

$$\textbf{MSE} = \frac{1}{n \times m} \sum_{i=1}^{M} \sum_{i=1}^{N} (P_1(i,j) - C_1(i,j))^2 \tag{4.6}$$

where M is the width of the image, N is the height of the image and $P_1(i,j)$ and $C_1(i,j)$are the pixel intensity of the plain image and cipher image at location (i,j) respectively. As the difference between two image pixel value in the same position is higher, the value of PSNR has become lower

and approach to zero for the maximum of different pixel value between two grayscale images.

Table 4.5: Peak Signal to Noise Ratio (PSNR)

Image	Logistic Map with CSCP	[4]	[5]
Gray Scale Lena	9.238843	9.221829	11.164834
Gray Scale Baboon	9.149312	9.173178	10.973994
Color Lena	8.637750	8.625500	9.895166
Color Baboon	8.787422	8.792451	10.041792

4.3 Discussion

As the result, the proposed algorithm with CSCP can produce the cipher image which is not visible to the human vision. Moreover, the algorithm is very sensitive to the key input. Even a slightly change of the key value to the decryption algorithm, the original information can not be retrieved back. In term of the image pixel values, the encrypted image is very different from the original image measured by PSNR. More importantly, with the feature of CSCP, the encrypted image pixel values are strongly depend on the previous pixels. This make the algorithm sensitive to the plain image input. The result from NPCR and UACI is better comparing to the method proposed in [4] and [5]. Therefore, the proposed algorithm is strongly resistant against differential analysis attack.

Chapter 5

Conclusion

5.1 Conclusion

In this thesis, the chaotic map called logistic map is used for generating the key sequence. The sequence of key is used for encrypting the image pixel bit by bit as the stream encryption. The Cipher Stream Chaining Process (CSCP) is deployed to improve the encryption algorithm. This process perform XOR operation on the encrypted pixel with the key that is used in the next pixel. In turn, each pixel depend on the previous pixel, creating a chain of encryption. Thus, the algorithm highly sensitive to the plain image. Some of the security confirmation method are used to evaluate the proposed process and algorithm. The experimental results show that the algorithm is able to produce a truly unintelligible cipher image. The encrypted image is completely different from the original, both in terms of human vision and statistics. Moreover, even just a small change to the key (X_0 or r), the original image can not be retrieved back. This show that the key generator provide high security to the algorithm. Lastly, the algorithm is very sensitive to the plain image. By changing the values of the image pixel, the algorithm is able to produce different cipher image.

5.2 Future Work

Even though the proposed algorithms is able to perform better toward most of the main security confirmation. there are still some more work need to be conducted. In this work, the input data like grey scale images and the color images in used for the experiment. In the future work, we

will introduced this work with other multimedia data such as text and video. A weak point of the proposed algorithm is the key space. Currently, the Logistic map is used for generating the key sequence for the algorithm. Since there is limit of key space to the logistic map. Expanding the key space will be considered as well for the next work.

References

[1] A. K. Mandal, C. Parakash, and A. Tiwari, "Performance evaluation of cryptographic algorithms: Des and aes," in *2012 IEEE Students' Conference on Electrical, Electronics and Computer Science*, March 2012, pp. 1–5.

[2] S. Lian, *Multimedia content encryption: techniques and applications*. Auerbach Publications, 2008.

[3] X. Li, "Image encryption scheme based on multiple chaotic maps," in *2013 Fourth International Conference on Emerging Intelligent Data and Web Technologies*, Sep. 2013, pp. 261–266.

[4] S. Rohith, K. N. H. Bhat, and A. N. Sharma, "Image encryption and decryption using chaotic key sequence generated by sequence of logistic map and sequence of states of linear feedback shift register," in *2014 International Conference on Advances in Electronics Computers and Communications*, Oct 2014, pp. 1–6.

[5] X.-Y. Wang, L. Yang, R. Liu, and A. Kadir, "A chaotic image encryption algorithm based on perceptron model," *Nonlinear Dynamics*, vol. 62, no. 3, pp. 615–621, Nov 2010. [Online]. Available: https://doi.org/10.1007/s11071-010-9749-8

[6] G. ALVAREZ and S. LI, "Some basic cryptographic requirements for chaos-based cryptosystems," *International Journal of Bifurcation and Chaos*, vol. 16, no. 08, pp. 2129–2151, 2006. [Online]. Available: https://doi.org/10.1142/S0218127406015970

[7] A. Epishkina, K. Kogos, and N. Nikiforova, "A course of mathematical logic and theory of algorithms as a mathematical background of modern cryptology," in *2016 Third International*

Conference on Digital Information Processing, Data Mining, and Wireless Communications (DIPDMWC), July 2016, pp. 200–204.

[8] D. E. Robling Denning, *Cryptography and Data Security*. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 1982.

[9] R. C. . Phan and M. U. Siddiqi, "A framework for describing block cipher cryptanalysis," *IEEE Transactions on Computers*, vol. 55, no. 11, pp. 1402–1409, Nov 2006.

[10] S. Manna, M. Prajapati, A. Sett, K. Banerjee, and S. Dutta, "Design and implementation of a two-layered hybrid cryptosystem," in *2017 Third International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN)*, Nov 2017, pp. 327–331.

[11] M. Islam, M. Shah, Z. Khan, T. Mahmood, and M. J. Khan, "A new symmetric key encryption algorithm using images as secret keys," in *2015 13th International Conference on Frontiers of Information Technology (FIT)*, Dec 2015, pp. 1–5.

[12] Z. Guosheng and W. Jian, "Security analysis and enhanced design of a dynamic block cipher," *China Communications*, vol. 13, no. 1, pp. 150–160, Jan 2016.

[13] I. Gorbenko, A. Kuznetsov, V. Tymchenko, Y. Gorbenko, and O. Kachko, "Experimental studies of the modern symmetric stream ciphers," in *2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S T)*, Oct 2018, pp. 125–128.

[14] Z. Yingbing and L. Yongzhen, "The design and implementation of a symmetric encryption algorithm based on des," in *2014 IEEE 5th International Conference on Software Engineering and Service Science*, June 2014, pp. 517–520.

