International Journal of Engineering Science Invention (IJESI)
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 7 Issue 5 Ver. V|| May 2018 || PP 71-75

Image Encryption using chaotic logistic maps with larger key

Dr.O.Srinivasa Rao[1],Ch.Mounika[2]
[1]Associate Professor of CSE, UCEK,JNTUK Kakinada
[2]MTECH(IT) Student, Dept of CSE, UCEK, JNTUK Kakinada

Abstract: Chaos-Based encryption technology has been studied for decades and it has become an important branch of cryptography because of its interesting features such as high security, speed, and dynamic in nature. The encryption phase works using an iterative cipher feedback mechanism combined with secret key and sequence generated by two chaotic logistic maps. After encryption of each pixel of plain-image the secret key is modified this makes the cipher more robust against any attack. The Proposed method enhances the secret key to 208-bit and analysis will be done with the existing one. Security analysis results of proposed and previous ones demonstrate the effectiveness and robustness of the efficient method among them.
Keywords: Chaos cryptography, Logistic maps, Iterative cipher feedback, image encryption, decryption.

Date of Submission: 07-05-2018 Date of acceptance: 22-05-2018

I. Introduction

The information to be transmitted over the computer networks nowadays is not only textual data but also the multimedia data such as audio, image, video and other multimedia types. With this ever-increasing growth of multimedia applications, security is an important aspect in communication and storage of images, and encryption is the way to ensure security. Image encryption techniques try to convert original image to another image that is hard to understand and to keep the image confidential between users. Traditional cryptosystems are not suitable for the encryption of images because, [5] the size of the image data is much larger than that of text data.

The chaos-based encryption has suggested a new and efficient way to deal with the intractable problem of fast and highly secure image encryption [1], which satisfies two properties (i) confusion and (ii) Diffusion, the permutation or confusion is achieved by scrambling all the pixels as a whole using 2D chaotic map(such as Baker map, Arnold cat map etc) and during diffusion the pixel values are modified sequentially and change made to a particular pixel depends on the accumulated effect of all the previous pixel values.

II. Logistic Map

Logistic map has chaotic behavior [2], also they have high sensitivity if there is any change of initial parameters. A. Ismail et al. [3] proposed an image encryption scheme using two chaotic logistic maps and an external secret key of 104-bit.

Mathematically, these 2D logistic maps can be discretely defined as follows [3]

$$x(n+1)=4x(n)[1-x(n)] \quad (1)$$
$$y(n+1)=4y(n)[1-y(n)] \quad (2)$$

The map is dynamic system, since each outcome state x(n+1) depends on previous value x(n) as input. The result of sequence is random and irregular. The initial value for these maps is floating point numbers in (0, 1), which will be calculated using different formulae as [3].

The external secret key for the proposed scheme is of length 208-bit and it is divided into 8-bit blocks.

$K=k_1k_2k_3k_4\ k_5\ldots\ldots\ldots\ldots\ k_{26}$ (in ASCII)

We reduce this key length to k_1 to k_{13} as

$K_1=k_1\oplus k_2$
$K_2=k_3\oplus k_4$
$K_3=k_5\oplus k_6$
.
.
.
.
$K_{13}=k_{25}\oplus k_{26}$

Now the key is of length k_1 to k_{13} and it is used to get the initial value for the two logistic maps by substituting in different mathematical equations as in [3].

Now this key is used to derive a vector of 5 parameters (L,L`,S,S`,C_0) as initial conditions of the system which are used in each pixel encryption. The steps required for proposed scheme is as follows:

1) We divide the key into 3 groups of 4 blocks. From this we get the initial conditions:
   L is a floating point number in (0,1) and S is an integer to be used as seed for the first logistic map.
   First group : k_1 , k_2 , k_3 , k_4 ,
   Second group : k_5 , k_6 , k_7 , k_8 ,
   Third group : k_9 , k_{10} , k_{11} , k_{12}
   For each group we calculate:

$$g_i = \sum_{j=1}^{4} k_j * 10^{-j} \qquad i=1,2,3 \tag{3}$$

$$R = \prod_{i=1}^{3} g_i \bmod 1 \tag{4}$$

   Now the value of L is:

$$L = (R + \frac{k_{13}}{256}) \bmod 1 \tag{5}$$

   And the value of S is:

$$S = \text{round}((\sum_{i=1}^{3} g_i * 10^4 + L * 10^4) \bmod 256) \tag{6}$$

To calculate initial conditions (L`,S`) for second logistic map,

$$v_1 = \sum_{i=1}^{13} k_i \qquad v2 = \oplus_{i=1}^{13} k_i \tag{7}$$

$$V = \frac{V_2}{V_1} \tag{8}$$

   Now the value of L` is:

$$L` = (V + \frac{k_{13}}{256}) \bmod 1 \tag{9}$$

   And the value of S` is:

$$S` = \text{round}((v_1 + v_2 + L` * 10^4) \bmod 256) \tag{10}$$

   And the initial value for the diffusion process c_0 is

$$c_0 = \text{round}((L * L` * 10^4) \bmod 256) \tag{11}$$

2) Use the initial conditions L (for the map x) and L`(for the map y) for two logistic maps in eq(1),(2).
3) The obtained values from previous step should be in the range (0.2, 0.8), then go to step4; otherwise keep step2 in execution, iterating the map, until a desired number in (0.2,0.8) is obtained.
4) The chaotic sequences $\{x_k\}$ and $\{y_k\}$ generated in step2 has to be amplified by a scaling factor (10^4) and round off to integer sequence $\{z_k\}$ as follows:

$$z_k = round((x_k * 10^4) \bmod 256) \tag{12}$$

   The digitized values are designated as Z(n) and Z`(n), respectively.
5) The intermediate values c_1 and c_2 will be calculated as follows:

$$c_1(n) = z(n) \oplus \{[k_1(n) + z(n)] \bmod N\} \oplus \{[c_1(n-1) + k_2(n)] \bmod N\} \tag{13}$$

$$c_2(n) = z`(n) \oplus \{[k_3(n) + z`(n)] \bmod N\} \oplus \{[c_2(n-1) + k_4(n)] \bmod N\}$$

   Where c_1(n-1) and c_2(n-1) are the previously output: $c_1(0) = s$, $c_2(0) = s`$; and N is the color level(for a 256 grey scale image, N=256).
6) Encrypt the pixel as,

$$c(n) = \{[k_5(n) + c_1(n)] \bmod N\} \oplus \{[k_6(n) + c_2(n)] \bmod N\} \oplus \{[k_7(n) + I(n)] \bmod N\} \oplus \{[k_8(n) + c(n-1)] \bmod N\} \tag{14}$$

Where I(n) is the current pixel to be encrypted, c(n-1) is the previously output cipher-pixel, and c(0) be an initial value that is computed according to (11).

7) After encryption of each pixel update the key and the coming logistic maps inputs as follows:

$$x = (x + \frac{c}{256} + \frac{k_9}{256} + \frac{k_{10}}{256}) \bmod 1 \tag{15}$$

$$y = (y + \frac{c}{256} + \frac{k_{11}}{256} + \frac{k_{12}}{256}) \bmod 1$$

And the modified key is

$$k_i = (k_i + k_{13}) \bmod 256, \tag{16}$$

$$k_{13} = k_{13} \oplus k_i, 1 \le i \le 12$$

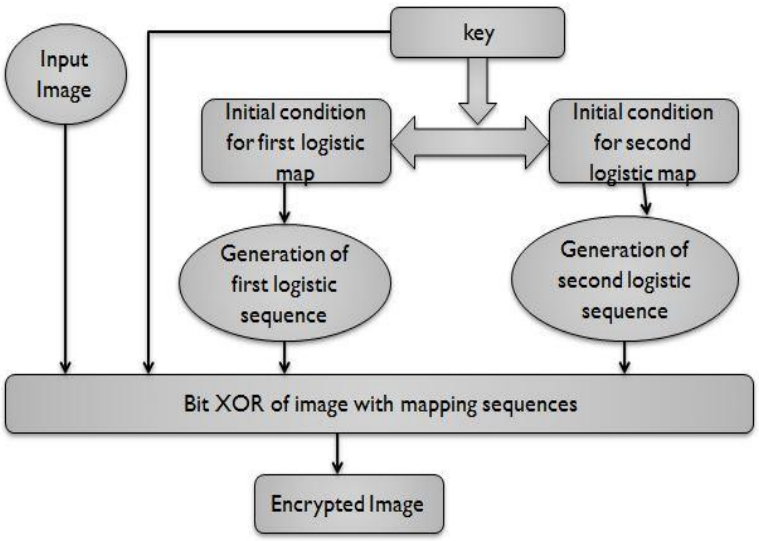
The decryption process is similar to the encryption process the only change is in step6. It can be expressed mathematically as:

$$I(n) = \{\{[k_5(n) + c_1(n)] \bmod N\} \oplus \{[k_6(n) + c_2(n)] \bmod N\} \tag{17}$$

$$\oplus \{[k_8(n) + c(n-1)] \bmod N\} \oplus \{c(n)\} + \{(N - k_7(n))\}\} \bmod N$$

The encryption phase includes iterative stream cipher module based feedback mechanism that is based on chaotic logistic function. Symmetric cryptography is split into block ciphers and stream ciphers, which are easy to distinguish. [4]Stream ciphers encrypt bits individually. This is achieved by adding a bit from a key stream to a plaintext bit. Block ciphers encrypt an entire block of plaintext bits at a time with the same key. This means that encryption of any plaintext bit in a given block depends on every other plaintext bit in the same block.

