Combining Two Chaos Maps and Determining Selective Methods for MSB Bits in a Digital Image Encryption Algorithm

Rinaldi Munir

School of Electrical Engineering and Informatics, Bandung Institute of Technology, Bandung, Indonesia
email: rinaldi-m@stei.itb.ac.id

ARTICLE INFO

History :

Submit on 27 October 2024
Review on 15 November 2024
Accepted on 30 November 2024

Keyword :

Encryption;
Image, Chaos;
Selective;
Arnold Cat Map;
Logistic Map

ABSTRACT

In order to reduce the computational volume, we employ selective encryption approaches in conjunction with a chaos-based picture encryption algorithm in this research. Two chaos maps are used, namely Arnold Cat Map and Logistic Map. Before encryption, the image is scrambled with Arnold Cat Map, then selective encryption techniques are applied by selecting only four MSB bits from each pixel to be XORed with the keystream generated from the Logistic Map. Experimental results show that the use of both chaos functions can produce confusion and diffusion effects, and the use of selective encryption techniques only processes 50% of the entire image data. The encrypted image shows a relatively uniformly distributed histogram, making it difficult for attackers to perform statistical analysis to find the key or plain image. Chaos sensitivity shows that this algorithm is safe from exhaustive-key search attacks. This method is sensitive to modest changes in the key, making it safe from exhaustive-key search assaults, according to experiments conducted by gently altering the initial value of chaos. This technique is immune to brute-force attacks because of its sufficiently huge key space.

Corresponding Author:

Rinaldi Munir ✉
School of Electrical Engineering and Informatics (STEI), Bandung Institute of Technology (ITB) Jl.Ganesha 10, Bandung 40132, Indonesia
Email: rinaldi-m@stei.itb.ac.id

INTRODUCTION

Image is one form of data or information presented visually. Image plays an important role in today's multimedia industry [1]. Image is also an element that forms a video, because a video is basically composed of a series of image frames that are displayed in a fast tempo [2]. In addition to being stored in storage media, images are also sent electronically through public channels such as the internet [3]. Storing or sending images through transmission channels is vulnerable to access or tapping by unauthorized parties. Therefore, to protect the confidentiality of images from illegal access, image encryption has been widely used as a way to maintain information security [4].

Most available cryptographic algorithms are intended to encrypt text data. Conventional cryptographic algorithms such as DES, AES, Blowfish, RC4, RSA, etc. are not effective for encrypting image data. This is because image data is generally very large in volume compared to text data, so it takes longer computing time to encrypt images [5]. For real-time applications such as teleconferences, live video streaming, etc., conventional algorithms are clearly not suitable for encrypting images [6].

Many researchers have developed encryption algorithms for digital images. According to Younes (2008)[7], most image encryption algorithms can be grouped into two groups: (a) non-chaos selective encryption algorithms, and (b) chaos-based selective or non-selective encryption algorithms. Selective algorithms mean that they only encrypt some elements in the image but the effect is to encrypt the image as a whole [8]. Selective encryption algorithms aim to minimize the computational volume during the encryption and decryption process so that they can be used for real-time application needs [9]. Chaos is an attractive topic in cryptography for three reasons: (1) sensitivity to initial conditions, (2) random behavior, and (3) no repeating period. The use of chaos in cryptography can produce a diffusion effect as stated by Shannon [10]. Chaos in cryptography is generally used as a random number generator. The random numbers are used as keystreams (with a simple XOR operation) or to randomize the arrangement of pixels in the image. The sequence of random numbers is generated with a chaos function (map) [11]. Use of Tent Map as an encryption key generator, Use of Arnold Cat Map to randomize pixels. The same thing also applies to the use of Henon Map for pixel permutations before being encrypted with a stream cipher, while others collaborate with Chebysev Map as a keystream generator [12].

In this paper, a chaos-based image encryption algorithm is proposed. The algorithm combines two chaos functions, namely Arnold Cat Map and Logistic Map. Arnold Cat Map is used to randomize the arrangement of pixels, while Logistic Map is used as a keystream generator. To save computational volume during the encryption/decryption process, the proposed selective encryption technique is applied by only XORing the keystream with the MSB bits that play a role in determining the visual perception of objects in the image.