[15] I. R. S. Reddy and G. Murali, "A novel triple des to enhance e-governance security," in *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, Aug 2017, pp. 2443–2446.

[16] Y. Yuan, Y. Yang, L. Wu, and X. Zhang, "A high performance encryption system based on aes algorithm with novel hardware implementation," in *2018 IEEE International Conference on Electron Devices and Solid State Circuits (EDSSC)*, June 2018, pp. 1–2.

[17] R. U. Ginting and R. Y. Dillak, "Digital color image encryption using rc4 stream cipher and chaotic logistic map," in *2013 International Conference on Information Technology and Electrical Engineering (ICITEE)*, Oct 2013, pp. 101–105.

[18] O. Elkeelany and S. Nimmagadda, "Performance evaluation of different hardware models of rc5 algorithm," in *2007 Thirty-Ninth Southeastern Symposium on System Theory*, March 2007, pp. 124–127.

[19] H. K. Verma and R. K. Singh, "Enhancement of rc6 block cipher algorithm and comparison with rc5 rc6," in *2013 3rd IEEE International Advance Computing Conference (IACC)*, Feb 2013, pp. 556–561.

[20] S. Halevi and H. Krawczyk, "Public-key cryptography and password protocols," *ACM Trans. Inf. Syst. Secur.*, vol. 2, no. 3, pp. 230–268, Aug. 1999. [Online]. Available: http://doi.acm.org/10.1145/322510.322514

[21] W. Küchlin, "Public key encryption," *ACM SIGSAM Bulletin*, vol. 21, pp. 69–73, 1987.

[22] S. Shukla and G. Sadashivappa, "Secure multi-party computation protocol using asymmetric encryption," in *2014 International Conference on Computing for Sustainable Global Development (INDIACom)*, March 2014, pp. 780–785.

[23] Y. Wu and X. Wu, "Implementation of efficient method of rsa key-pair generation algorithm," in *2017 IEEE International Symposium on Consumer Electronics (ISCE)*, Nov 2017, pp. 72–73.

[24] F. J. Aufa, Endroyono, and A. Affandi, "Security system analysis in combination method: Rsa encryption and digital signature algorithm," in *2018 4th International Conference on Science and Technology (ICST)*, Aug 2018, pp. 1–5.

[25] D. P. Shah and P. G. Shah, "Revisting of elliptical curve cryptography for securing internet of things (iot)," in *2018 Advances in Science and Engineering Technology International Conferences (ASET)*, Feb 2018, pp. 1–3.

[26] S. Chandra, S. Paira, S. S. Alam, and G. Sanyal, "A comparative survey of symmetric and asymmetric key cryptography," in *2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE)*, Nov 2014, pp. 83–93.

[27] G. Hanchinamani and L. Kulkarni, "An efficient image encryption scheme based on a peter de jong chaotic map and a rc4 stream cipher," *3D Research*, vol. 6, no. 3, p. 30, Jul 2015. [Online]. Available: https://doi.org/10.1007/s13319-015-0062-7

[28] T. Wontchui, J. Y Effa, H. Ekobena, and J. S A E Fouda, "Dynamical behavior of peter-de-jong map using the modified 0-1 and 3st tests for chaos," *Ann. Rev. Chaos Theor. Bif. Dyn. Syst.*, vol. 7, p. 1, 01 2017.

[29] K. K.-H. Wong, G. Carter, and E. Dawson, "An analysis of the rc4 family of stream ciphers against algebraic attacks," in *Australasian Information Security Conference AISC 2010*, C. Boyd and W. Susilo, Eds. Brisbane, Australia: Australian Computer Society, 2010, pp. 67–74, an open access copy of this article can also be accessed from the publisher's webpage - see Official URL above. [Online]. Available: https://eprints.qut.edu.au/34330/

[30] M. Long and L. Tan, "A chaos-based data encryption algorithm for image/video," in *2010 Second International Conference on Multimedia and Information Technology*, vol. 1, April 2010, pp. 172–175.

[31] K. Vasuyta and I. Zakharchenko, "Modified discrete chaotic map based on chebyshev polynomial," in *2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S T)*, Oct 2016, pp. 217–219.

[32] S. Mazloom and A. M. Eftekhari-Moghadam, "Color image encryption based on coupled nonlinear chaotic map," *Chaos, Solitons Fractals*, vol. 42, no. 3, pp. 1745 – 1754, 2009. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0960077909002045

[33] H. W. Safi and A. Y. Maghari, "Image encryption using double chaotic logistic map," in *2017 International Conference on Promising Electronic Technologies (ICPET)*. IEEE, 2017, pp. 66–70.

[34] N. K. El Abbadi, E. Yahya, and A. Aladilee, "Digital rgb image encryption based on 2d cat map and shadow numbers," in *2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT)*. IEEE, 2017, pp. 162–167.

[35] C. Fu, J.-j. Chen, H. Zou, W.-h. Meng, Y.-f. Zhan, and Y.-w. Yu, "A chaos-based digital image encryption scheme with an improved diffusion strategy," *Optics express*, vol. 20, no. 3, pp. 2363–2378, 2012.

[36] Z. Yan-Bin and D. Qun, "A new digital chaotic sequence generator based on logistic map," in *2011 Second International Conference on Innovations in Bio-inspired Computing and Applications*, Dec 2011, pp. 175–178.

[37] X. Wang and C. Jin, "Image encryption using game of life permutation and pwlcm chaotic system," *Optics Communications*, vol. 285, no. 4, pp. 412 – 417, 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0030401811010893

[38] C. E. Shannon, "Communication theory of secrecy systems," *Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[39] Y. Wu, J. P. Noonan, S. Agaian *et al.*, "Npcr and uaci randomness tests for image encryption," *Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT)*, vol. 1, no. 2, pp. 31–38, 2011.