Iterative cipher feedback mechanism means the encryption of image is done pixel-by-pixel by considering the values of previously encrypted pixels iteratively. This feedback property combined with external secret key and also with sequence generated by chaotic logistic maps. [3]After encryption of each pixel of the plain image the secret key is modified this makes the cipher more robust against any attack.



Fig(1): block diagram of image encryption using two chaotic logistic maps

III. Experimental results:

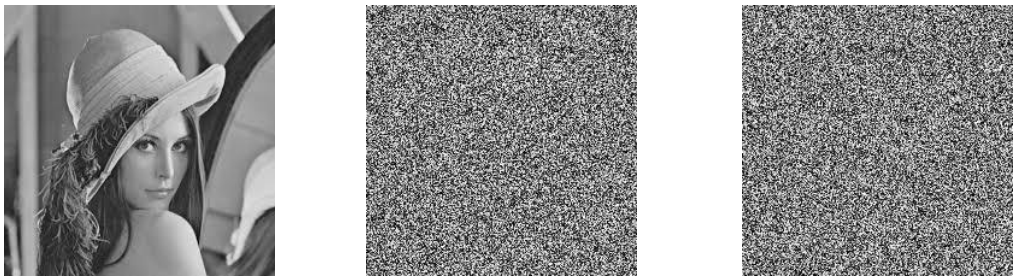
The encrypted image should resist from all kinds of attacks. Chin-Chen Chang et al. [5] defined some kinds of attacks such as cipher image-only attack, known-plain image attack, and chosen-plain image attack. Some of the analysis such as key space analysis and statistical analysis demonstrates security of proposed encryption scheme. Lena image is used for illustration.

1.1 Key space analysis:

When the key space is increased then brute force attacks are infeasible towards the cipher image. The proposed image cipher has $2^{208}(\approx 4.1137*10^{62})$ different combination of secret key.

An ideal image encryption algorithm should be sensitive with respect to the key, i.e., whenever there is a slight change in single bit of key then it should produce a completely different encrypted image.

For example, an original image of Lena is encrypted using the secret key "abcdefghijklmnopqrstuvwxyz" gives us the encrypted image **A**. And the same original image is encrypted by making the slight modification in the key i.e., "abcdefghijklmnopqrstuvwxyy" gives us the encrypted image **B.**

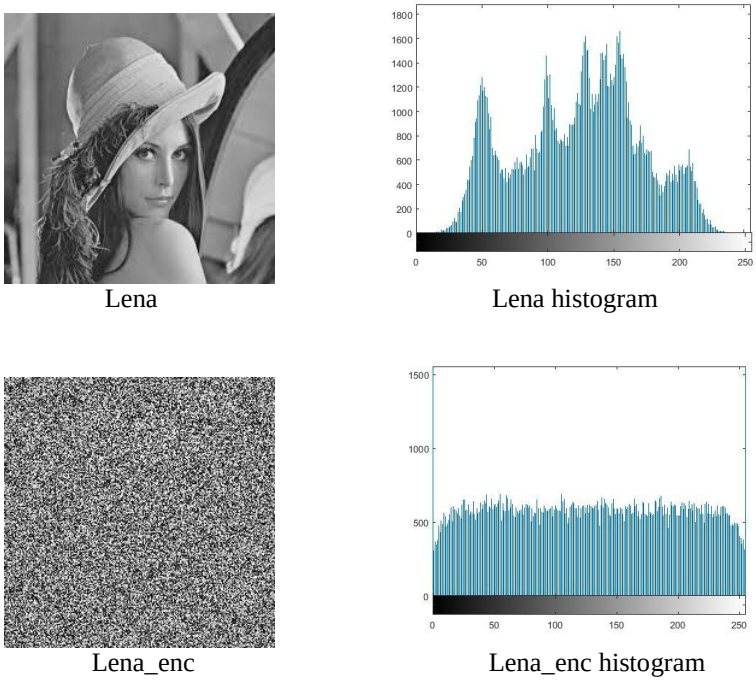


Lena **A** **B**

Fig(2): Key sensitivity test by encrypting source image by slightly different keys.

1.2 Histogram Analysis:

A frequency distribution shows how often each different value in a set of data occurs. A **histogram** is the most commonly used graph to show frequency distributions .The histogram of ciphered images is fairly uniform and is significantly different from that of the original image.