METHOD

In our method we use several experiments including the use of encryption such as chaos Arnold Cat Map (ACM) and Logistic Map [2]. Added with several encryptions derived from previous research such as selective encryption. For the stages in the experiment can be seen in the following figure 1:

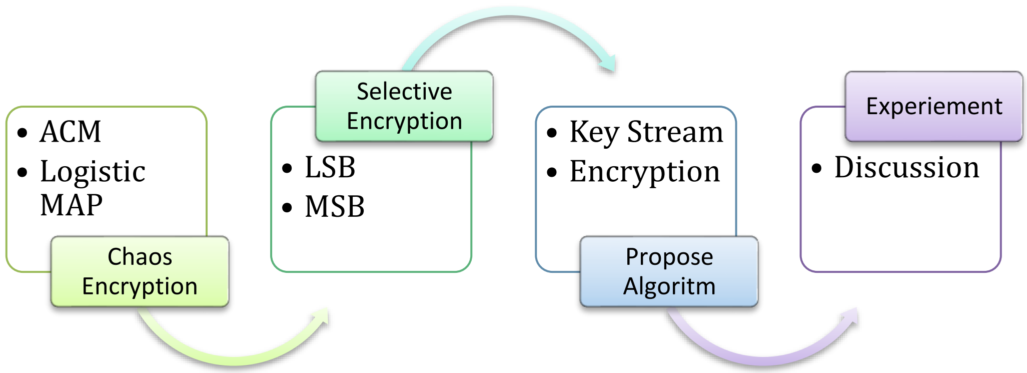

Figure 1, Image Encryption Experiment Stages.

RESULT & DISCUSSION

The main characteristic of chaotic systems is their sensitivity to the initial value parameters. This sensitivity means that if the chaos map is iterated a certain number of times, then small changes in the initial value parameters of the map produce significant differences in the value of its function [13]. This characteristic is important in cryptography because it is in accordance with the diffusion principle proposed by Shannon [14]. With this diffusion principle, changing one bit of the initial value parameter of chaos can cause the ciphertext to be unpredictable and as a consequence the ciphertext remains undecryptable [15]. The two chaos functions used in this algorithm are Arnold Cat Map and Logistic Map. Each function is explained in the sub-sections below.

3.1. Arnold Cat Map.

Arnold Cat Map (ACM) is a two-dimensional chaotic function that transforms the (x, y) coordinates in an image to new coordinates in the same image. The transformation equation is,

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} - \begin{bmatrix} 1 & p \\ q & p\,q+1 \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} \quad \mathrm{mod}(N) \tag{1}$$

which in this case (xi, yi) is the pixel position in the image of size NxN and (xi+1, yi+1) the new pixel position after the transformation; p and q are positive integer.

ACM iteration on an image will scramble the image, which is the same as encrypting the image [16]. By doing iterations many times, different random images are obtained. However, after a certain iteration, the original image is produced again, therefore ACM has a period. Figure 2 shows the ACM iteration on the image of a 'bird'. The number of iterations required for a random image to return to its original state varies depending on the size of the image. The number of iterations required is less than 3N, where N is the image dimension (e.g. if the image is 256x256 then N = 256)