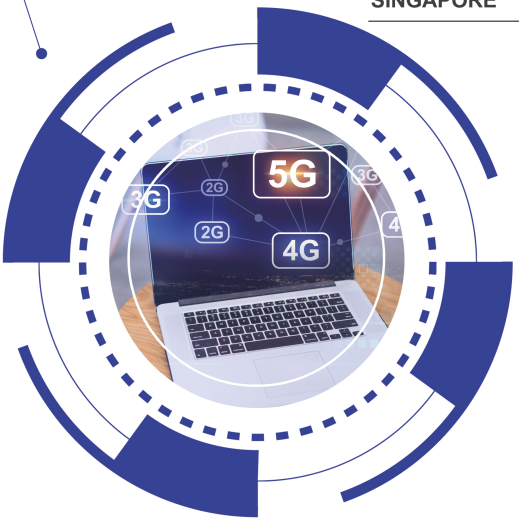
[40] N. Taneja, B. Raman, and I. Gupta, "Combinational domain encryption for still visual data," *Multimedia Tools and Applications*, vol. 59, no. 3, pp. 775–793, Aug 2012. [Online]. Available: https://doi.org/10.1007/s11042-011-0775-4

ISBN: 978-1-7281-1321-0
IEEE Catalog Number: CFP19D48-USB

Proceedings of 2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS 2019)

ISBN: 978-1-7281-1321-0
IEEE Catalog Number: CFP19D48-USB

February 23-25, 2019
SINGAPORE



ICCCS 2019

Proceedings of 2019 IEEE 4th International Conference on Computer and Communication Systems

IEEE

êèéñ & ìÈ– &«È^¾«sÈ˜±«s¤ ±«‘^¾^«•^ ±«
±ª»ÍÈ^¾ s«„ ±ªªÍ«˜•sÈ˜±« PÝÂÈ^ªÂ

P˜«’s»±¾^ Ø ^~¾Ís¾Ýêë êí÷ êèéñ
PÍ~ª˜ÂÂ˜±« ^s„¤˜«^ö 'HFHPEHU

ÜuFheY[[Z_d]i

$FFHSWHG SDSHUV ZLOO EH SXEOLVKHG LQ WKH FRQIHUHQFH
SURFHHGLQJV ZKLFK ZLOO EH VXEPLWWHG IRU LQFOXVLRQ LQWR
,(((;SORUH VXEPLWWHG IR &RQIHUHQFH LQ
DQG FRSXV

Ü Jef_Yi

- $OJRULWKPV
- %LJ 'DWD
- &RPSXWHU $UFKLWHFWXUH
- 'DWD &RPSUHVVLRQ
- ,PDJH 3URFHVVLQJ
- 0RELOH &RPSXWLQJ
- +LJK 3HUIRUPDQFH &RPSXWLQJ
- $XWRQRPLF DQG 7UXVWHG &RPSXWLQJ
- 3DUDOOHO DQG 'LVWULEXWLQJ &RPSXWLQJ
- %LRPHGLFDO ,QIRUPDWLFV DQG &RPSXWDWLRQ
- 6RIWZDUH (QJLQHHULQJ DQG .QRZOHGJH (QJLQHHULQJ
- :LUHOHVV &RPPXQLFDWLRQV
- 1HWZRUN &RPPXQLFDWLRQ
- &RPPXQLFDWLRQV 7UDQVPLVVLRQ
- 1HWZRUN 6HFXULW\ DQG &U\SWRJUDSK\
- :LUHOHVV DQG 6HQVRU 'HYLFHV
- 5HPRWH 6HQVLQJ DQG *36
- 5) DQG 0LFURZDYH &RPPXQLFDWLRQ
- ,QIRUPDWLRQ DQG ,WV 7HFKQLFDO (GXFDWLRQ
- 6SHHFK DQG $XGLR 3URFHVVLQJ
- 6LJQDO ,PDJH DQG 9LGHR 3URFHVVLQJ
- 6LJQDO 'HWHFWLRQ DQG 3DUDPHWHU
- $UWLILFLDO ,QWHOOLJHQFH DQG 0DFKLQH /HDUQLQJ
- 5) 0LFURZDYH DQG PLOOLPHWHU FLUFXLW
- 7HFKQLTXHV RI /DVHU
- $QWHQQD DQG 3URSDJDWLRQ
- 5) DQG 0LFURZDYH GHYLFHV
- (OHFWURPDJQHWLF DQG 3KRWRQLFV
- 0LFURZDYH 7KHRU\ DQG 7HFKQLTXHV
- 9LUWXDO 5HDOLW\ DQG 9LVXDOL]DWLRQ
- 0RGXODWLRQ &RGLQJ DQG &KDQQHO $QDO\VLV
- ,QWHJUDWHG 2SWLFV DQG (OHFWUR RSWLFV 'HYLFHV

ÜuA[odej[If[Wa[hi

¼3URI 3HUU\ 6KXP
26$)HOORZ 63,( )HOORZ
1DQ\DQJ 7HFKQRORJLFDO 8QLYHUVLW\
¼3URI *XX &KDQJ <DQJ ,((( )HOORZ
1DWLRQDO &KXQJ +VLQJ 8QLYHUVLW\
¼3URI <DQJ ;LDR ,(7)HOORZ
7KH 8QLYHUVLW\ RI $ODEDPD 86$

Üu>_ijeh

¼&&&6
.DQ\DNXPDUL ,QGLD _ 1RYHPEHU
3XEOLVKHU ,(((3UHVV ,6%1
3DSHUV RI ,&&&6 KDYH EHHQ LQGH[H
6FRSXV
¼&&&6
UDFRZ 3RODQG _ -XO\
3XEOLVKHU ,(((3UHVV ,6%1
3DSHUV RI ,&&&6 KDYH EHHQ LQGH[H
6FRSXV
¼&&&6
1DJR\D ,QVWLWXWH RI 7HFKQRORJ\ 1DJ
3XEOLVKHU ,(((3UHVV ,6%1
7KH FRQIHUHQFH SURFHHGLQJV RI ,&&&6
;SORUH