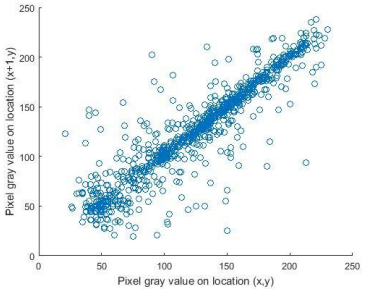
Lena Lena histogram

Lena_enc Lena_enc histogram

1.3 Correlation Analysis:

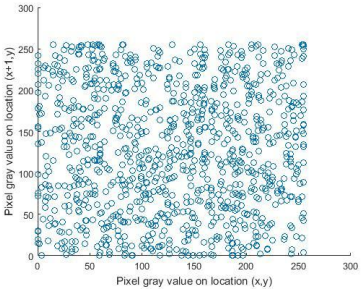
Correlation analysis gives shows us how strongly the pixels are related to each other within the image and also with other images. [6] Higher the correlation coefficient indicates the high similarities and lower the correlation indicates low similarities between the images. Original image should have low correlation coefficient with the encrypted image. Referring [7] correlation coefficient will be calculated between the Lena original image and encrypted image. Correlation distribution of two horizontally adjacent pixels in plain image and encrypted image is shown below.

Correlation coefficient 0.9160



Correlation in Lena

correlation coefficient -0.0233



correlation in lena_enc

And the correlation between Lena original image and its encrypted image is -0.0054.

1.4 Time Analysis:

[2] Along with the security the running speed is also an important aspect for an ideal encryption algorithm. A longer key would require more computational time for encryption/decryption which may not be preferable for real time transmission. The following table shows the rate at which the Lena grayscale image of different sizes are encrypted with the proposed scheme. The time analysis has been done on Intel core i3 processor with 4GB RAM. The average encryption time taken by the proposed algorithm for the different sized images is shown below:

Image size in pixels	104-bit	208-bit
256×256	0.88s	1.20s
512×512	1.90s	2.20s
1024×1024	4.20s	5.70s

Table1: Average ciphering speed of a few different sized colored images

IV. Conclusion:

In this paper, Logistic chaotic maps are efficiently worked to confuse the relationship between the plain image and the cipher image. The proposed image encryption scheme successfully deals the secure image encryption using 204-bit secret key and two logistic maps. It also proves the fact that as long as the length of the key increases, it consumes more computational time for encryption/decryption which is not preferable for real time transmission.

References:

[1]. A New Chaotic Algorithm for Image Encryption,Xin Zhang[a], Weibin Chen[b]
[2]. Image encryption using chaotic logistic map,N.K. Pareek, Vinod Patidar , K.K. Sud , Image and Vision Computing 24 (2006) 926–934
[3]. A Digital Image Encryption Algorithm Based A Composition Of Two Chaotic Logistic Maps,I. A. Ismail, Mohammed Amin, Hossam Diab
[4]. An Efficient Chaos-Based Feedback Stream Cipher (ECBFSC) for Image Encryption and Decryption,Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S. Farag Allah
[5]. C.C. Chang, M.S. Hwang, T.S. Chen, A new encryption algorithm for image cryptosystems, J. Syst. Software 58 (2001) 83–91.
[6]. A Novel Partial Image Encryption using Chaotic Logistic Map, Nitumoni Hazarika, Monjul Saikia
[7]. G. Chen, Y. Mao, C.K. Chui, A symmetric image encryption based on 3D chaotic maps, Chaos Solitons Fractals 21 (2004) 749–761.
[8]. Multi Chaotic Systems Based Pixel Shuffle for Image Encryption, H. H. Niena & C. K. Huangb
[9]. Image Encryption using the Two-dimensional Logistic Chaotic Map,Yue Wua, Gelan Yangb_, Huixia Jinb and Joseph P. Noonana
[10]. M. S. Baptista, Cryptography with chaos, Phys. Lett. A, vol.240, pp.50-54,1998.
[11]. Fridrich Jiri, Symmetric ciphers based on two dimensional chaotic maps, Int. J. Bifurcat Chaos 8 (6) (1998) 1259–1284.
[12]. J.C. Yen, J.I. Guo, A new chaotic key based design for image encryption and decryption, Proceedings of the IEEE International Symposium Circuits and Systems, vol. 4, 2000, pp. 49–52

Dr.O.Srinivasa Rao "Image Encryption using chaotic logistic maps with larger key "International Journal of Engineering Science Invention (IJESI), vol. 07, no. 05, 2018, pp 71-75