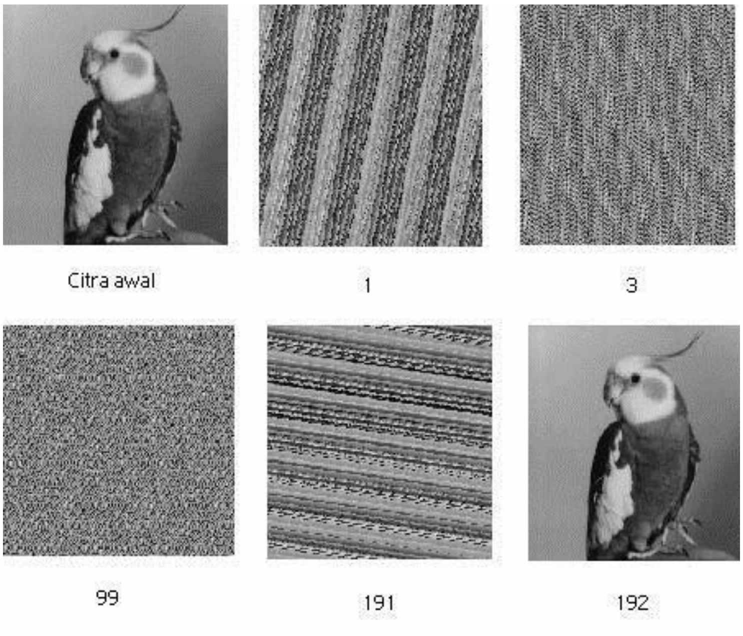

Figure 2, ACM iteration on the 'bird' image

Although p and q are secret parameters, due to the periodic nature of ACM which can reproduce the original image, encryption using ACM alone is not secure, because through a simple hack the values of p and q can be found through brute force operations. In addition, ACM only changes the position of the pixel in the image but does not change the pixel value [17]. Therefore, we need to encode the pixel values using the second chaos map, namely the Logistic Map.

3.2. Logistic Map.

Logistic Map is a one-dimensional chaotic function in the form $x_i + 1 = r\,x_i\,(1 - x_i)$. The value of xi is between 0 and 1. The constant r represents the growth rate of the function and $0 \leq r \leq 4$. This equation starts to become chaotic when r > 3.75. When r = 4 the function becomes totally chaotic and the values of xi are no longer predictable, meaning they are random. The initial value of chaos, x0, and the constant r act as secret parameters of the Logistic Map. The random values generated do not have a period, although the Logistic Map remains deterministic. The sequence of random values generated from iterations of the Logistic Map is sensitive to small changes in the initial value. By changing the value of x0 by just a small amount Δ (is $x_0 + \Delta$), the sequence of random values generated - after several iterations - is significantly different from the previous random sequence with the initial value of x0.

3.3. Selective ENCRYPTION

Each pixel is represented by a number of bytes. The bit arrangement in each byte is b7b6b5b4b3b2b1b0. The leftmost bits are the most significant bits (MSB), while the rightmost bits are the least significant bits (LSB) [17]. If every i-th bit of each pixel in the grayscale image is extracted and plotted into each bitplane image, we obtain eight binary images. Figures 3(a) to 3(i) show the bitplane images of the cameraman image. Figures 3(b) to 3(f) taken from the MSB bits can still show the shape of the object in the image, but from Figures 3(g) to 3(i) taken from the LSB bits, it already looks like a random image.

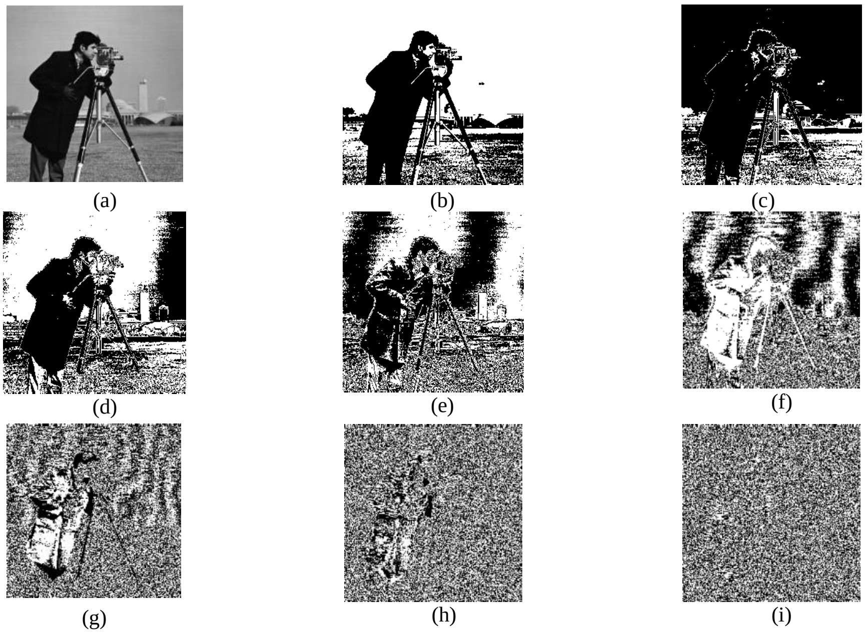

Figure 3, Eight Bitplanes on the cameraman image

Since the MSB bits determine the appearance of the object in the image, changing the MSB bits produces an image that is no longer recognizable. So, we only need to select only the MSB bits to be encrypted because by encrypting only those bits, the entire image becomes unrecognizable. This is the basis of the selective encryption technique based on MSB bits.