Üu9ecc_jj[[

&RQIHUHQFH &KDLUV
3URI <DQJ ;LDR 7KH 8QLYHUVLW\ RI $O
3URI *XX &KDQJ <DQJ 1DWLRQDO &KXQJ
3URJUDP &KDLUV
3URI %R <DQJ 8QLYHUVLW\ RI (OHFWUR
&KLQD &KLQD
3URI 1REXR)XQDELNL 2ND\DPD 8QLYHU
3XEOLFLW\ &KDLU
$VVRF 3URI .U]\V]WRI .RV]HOD 3R]QDQ
3RODQG

ÜuIkXc_ii_e

/RJ LQ WKH (OHFWURQLF 6XEPLW \RXU
$Q\ TXHVWLRQV DERXW VXEPLVVLRQ S
LFFFV#DFDGHPLF QHW

Robust Image Encryption Method with Cipher Stream Chaining Process

Sovan Tep
International College
King Mongkut's Institute of Technology Ladkrabang
Bangkok 10520, Thailand
e-mail: 60610023@kmitl.ac.th

Isara Anantavrasilp
International College
King Mongkut's Institute of Technology Ladkrabang
Bangkok 10520, Thailand
e-mail: isara.an@kmitl.ac.th

***Abstract*—A new image encryption algorithm that uses one dimensional logistic map combined with perceptron model is proposed. The algorithm uses logistic map to produce pseudo random sequences, which are used sequences of keys to specify the weights of the perceptron. The, perceptron is used to encrypt the pixels of the image. The approach is also equipped with the novel Cipher Stream Chaining Process (CSCP), making it highly sensitive to given image. Our work is evaluated against histogram analysis, information entropy, key sensitivity analysis. Experiment results show that, the cipher image does not give out any information on the plain image and the algorithm is highly sensitive to plain image and key.**

Keywords-chaos; logistic map; perceptron model; encryption; security

I. INTRODUCTION

Today, the internet is used, not only for legacy services such as email, chat or file transfer, but also social interaction, multimedia, games and other entertainment. Countless amount of non-textual data such as images, video and audio are being shared and transferred every day. This raises privacy and security concerns, especially for personal multimedia data. Several data encryption standards such as DES, triple DES, AES [1] have been introduced. However, such algorithms may only be suitable to encrypt textual data [2], but not multimedia ones. The reason is that multimedia data especially images and videos may be highly redundant (adjacent pixels may contain the same color). Thus, human may still be able to perceive the original image from the cipher image [3]. Multimedia data are also much larger than textual ones.

Recently, the encryption scheme based on the chaotic map is also considered as a good technique in cryptography [4] due to its nonlinear behavior. It also produces unpredictable condition where a slightly change in the initial point can lead to two different divergence outcomes which is the most desirable to the property of the key in cryptography.

In the last decade, many algorithms using chaos-based application have been proposed. Hanchinamani and Kulkarn [5] proposed the image encryption based on the Peter de Jong chaotic map [6] and a RC4 stream cipher [7]. The algorithms involve with three steps: 1) Permutation: Scramble the position of the row and column along with the circular rotations in the alternative orientation. This is to decorrelate the adjacent pixels of the image based on the value obtained from chaotic map. 2) Pixel value circular rotation: Changing the value of the pixels. 3) Diffusion: Spreading the effectiveness of each pixel over the entire image. Thanks to their two rounds of encryption, the scheme is very sensitive the plain image. Hence, the algorithm is robust against differential attack. Long and Tan [8] proposed multiple chaotic map for the digital image encryption. The algorithm consists of three chaotic maps: Chebyhev map, Nonlinear Chaotic Algorithm (NCA) and Logistic map. The algorithm produces the keys of the encryption and decryption which are generated by the plaintext values and Chebyshev map. The keys are then fed into Logistic map and NCA for confusing and shuffling the plain image respectively. Rohith et al. [9] proposed image encryption using 1-D logistic map because it is simple to implement but very efficient. The algorithm uses map function to generate pseudo-random sequence as the key streams. Then it applies XOR operation with a new sequence, generated from linear feedback shift register to produce another set of key streams. Finally, they use the last output key steams to confuse the image pixel by using XOR operation. Wang et al. [10] proposed encryption algorithm based on Lorenz chaotic map without XOR operation, instead they introduce a new way to scramble the image pixel value using a perceptron model. Due to the complex structure of the perceptron, it is a good approach for confusing and changing the pixel values of the image. However, [9] and [10] encrypt each pixel separately. Thus, they are not sensitive to plain text. That is, if some parts of the plain text are changed, only some parts of cipher text change accordingly. Thus, the algorithms are vulnerable to the differential analysis attack.

To be resistant to differential analysis attack, a good cryptosystem should be sensitive with respect to the given key and plain image. Even just one bit of the key is flipped, it should yield two completely different cipher images when applied to an identical plain image. Also, using the same key, even just one bit in plain image is flipped, it should produce completely different cipher images [11]. In our work, the combination logistic map and perceptron-model approach is used to encrypt pixel values. More importantly, linear feedback shift register, which improves the encryption statistic, is deployed into the cipher stream chaining process. Such approach allows for image-wide pixel-dependent encryption. As a result, when the value in even one pixel is changed, the entire cipher image is changed.

The rest of the paper is structured as follows: The encryption and decryption algorithms are explained in

Section II. Experimental and result are discussed in Section III. In Section IV concludes the paper.

II. Encryption and Decryption Algorithms

A. Chaotic System and Logistic Map

Chaotic system is the type of nonlinear dynamical system which consists of a few parameter interactions and it is ruled by simple mathematic function. Despite their simplicity, the system is capable of producing a totally unpredictable value over time and widely divergent sequence parameter which is known as the chaotic behavior.

Logistic map is the one-dimensional chaotic system [12] defined by the following equation:

$$X_{i+1} = r \times X_i \times (1-X_i) \quad (1)$$

where r represents the growth rate and X_i denotes the population at a given index i. The distribution graph of the growing population X with respect to r from 0 to 4 is illustrated in the bifurcation diagram in Fig. 1.

