International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 23 (2018) pp. 16573-16577

Logistic map based image encryption scheme

Harshvardhan Tiwari[1], Hamsapriye[1], N. Satish Kumar[2]

[1]Centre for Incubation, Innovation, Research and Consultancy (CIIRC)
[2]Information Science and Engineering, Jyothy Institute of Technology,
Bangalore, Karnataka, India

Abstract

In this paper we have presented a simple and secure scheme for image encryption using one-dimensional logistic map. This image encryption scheme first shuffles the position of pixel values and then changes the gray values to make the complex relationship between original plain image and encrypted image. Image scrambling and diffusing, both operations are performed by logistic map. Various experiments have been conducted to test the robustness and security of proposed image cipher algorithm and the experimental results shows that the proposed scheme is resistant to different cryptanalytic attacks and provides adequate security.

Keywords: Image encryption; logistic map; diffusion; cryptographic attacks.

I. INTRODUCTION

Digital technology is growing rapidly and it causes the wide spread distribution of digital documents and images over the Internet. The security of digital documents, images and other multimedia data has become extremely important for common people and government. The secure transmission of digital images is an important issue of information security field. Cryptographic encryption techniques provide the effective security to data by converting it into un-understandable form to attackers. Public key based cryptographic encryption algorithms are widely used in a large number of applications. One possible way of digital image protection is to use well-known and traditional cryptographic algorithms such as DES, Blowfish, AES, and IDEA [1, 2, 3] to mask the digital image information. However the encryption of image is not similar to the encryption of text. Intrinsic features of images, such as large data capacity, high redundancy and high correlation among adjacent pixels make image encryption very complex. Due to above mentioned features and high computation requirements these traditional text encryption algorithms are not suitable for the encryption of image. Chaotic theory has drawn wide attention among researchers so far, since it is very sensitive to system parameters and initial values. These distinct features make the chaos system more ergodic[4]. Chaotic system strengthens various security applications by its unique chaotic characteristics and makes it different from traditional text encryption algorithms. Thus, chaotic encryption system has great importance in information security field because of its easy to control, deterministic and pseudo-random behavior [5, 6]. Chaos-based cryptosystem is based on chaotic maps. There are two types of chaotic maps: single dimensional chaotic maps [7] and multi-dimensional chaotic maps [8]. One-dimensional chaotic maps are having less number of control parameters and variables as compared to high dimensional chaotic maps. In recent times, different chaotic maps based image encryption schemes have been given. The vast majority of them are built on the permutation and diffusion methods. In [9] authors have proposed substitution-permutation network structure and chaotic systems based image encryption approach. In this work two chaotic systems used. They have performed two diffusion phases along with diffusion and permutation to achieve a good randomness in encryption method. In [10] authors have proposed a hyper-chaotic map. The map is derived from the Sine map and iterative chaotic map within finite collapse. This map has shown good dynamical characteristic for encryption application. A. Houas et al. [11] proposed an algorithm to encrypt binary images. Ye and Huang [12] designed an image encryption algorithm which is based on auto-blocking and a medical Electrocardiography (ECG) signal with the help of the chaotic Logistic map and generalized Arnold map. In [13] researchers have given an image encryption scheme using random vectors. In decryption phase they have used both the randomly generated vectors and the ciphered image to reconstruct the original image by applying least square approximation techniques. In [14] image encryption design is based on two pseudorandom bit generators. These pseudorandom bit generators are used for substitution and permutation. Researchers in [15] have used a four-dimensional hyper-chaotic map to encrypt the image.

This paper presents a logistic map based encryption scheme for images. The proposed scheme uses chaotic logistic map to mix up the pixels and generate the random sequences for performing the operations to confuse the pixel values in an image. A 256-bit secret key has been generated with the help of SHA-512 [18] hash function to produce initial conditions for each logistic function. SHA-512 hash function generates 512-bit hash value for a given input, one part of it (256-bit) is used for shuffling and other part is used in confusion operations. The rest of paper is organized as follows. In Section 2 the chaotic logistic map is discussed. In Section 3 image encryption algorithm is presented. Its performance and security is analysed in Section 4. Finally we concluded the paper in Section 5.