3.4. Propose Encryption

The selected MSB bits of each pixel are XORed with a four-bit keystream. The four-bit keystream ki is obtained as follows: the chaos value xi is multiplied by 10 repeatedly until it reaches the desired size, then truncated to take only the integer part. Mathematically, the chaos value x is converted to an integer using the following equation:

$$T(x, size) = x * 10^{count} , x \neq 0 \qquad (2)$$

which in this case count starts from 1 and increases by 1 until $x * 10^{count} > 10^{size - 1}$. The result is then taken only the integer part (symbolized by a pair of double lines in equation 5 which symbolizes truncation). The last four bits of the binary representation of the integer are used as ki. Without loss of generality, the following explains the steps in the encryption algorithm for grayscale images.

3.5. Experiments and Discussion

To determine the functionality and security of the algorithm, an experiment was conducted using Matlab tools. Two test images used were a grayscale image and a color image. The two images were the image of a 'ship' (512 x 512) and the image of a 'flower' (512 x 512), as shown in Figures 4(a) and 4(b). The key parameters used in the experiment were: p = 15, q = 27, r = 3.98, x0 = 0.6938, and m = 5. The encrypted images (cipher-image) are shown in Figures 4(c) and 4(d) respectively. It appears that the encrypted image is no longer recognizable because it looks like a random image. Decryption of the cipher-image produces exactly the same image as the original 4(a) and 4(b).

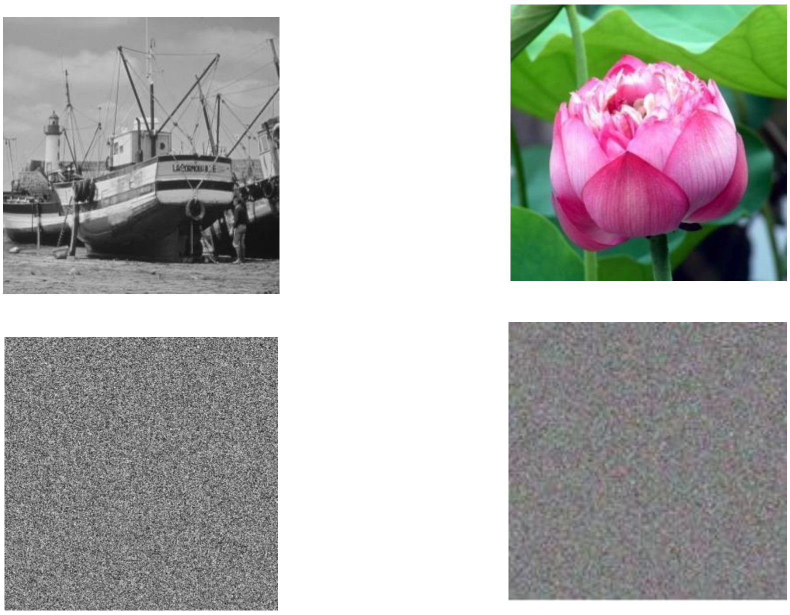

Figure 4. (a) and (b) plain-images, (c) and (d) cipher-images

The experimental results above are then discussed in the sections below, including histogram analysis, ACM iteration result analysis, sensitivity analysis, and key space.

3.6. Analysis of ACM Iteration Results

Before encryption, the image is scrambled by iterating ACM five times. The results of the scrambled image pixels are shown in Figures 5(a) and 5(b), for the 'ship' image and the 'flower' image, respectively. Five iterations can make the image unrecognizable. However, this scramble does not change the pixel values, so it is still not cryptographically secure. The histogram remains the same as in Figures 4(a) and 5(a)-(c).