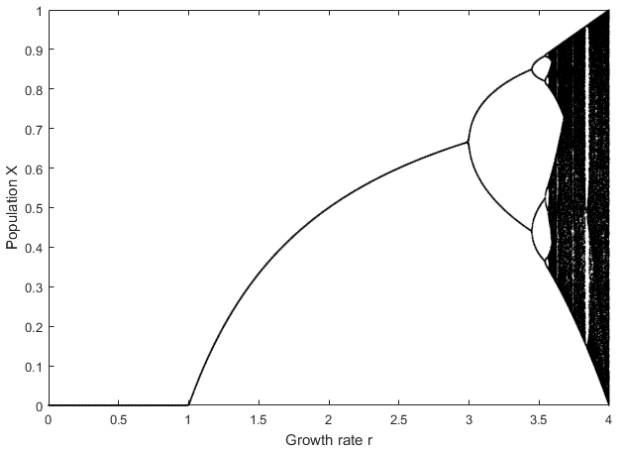


Figure 1. The chaotic behavior of the Logistic map function.

Each vertical slide in the Fig. 1 depict the population X of 100 generations toward the 1,000 discrete values of growth parameter r. At $r < 1.0$, the system population are always almost zero. Between 1.0 and 3.0, the population starts to settle into the exact point for each generation. From 3.0, the population is bifurcated into two different path and bifurcated into four different paths after the growth rate is set to 3.4. However, after $r > 3.6$, the system begins to oscillate into two then four, eight, sixteen and so on follow 2^n formula. At $r = 3.9$, it has bifurcated so many times that the system populations jump randomly in between all the paths. In this work, the value of growth parameter r is chosen to be 3.99, where the system produces highest randomness of the population X_i.

B. Perceptron Model

Our work employs Logistic map and perceptron model to encrypt images similar to that proposed in [10]. The perceptron model is very suitable for image encryption due to the complex relationship between the input and the output of the model. However, in [10], the encryption is done on each pixel separately, making the approach vulnerable to differential analysis attack. To overcome this problem, a new encryption/decryption algorithm called Cipher Stream Chaining Process (CSCP) is introduced.

C. Cipher Stream Chaining Process

Cipher Stream Chaining Process (CSCP) is a symmetric-key encryption and decryption method that perform XOR cipher, adding previous cipher pixel on the key that is used in the current pixel. In turn, the encryption result of each pixel depends on the previous pixel, creating a chain of encryptions.

To be more precise, after a pixel is encrypted Linear Feedback Shift Register (LFSR) [9] is applied to the cipher pixel. Then it is XORed with the key used to encrypt the next pixel. This novel approach ensures that the pixels are chained to each other, making highly sensitive to given plain image. Fig. 2 shows the encryption process. Decrypting an image is simply reversing the encryption process. LFSR is applied to the cipher image. Then the result is XORed with the key. (See Fig. 3.)

Our method is a symmetric-key method such that, different pixels being encrypted and decrypted with the different keys. Corresponding plain and cipher pixels use the same key to encrypt and decrypt respectively. Detail of the encryption and decryption processes are described in the following sections.

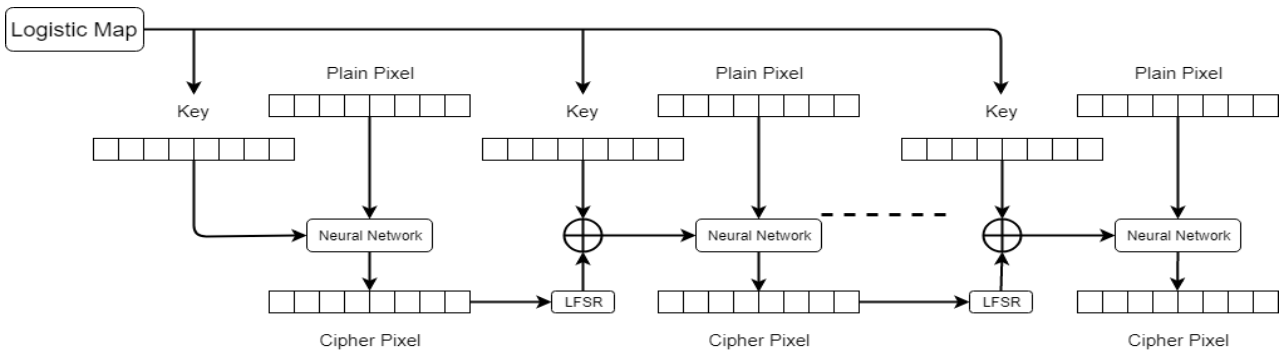


Figure 2. Encryption process.

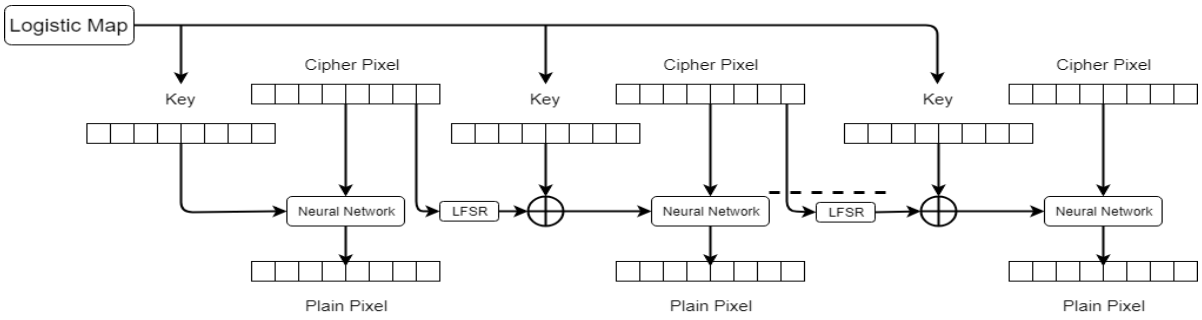


Figure 3. Decryption Process.

D. Encryption Algorithms

Image encryption process is as follows:

1) Given an 8-bit grayscale image of size M×N pixels, the image can be represented as a one-dimensional array P = <P_1, P_2,…….,P_n>, where P_i denotes values the i^{th} pixel of the image, $1 \le i \le n$, n = M×N and the value of a pixel is the 8-bit binary number corresponding to intensity of that pixel.