II. LOGISTIC MAP

The Logistic map presents a polynomial map of degree two. It is a simple and one-dimensional discrete-time non-linear system. This widely used function exhibits quadratic non-

linearity and is defined by following equation [16]: $x_n = \mu x_{n-1}(1-x_{n-1})\ldots\ldots(1)$

Where μ is a control parameter and it lies between 0 and 4. The chaotic sequence is represented by x_n and it lies between 0 and 1. The logistic map becomes chaotic when the control parameter lies between 3.57 and 4. The bifurcation figure of one-dimensional logistic map has been shown in Figure 1. The diagram presents periodic windows in fixed intervals. The existence of periodic windows must be avoided; otherwise the ciphertext would not show random-like behaviour and resulting in an inefficient encryption procedure [17].

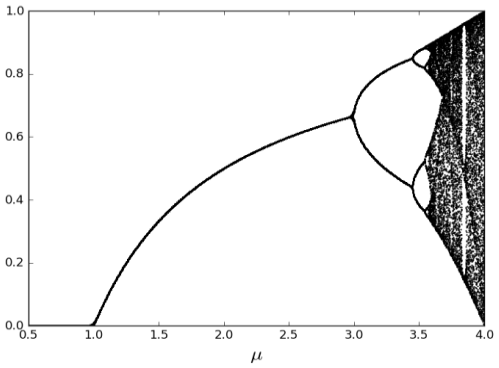

Fig.1(a) Bifurcation diagram for μ<1

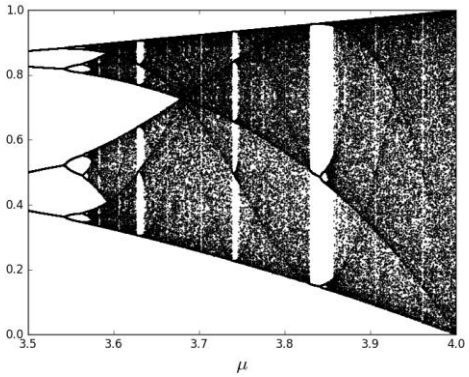

Fig.1(b) Bifurcation diagram for μ>3.5

III. SHA-2

In addition to the SHA-0/1 hash functions, the NSA and NIST also published a set of more complex hash functions to incorporate the need for hashes that offer more security, especially longer hash values ranges from 224-bit to 512-bit. These hash algorithms, called SHA-224, SHA-256, SHA-384 and SHA-512 (referred to as SHA-2) are more complex because of the added nonlinear functions to the compression function. Their suffix originates from the bit length of the hash value they produce. The versions SHA-224 and SHA-384 are obtained by truncating the result from SHA-256 and SHA-512 respectively. Fortunately, the SHA-2 hash functions produce longer hashes, making a feasible attack more difficult. Consider for example the SHA-512 hash function, producing 512 bit hashes and thus having an approximate complexity against collision attacks of 2256. Even if the logarithmic complexity would be halved (from 256 to 128), this would still be out of reach for practical purposes for the coming decade or so. SHA-512 uses a block size of 1024-bit and has 80 steps.

IV. PROPOSED WORK

The proposed encryption scheme involves three steps to produce cipher image. In the first step hash value of input image has been calculated. SHA-512 [18] generates 512-bit (64-characters) hash value. This hash value has been divided into two parts. In the next two steps we performed the confusion and shuffling operations respectively. For performing confusion and shuffling operation two chaotic systems (both are logistic map) are used. In second step first 256-bits of hash value is used for generating the initial conditions for first logistic map. Similarly the last 256-bits of hash value is used for generating the initial conditions for second logistic map in third step.