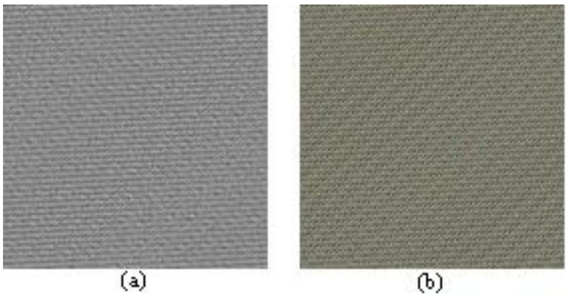

Figure 5. (a) and (b) are the randomized images with m = 5 iterations for each plain image.

The initial value parameter of the chaos function acts as (one of) the secret keys. The nature of chaos is sensitive to small changes in the initial value. Sensitive means that if the key value is changed even slightly, the decryption result of the cipher-image produces another different cipher-image.

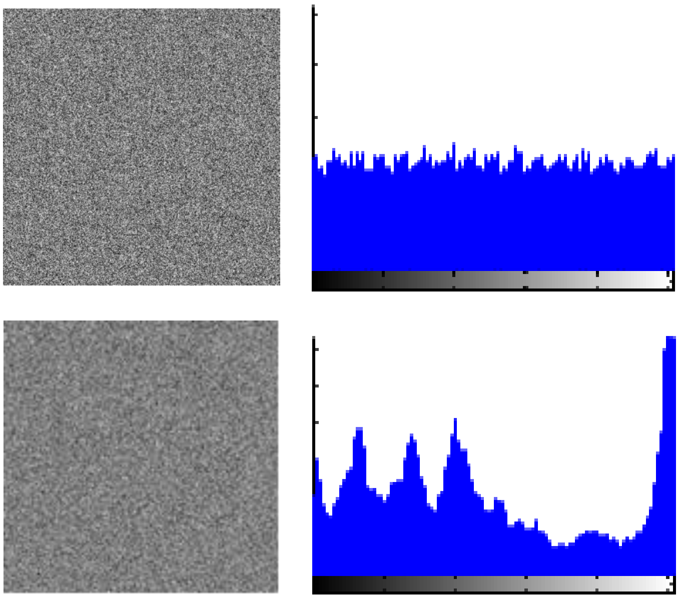

Figure 6. Results of the decryption experiment with a change in x0 of $\Delta = 10^{-10}$

In this experiment, the initial value of the logistic map is changed by Δ so that it becomes $x_0 + \Delta$, then the image is decrypted with the key $x_0 + \Delta$. Suppose Δ= 10–10 so that the initial value of the logistic map becomes 0.6938000001. Figure 7 shows the decryption result of the cipher-image from the image of the 'ship'. The result is another cipher-image that turns out to be still scrambled (does not return to the original image). Small changes in the initial value of chaos make the resulting random value significantly different after the chaos function is iterated a number of times. Attackers who perform brute force attacks to find the key will be frustrated because very small changes in the key cause the decryption result to remain wrong. The key space represents the total number of different keys that can be used for encryption/decryption. The key space should be large enough to make brute-force attacks inefficient. There are more than one secret key parameter used in the encryption algorithm, namely p, q, m, x0, and r. The first three parameters, p, q, and m are positive integers. Matlab supports a maximum of unsigned integers up to 32 bits, so the possible integer choices are about 232 = 4.3 ⍰⍰109. For the initial value of the Logistic Map (x0), the computational precision for a 64-bit double-precision according to the IEEE floating-point standard is 10–15 (Fu, 2012), so the number of possible values of x0 is 1015. Thus, the total key space is:

$$\begin{aligned} H(p, q, m, x_0, r) &\approx (4.3 \times 10^9) \times (4.3 \times 10^9) \times \\ &\quad (10^{15}) \times (10^{15}) \\ &\approx 18.49 \times 10^{48} \end{aligned}$$

which is large enough to withstand brute-force attacks.

CONCLUTIONS

In this paper, a proposed digital image encryption algorithm has been presented that combines the use of two chaos maps and selective encryption techniques. Arnold Cat Map is iterated on plain images m times before being selectively encrypted with a keystream generated by Logistic Map. With selective encryption techniques, only 4-bit MSB of each pixel is encrypted. So, only 50% of the entire image is processed to obtain the overall encrypted image. Experimental results show that this algorithm can encrypt any image (both grayscale and color images) well. The pixels in the cipher image have a relatively uniform distribution, as shown by the relatively flat shape of its histogram, making it difficult for attackers to attack using statistical analysis. Experiments by slightly changing the initial value of chaos show that this algorithm is sensitive to small changes in the key so that it is safe from exhaustive-key search attacks. The large enough key space makes this algorithm resistant to brute-force attacks.