2) Set X_0 to any value within the range of [0,1] and r to any value between [3.99,4] as the initial parameters of the logistic map.

3) Calculate the Eq. (1) 2×n times, starting with X_0 to produce a sequence of population X = <X_1,X_2,……,X_{2n}>.

4) Normalize each value X_i, $1 \le i \le 2n$, as 8-bit binary representation using the following steps:

- Transform the value of X_i into unsigned integer in the range of [0, 255] by multiplying with 255:

$$X_i = X_i \times 255 \quad (2)$$

- Use round function to the sequence elements for converting them into their nearest decimal value:

$$X_i = \text{Round}\,(X_i) \quad (3)$$

- Convert each rounded X_i into 8-bits binary representation. This 8-bit representation will be used as encryption keys.

After repeating Step (4) for all elements in X, the sequence of the keys K = <K_1,K_2,……,K_{2n}>, where K_i is an 8-bit representation of rounded X_i is obtained.

5) To encrypt each pixel P_i in image P = <P_1,P_2,…….,P_n>, two keys in K, K_{2i-1} , K_{2i}, are required. Both keys are fed into the structure of perceptron to generate the values of weight and threshold for the perceptron model. The algorithm for producing the perceptron model is well explained in [10]. The overview process of encrypting the a plain pixel into a cipher pixel is described in Eq. (4).

$$C_i = NeuronNet(P_i\,,(\,K_{2i-1}\,,\,K_{2i}\,)) \quad (4)$$

where C_i, P_i, K_{2i-1} and K_{2i} denote the i^{th} cipher pixel, the i^{th} plain pixel and encryption keys at index *2i-1 and 2i, $1 \le i \le n$*, respectively. *NeuronNet*() is the function to encrypt the pixel using perceptron model.

6) To make our method more robust to differential analysis attack, pixel-chaining process is employed.

For the first plain pixel, we encrypt it using perceptron model directly. The cipher pixel is then applied by LFSR process. Next, it is XORed with the corresponding key. The process is repeated until the last pixel is encrypted. Chaining the pixel create better chaos to the cipher image, and thus more prone to differential analysis attack. The encryption process is described in Fig. 4.

For *i* from 1 to *n* do
  If *i* equal to 1
    $C_i = NeuronNet(P_i\,,(\,K_{2i-1}\,,\,K_{2i}\,))$
  Else
    C'_{i-1} = LFSR(C_{i-1})
    $K'_{2i-1} = K_{2i-1} \oplus C'_{i-1}$
    $K'_{2i} = K_{2i} \oplus C'_{i-1}$
    $C_i = NeuronNet(P_i\,,(\,K'_{2i-1}\,,\,K'_{2i}\,))$
  End if
End for

Figure 4. Encryption pseudo code.

7) After finishing the Step 6, the array of cipher pixels C = <C_1,C_2,…….,C_n> is generated. Then, the array is converted back into 8-bits grayscale cipher image. The encryption process is illustrated in Fig. 2.

E. Decryption Algorithms

In the decryption process, the cipher image is received. The procedure of the proposed image decryption process is described as follow:

8) An 8-bit grayscale of the cipher image of size M×N is obtained. It is then converted into array of pixels C = <C_1, C_2,…….,C_n>, where n = M×N and the value of a pixel is the 8-bit binary number corresponding to intensity of that pixel.

9) As the proposed method is symetric-key algorithm, the same key is used for both encryption and decryption process. Thus, the values of X_0 and r are chosen the same as Step 2 of the encryption process.

10) The value of X_0 and r obtained from Step 2 are used to generated the sequence of population X = <X_1,X_2,……,X_{2n}> using Eq. (1).

11) Normalize each value of X_i, $1 \le i \le 2n$, into 8-bit binary representation as described in Step 4 of the encryption process.

12) The perceptron model which is used for decrypting the pixel is the same as the encryption [10]. Thus, the process of decrypting the a cipher pixel into a plain pixel can be expressed as in Eq. (5):

$$P_i = NeuronNet(C_i, (K_{2i-1}, K_{2i})) \quad (5)$$

13) To decrypt the image, the reverse of CSCP is employed. (See Fig. 5.)

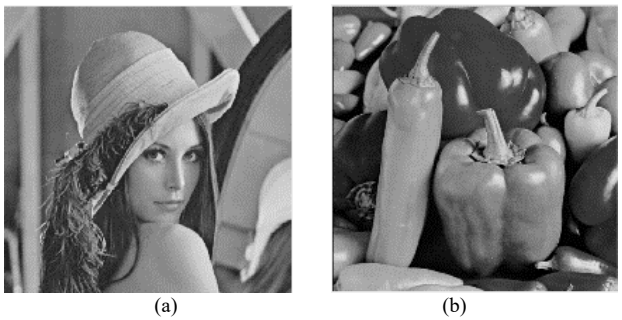
For i from 1 to n do
  If i equal to 1
    $P_i = NeuronNet(C_i, (K_{2i-1}, K_{2i}))$
  Else
    $C'_{i-1} = LFSR(C_{i-1})$
    $K'_{2i-1} = K_{2i-1} \oplus C'_{i-1}$
    $K'_{2i} = K_{2i} \oplus C'_{i-1}$
    $P_i = NeuronNet(C_i, (K'_{2i-1}, K'_{2i}))$
  End if
End for

Figure 5. Decryption pseudo code.

14) The one dimensional array of plain pixels $P = <P_1, P_2, \ldots\ldots, P_n>$ is generated. Finally, it is converted back into original 8-bit grayscale image. The decryption process is shown in Fig. 3.

III. Experimental Set Up and Result

Simulation was done in MATLAB to explore the efficiency of the proposed image encryption method. Grayscale images are used in the experiment because of high redundancy of adjacent pixels. As the initial value of logistic map, population $X_0 = 0.1$ and grow rate parameter $r = 3.99$ are chosen. In our experiments, we apply our method to the same images, Lenna and Peppers, that have been used in previous works [5][8]. Both, shown in Fig. 6, are grayscale images of size 256×256.