Let the size of an image I is $M \times N$. Each pixel of image I represented as $I(p,q)\ for 1 \le p \le M, 1 \le q \le N$. $I(p,q)$ denotes the gray value at the pixel position (p,q) of the image I. Initial conditions for logistic maps are calculated as follows:

$$x_0 = \sum_{i=1}^{32} \mathrm{mod}(h_i \times 10^i), 1) \ldots\ldots(2)$$

$$x_0' = \sum_{i=33}^{64} \mathrm{mod}(h_i \times 10^i), 1) \ldots\ldots(3)$$

Where $h_i, 1 \le i \le 64$, is a character of hash value. The complete procedure is explained below:

Step1: Convert an image I of size $M \times N$ pixels into an array of $P_i = \{p_{1\ldots} p_n\}, 1 \le i \le n$. Here n is the size of image in number of pixels.

Step 2: Produce a chaotic sequence of length n $x_i = \{x_{1\ldots} x_n\}, 1 \le i \le n$ using the equation (1) with initial condition x_0 and taking the parameter μ = 3.99. Next transform x_i into unsigned integer. Sequence lies in the range of 0 to 255.

Step 3: Generate the sequence $C_i = P_i \oplus x_i, 1 \le i \le n$ for confusing the pixel value. The sign $\oplus$ indicates bitwise EX-OR operation. It creates a cipher matrix of order $1 \times N$.

Step 4: Create a position matrix S by generating n number of chaotic sequence $x_i = \{x_{1\ldots} x_n\}, 1 \le i \le n$ using the equation (1) with initial condition x_0'. Then sort the chaotic sequence in increasing order. Matrix S provides the index values for the above generated cipher matrix. Finally turn the cipher matrix

into a jumbled image matrix where position of each pixel is set according to the position matrix *S*.

V. EXPERIMENTS

This section evaluates performance and security of given image encryption scheme. For experiments we have taken gray-scale Lena image 256×256 of size. The experiments have been carried out on a 1.70 GHz Intel Core i3, 4 GB memory. Figure 2(a) and Figure 2(b) shows the original images and corresponding cipher image respectively.

Fig.2 (a) Original images

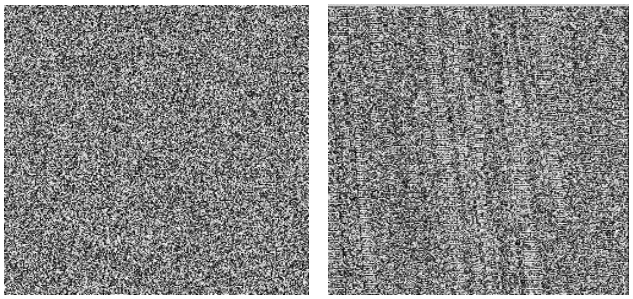

Fig.2 (b) Encrypted images

Experiments results show that effect of encryption process is good, as the logistic map generates the random chotic sequencs. It shows high sensitivity to initial conditions and key. Any change in secret key generates a different encrypted or deciphered image. We have used 32-character (256-bit) key for each logistic map. 256-bit secret key provides a large key space which is sufficient to resist against the brute-force attack. Different tests [20] have been conducted to test the security of scheme which are discussed below.

A. Analysis of Image Histogram

The image histogram is used to represent the distribution of pixels at different gray levels. Histogram of an image plots number of pixels at each gray intensity level. One can take out a great deal of statistical information about image from its histogram. The encrypted image histogram should have an even distribution and it should not be similar to histogram of original image. It is very difficult for an attacker to get any meaningful information from uniform distribution of encrypted image. Figure 3(a) represents the original Lena image histogram and corresponding cipher image histogram. Figure 3(b) represents the original Baboon image histogram and corresponding cipher image histogram. The histogram spikes of the original image are not uniform and they reveal the information about the different gray values of plain images. The histograms of cipher images are representing uniform spikes. It shows that encrypted image does not reveal the statistical similarity structure of the original images to attacker. It becomes extremely difficult to implement any statistical attack on the scheme.