REFERENCE

[1] L. E. George, E. K. Hassan, S. G. Mohammed, and F. G. Mohammed, "Selective image encryption based on DCT, hybrid shift coding and randomly generated secret key," *Iraqi J. Sci.*, pp. 920–935, 2020.

[2] N. Iqbal *et al.*, "On the image encryption algorithm based on the chaotic system, dna encoding, and castle," *IEEE Access*, vol. 9, pp. 118253–118270, 2021.

[3] A. ur Rehman, X. Liao, A. Kulsoom, and S. A. Abbas, "Selective encryption for gray images based on chaos and DNA complementary rules," *Multimed. Tools Appl.*, vol. 74, pp. 4655–4677, 2015.

[4] S. Kaur and D. Gupta, "A review of image encryption schemes based on the chaotic map," *Int. J. Comput. Technol. Appl.*, vol. 5, no. 1, p. 144, 2014.

[5] X. Liu, Y. Song, and G.-P. Jiang, "Hierarchical bit-level image encryption based on chaotic map and feistel network," *Int. J. Bifurc. Chaos*, vol. 29, no. 02, p. 1950016, 2019.

[6] A. Kulsoom, D. Xiao, and S. A. Abbas, "An efficient and noise resistive selective image encryption scheme for gray images based on chaotic maps and DNA complementary rules," *Multimed. Tools Appl.*, vol. 75, pp. 1–23, 2016.

[7] A. Shafique and J. Shahid, "Novel image encryption cryptosystem based on binary

bit planes extraction and multiple chaotic maps," *Eur. Phys. J. Plus*, vol. 133, no. 8, p. 331, 2018.

[8] S. S. Moafimadani, Y. Chen, and C. Tang, "A new algorithm for medical color images encryption using chaotic systems," *Entropy*, vol. 21, no. 6, p. 577, 2019.

[9] S. Som, A. Mitra, S. Palit, and B. B. Chaudhuri, "A selective bitplane image encryption scheme using chaotic maps," *Multimed. Tools Appl.*, vol. 78, pp. 10373–10400, 2019.

[10] Y. Liu, Z. Qin, and J. Wu, "Cryptanalysis and enhancement of an image encryption scheme based on bit-plane extraction and multiple chaotic maps," *IEEE Access*, vol. 7, pp. 74070–74080, 2019.

[11] A. Ur Rehman, D. Xiao, A. Kulsoom, M. A. Hashmi, and S. A. Abbas, "Block mode image encryption technique using two-fold operations based on chaos, MD5 and DNA rules," *Multimed. Tools Appl.*, vol. 78, no. 7, pp. 9355–9382, 2019.

[12] R. Premkumar and S. Anand, "Secured and compound 3-D chaos image encryption using hybrid mutation and crossover operator," *Multimed. Tools Appl.*, vol. 78, pp. 9577–9593, 2019.

[13] H. Kolivand, S. F. Hamood, S. Asadianfam, and M. S. Rahim, "Image encryption techniques: A comprehensive review," *Multimed. Tools Appl.*, 2024.

[14] T. M. Hoang, M.-H. Hoang, and Q.-A. Pham, "Dynamical Selective Image Encryption Using Chaos," in *2024 9th International Conference on Integrated Circuits, Design, and Verification (ICDV)*, 2024, pp. 67–72.

[15] M. Lyle, P. Sarosh, and S. A. Parah, "Adaptive image encryption based on twin chaotic maps," *Multimed. Tools Appl.*, vol. 81, no. 6, pp. 8179–8198, 2022.

[16] T. M. Hoang, "A novel design of multiple image encryption using perturbed chaotic map," *Multimed. Tools Appl.*, vol. 81, no. 18, pp. 26535–26589, 2022.

[17] J. Shankar and C. Nandini, "Hybrid hyper chaotic map with LSB for image encryption and decryption," *Scalable Comput. Pract. Exp.*, vol. 23, no. 4, pp. 181–192, 2022.