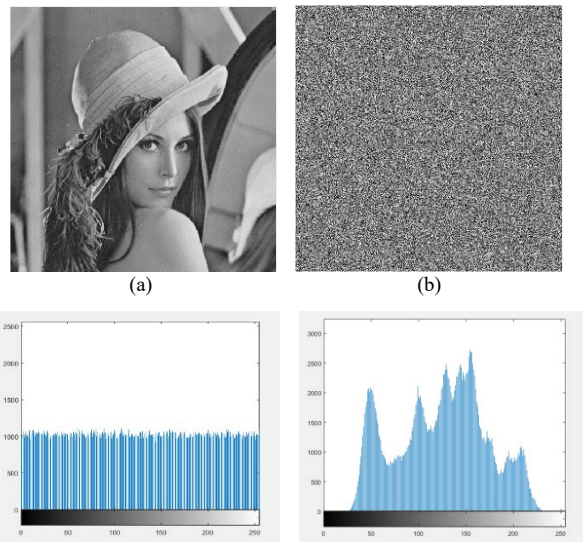
(a) (b)

Figure 6. The images, Lenna and Peppers, that are used in the experiments.

A. Histogram Analysis

A histogram is used to present the frequency distribution of pixel intensities of the image. An ideal cipher image should have the flat or uniform distribution, which is difficult to analyze the relationship between plain and cipher images.

In Fig. 7(a) and Fig. 7(b), it is shown that the image after encryption shows no information about the original image. More importantly, the histogram of the encrypted image in Fig. 7(d) is flat and does not resemble the the histrogram of the original image shown in Fig. 7(c).



(a) (b)

(c) (d)

Figure 7. (a) and (b) illustrate the plain and cipher images. Histograms corresponding to (a) and (b) are shown in (c) and (d), respectively.

B. Entropy Analysis

Entropy, introduced by Shannon in 1949 [13], is the important concept to study the degree of randomness of the given information. In our work, we use entropy to measure unpredictability or the randomness of the image pixel intensities. In other words, how random the intensity values of the cipher image is. To calculate the entropy, we use the following formula:

$$H(m) = \sum_{i=0}^{L-1} p(m_i) \log_2 \frac{1}{p(m_i)} \quad (6)$$

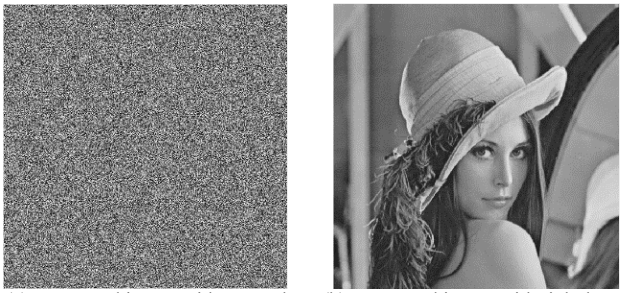
where L is the total number of the pixel intensity (normally L=256 for the 8-bit grayscale image), m_i denotes each of the pixel intensity values and $p(m_i)$ is the probability of m_i. According to the equation, the optimal value of the entropy is 8, which means that each pixel intensity has the same probability. Table 1 shows the comparison of the image entropy of the proposed scheme with other scheme in the literature. As shown in the table, entropies of cipher images of all approaches are almost 8.

TABLE I. Comparison of the Entropy Value of Proposed Method with Other Methods

Entropy of Encrypted image	Proposed Method	[5]	[8]	[10]
Fig. 6(a)	7.997637	7.997279	7.9976	7.9072
Fig. 6(b)	7.996949	7.997114	7.9972	7.6514

C. Key Sensitivity and Key Space Analysis

As mentioned earlier, good cryptosystem should be sensitive to keys. This is to make sure that different two keys cannot be used produce similar cipher image or to decrypt the same cipher image. In our experiment, we change the value of X_0 by 0.0000000000000001, while using the same parameter r, to study the effect of infinitesimal difference of key values.



(a) Decrypted image with wrong key. (b) Decrypted image with right key.

Figure 8. Decrypted images with different and same key.

As shown in Fig. 8(a), decrypting image with the wrong key cannot be reversed back to the original image.

Another aspect of the strength of encryption algorithm is the size of the key space or the amount of all possible key values. The larger the key space, the more difficult to conduct the brute force attack. In logistic map, number of possible values of both X_0 and r are 10^{16} [14]. The key space of the algorithm is, therefore, $10^{16} \times 10^{16} = 10^{32}$.

D. Differential Attack Analysis

Strong cryptography algorithms should be sensitive to the plaintext attack or differential analysis attack where the algorithms produce two different cipher images from two plain images with a small difference. Let C_1 and C_2 be the cipher images which are corresponding to the original image P_1 and P_2 with only one-pixel difference, respectively. Number of Pixels Change Rate (NPCR) can be used to calculate the percentage of different pixel between C_1 and C_2 and the Unified Average Changing Intensity (UACI) can be used to measure the average differences of pixel intensity between C_1 and C_2 [15]. NPCR and UACI are defined as follows:

$$NPCR = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i,j) \times 100\% \quad (7)$$

$$UACI = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\% \quad (8)$$

where M and N are the width and height of the image, respectively, $C_1(i,j)$ and $C_2(i,j)$ are the intensity values of the two cipher images at position (i,j) and $D(i,j)$ is the bipolar array which is defined as the following formula:

$$D(i,j) = \begin{cases} 0 & if\ C_1(i,j) = C_2(i,j) \\ 1 & if\ C_1(i,j) \neq C_2(i,j) \end{cases} \quad (9)$$

The results of NPCR and UCAI evaluations are shown in Table 2 and 3.