B. Analysis of Correlation Coefficients

In all kinds of images, usually there exists a strong correlation between two adjacent pixels. Any image encryption scheme should generate cipher image with a little correlations between two adjacent pixels. The correlation coefficient factor provides the difference measure between original image and its encrypted variant [19]. This basic dissimilarity factor, correlation coefficient factor, between two images has been calculated by using the following formulas:

$$\zeta_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad \ldots\ldots(4)$$

$$\mathrm{cov}(x, y) = Exp(x - Exp(x))(y - Exp(y)) \quad \ldots\ldots(5)$$

$$Exp(x) = \frac{1}{n}\sum_{i=1}^{n} x_i, D(x) = \frac{1}{n}\sum_{i=1}^{N}[x_i - Exp(x)]^2 \ldots\ldots(6)$$

The gray-scale values of two adjacent pixels in the image are represented by *x* and *y*. *Exp(x)* is the expectation of variable *x* and *D(x)* is a variance of variable *x*. The results of tests are given in the Table 1.

In Table 1, we draw the conclusion that the calculated values for correlation coefficients are very low i.e. near to zero and correlation coefficients of original image are almost close to 1. It indicates that the adjacent pixels in the encrypted image are not correlated.

C. Analysis of Entropy

The entropy is a statistical measure of uncertainty and randomness of information. One can also use this criterion to show the uncertainty present in image. It also expresses the distribution of gray levels in the image. In general entropy of image represents the total number of bits required for encoding the each pixel of the image. The ideal value for image entropy of the cipher image is 8. This measure of randomness and uncertainty of gray-scale values is described by following:

$$E = \sum_{i=0}^{n} p_i \log_2 p_i \ldots\ldots(7)$$

Fig.3 (b) Original image and Cipher image histogram-Baboon

where *n* is the total number of gray levels. Total 256 gray levels are possible for an image. p_i is the probability of occurrence of intensity *i* in the given image. p_i is determined

by dividing the number of pixels with intensity i with the total number of pixels present in the image. The $\log_2$ represents the base-2 logarithm which is used to calculate the image entropy in bits.

The calculation of image entropy is performed for the original 256-gray level image of Lena and corresponding cipher image is produced by the proposed encryption algorithm. Table 2 shows the calculated entropy values for original and encrypted images. Calculated experimental value for cipher image is very close to 8 that mean the encryption algorithm is not vulnerable to information entropy attack.

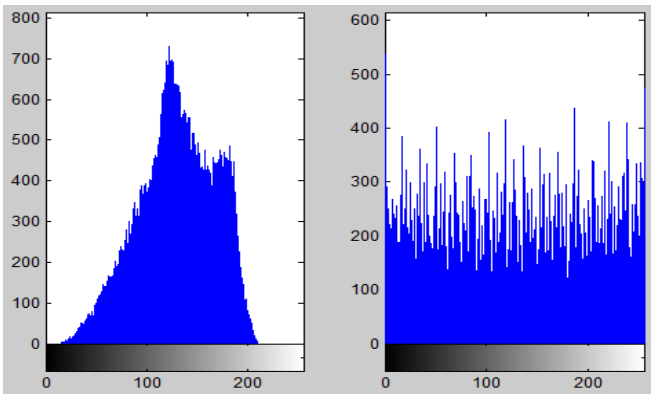

Fig.3 (a) Original image and Cipher image histogram-Lena

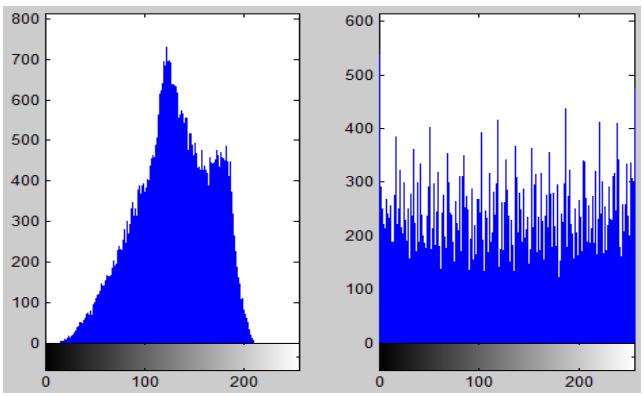

TABLE I. VALUES OF CORRELATION COEFFICIENTS OF ADJACENT PIXELS IN ORIGINAL AND ENCRYPTED IMAGE.