TABLE II. COMPARISON OF NUMBER OF PIXEL CHANGE RATE RESULTS WITH OTHER METHODS

Image	Proposed Method	[5]	[8]	[10]
	NPCR	NPCR	NPCR	NPCR
Fig. 6(a)	100	99.61	99.62	0.00152587
Fig. 6(b)	100	N/A	99.63	0.00152587

TABLE III. COMPARISON OF UACI RESULTS WITH OTHER METHODS

Image	Proposed Method	[5]	[8]	[10]
	UACI	UACI	UACI	UACI
Fig. 6(a)	33.53	33.46	33.54	0.00040091
Fig. 6(b)	33.59	N/A	33.43	0.00129250

E. Peak Signal-to-Noise Ratio

To measure the ratio of mean square difference between the original image the encrypted image, Peak Signal-to-Noise Ratio (PSNR) [16] is used. In this case, the original image and the cipher image are considered as the signal and noise, respectively. The formula is defined as below:

$$PSNR = 10 log_{10}\left(\frac{255^2}{MSE}\right) \quad (10)$$

where MSE is the mean square error between two images and computed as follow.

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (P(i,j) - C(i,j))^2 \quad (11)$$

where M is the width of the image, N is the height of the image and $P(i,j)$ and $C(i,j)$ are the pixel intensity of the plain image and cipher image at location (i,j), respectively.

As the difference between two image pixel value in the same position is higher, the value of PSNR has become lower and approach to zero for the maximum of different pixel value between two grayscale images. Table 4 shows the comparison result of PSNR of the proposed method.

TABLE IV. COMPARISON OF THE PEAK SIGNAL-TO-NOISE RATIO RESULT OF PROPOSED METHOD WITH OTHER METHOD

Image	Proposed Method	[5]	[10]
	PSNR	PSNR	PSNR
Fig. 6(a)	9.226572	9.215507	11.1648
Fig. 6(b)	8.463215	8.924724	9.2049

IV. CONCLUSION

In this research work, a new image encryption method based on the Logistic map combined the perceptron model, called Cipher Stream Chaining Process (CSCP), is proposed.

It is equipped with cipher-pixel chaining making it highly sensitive to input image. The experiment results show that the encrypted image is completely different from the original, both in terms of human vision and statistics. The pixel change rate and unified average changing intensity of the proposed method suggest that it is robust against the differential attack analysis. In the future, we will evaluate our approach on other images with different sizes. Potential implementations on color images and video files must also be investigated.

REFERENCES

[1] R. A Mollin. 2006. “An Introduction to Cryptography”. Boca Raton, FL: CRC Press.

[2] J A. K. Mandal, C. Parakash and A. Tiwari, “Performance evaluation of cryptographic algorithms: DES and AES, ” *2012 IEEE Students' Conference on Electrical, Electronics and Computer Science*, Bhopal, 2012, pp. 1-5.

[3] S. Lian, Multimedia Content Encryption: Techniques and Application, CRC, 2008.

[4] G. Srividya and P. Nandakumar, "A Triple-Key chaotic image encryption method," 2011 International Conference on Communications and Signal Processing, Calicut, 2011, pp. 266-270.

[5] Hanchinamani,G.; Kulkarn,L. ; “An Efficient Image Encryption Scheme Based on a Peter De Jong Chaotic Map and a RC4 Stream Cipher”, in 3D Res 6:30, DOI 10.1007/s13319-015-0062-7, 2015.

[6] M. Budhraja, N. Kumar, and L. M. Saha. The 0-1 test applied to peter-de-jong map. *Int. J. Eng.Innov. Tech.,* 2(6):253-257, 2012.

[7] Wong, K.K, Carter, G., Dawson, E.(2010). An analysis of the RC4 family of stream ciphers against algebraic attacks. *Proceesing 8th Australasian information security conference, 103,* pp. 67-74.

[8] M. Long and L. Tan, "A Chaos-Based Data Encryption Algorithm for Image/Video," *2010 Second International Conference on Multimedia and Information Technology*, Kaifeng, 2010, pp. 172-175.

[9] S. Rohith, K. N. H. Bhat and A. N. Sharma, "Image encryption and decryption using chaotic key sequence generated by sequence of logistic map and sequence of states of Linear Feedback Shift Register," *2014 International Conference on Advances in Electronics Computers and Communications*, Bangalore, 2014, pp. 1-6.

[10] Xing-Yuan Wang, Lei Yang, Rong Liu. “A Chaotic image encryption algorithm based on perceptron model”, Springer Science + Business Media B.V. 2010.

[11] Alvarez, G., Li, S.J.: “Some basic cryptographic requirement for chaos-based cryptosystem”, Int. J. Bifurcation Chaos, 2006, 16, (8), pp. 412-417

[12] Z. Yan-Bin and D. Qun, "A New Digital Chaotic Sequence Generator Based on Logistic Map," *2011 Second International Conference on Innovations in Bio-inspired Computing and Applications*, Shenzhan, 2011, pp. 175-178.

[13] C. Shannon, “Communication theory of secrecy sytem”, Bell system Technical Journal 28:656-715, 1949.

[14] X. Wang, C. Jin, “Image encryption using game of life permutation and PWLCM chaotic system”, Opt. Commun., 2012, 285, pp. 412-4.

[15] Y. W. Joseph, P. Noonan and S. Agaian, “NPCR and UACI Randomness Tests for Image Encryption”, Department of electrical and Computer Engineering Tufts University Medford, MA, USA.

[16] Taneja, N., Raman, B., & Gupta, I. “Combinational domain encryption for still visual data”, Multimedia Tools and Application, (2012), 159(3), 775-793. doi:10.1007/s11042-011-0775-4.

Personal Information

Name	Sovan TEP
Sex	Male
Nationality	Cambodian
Date of Birth	27 September, 1994
Place of Birth	Russey Kev district, Phnom Penh City, Cambodia

Education

Bachelor degree

Project	GIC Infrastructure Installation
Field of Study	Information Technology
Duration	2011-2016
Department	Department of Information and Communication Engineering
University	Institute of Technology of Cambodia

Master degree

Thesis	Robust Image Encryption Method with Cipher Stream Chainning Process
Field of Study	Computational Intelligence System
Duration	2017-2019
College	International College
University	King Mongkut's Institute of Technology Ladkrabang, BangKok, Thailand

Research Interests

Data Security, Machine Learning, and Optimization