	Original image (Lena)	***Encrypted image (Lena)***	***Original image (Baboon)***	***Encrypted image (Baboon)***
Horizontal	0.9987	0.2687	0.9856	0.2732
Vertical	0.9865	0.2769	0.9959	0.2781
Diagonal	0.9934	0.2793	0.9995	0.2804

TABLE II. RESULTS OF INFORMATION ENTROPY ANALYSIS

Test Image	***Original image***	***Encrypted image***
Lena	7.4429	7.9569
Baboon	7.5334	7.9773

VI. CONCLUSION

This paper presented a simple image encryption scheme. It confuses an image matrix and then shuffles the pixels to generate the final cipher image. Confusing and shuffling are performed with the help of logistic map. Different experiments demonstrate that given scheme for image encryption is strong enough to statistical and other cryptanalytic attacks.

REFERENCES

[1] B. Schneier. "Applied cryptography- protocols, algorithms and source code in C". John Wiley & Sons, New York, 1996.

[2] Menezes , P van Oorschot , S Vanstone . Handbook of applied cryptography. Boca Raton FL: CRC Press, 1997.

[3] W. Stallings, Cryptography and network security: principles and practice. 3rd ed., Prentice-Hall, New Jersey, 2003.

[4] M. S. Baptista, "Cryptography with chaos," Physics Letters A, vol. 240, pp. 50–54, 1998.

[5] R. Matthews, "On the derivation of a chaotic encryption algorithm," Cryptologia, vol.13, pp. 29-42, 1989.

[6] S.Li et al., "Baptista-type chaotic cryptosystems: problems and countermeasures," Physics Letters A, vol. 332, pp. 368-375, 2004.

[7] RC Hilborn, Chaos and nonlinear dynamics: an introduction for scientists and engineers, Oxford University Press, 2001.

[8] OE Rössler, An equation for hyper chaos, Physics Letters A, Vol. 71, pp. 155-157, 1979.

[9] A. Belazi, A. Ahmed, A. El-Latif, S. Belghith, "Novel image encryption scheme based on substitution-permutation network and chaos", Signal Processing, Vol. 128, pp. 155-170, 2016.

[10] W. Liu, K. Sun, C. Zhu, "A fast image encryption algorithm based on chaotic map. Optics and Lasers in Engineering, vol. 84, pp.26-36, 2016.

[11] A. Houas, Z. Mokhtari, K.E. Melkemi, and A. Boussaad, A novel binary image encryption algorithm based on diffuse representation, Engineering Science and Technology, an International Journal, Vol. 19, pp. 1887-1894, 2016.

[12] G. Ye, X. Huang, An image encryption algorithm based on autoblocking and electrocardiography, IEEE MultiMedia, Vol. 23, pp. 64-71, 2016.

[13] M. Al-khassaweneh, S. Aviyente, Image encryption scheme based on using least square approximation techniques. Electro/Information Technology(EIT) 2008. pp. 108-111, 2008.

[14] B. Stoyanov, K. Kordov, Image encryption using Chebyshev map and rotation equation. Entropy, Vol. 17, pp. 2117-2139, 2015.

[15] X. Tong, Y. Liu, M. Zhang, H. Xu, Z. Wang, An image encryption scheme based on hyperchaotic Rabinovich and exponential chaos maps, Entropy, Vol. 17, pp.181-196, 2015.

[16] R.M. May, "Simple mathematical models with very complicated dynamics", Nature, vol. 261, pp. 459–467, 1976.

[17] X. Tong, M. Cui, "Image encryption with compound chaotic sequence cipher shifting dynamically," Image and Vision Computing, vol. 26, pp. 843–850, 2008.

[18] National Institute of Standards and Technology (NIST), Secure Hash Standard (SHS), Federal Information Processing Standards Publication (FIPS PUB)180-2, 2002.

[19] E.B. Corrochano, Y. Mao, G. Chen, "Chaos-based image encryption," Book Chapter:Handbook of geometric computing, Springer, pp. 231-265, 2005.

[20] A.L. Rukhin et al., "A statistical test suite for random and pseudorandom number generators for cryptographic applications", NIST Special Publication 800-22rev.1a, 2010