International Journal of Computer Applications Technology and Research
Volume 4– Issue 2, 165 - 169, 2015, ISSN:- 2319–8656

New Technique for Image Encryption Based on Choas and Change of MSB

Fariba Ghorbany beram
Sama Technical and Vocational Training College
Islamic Azad University
Shoushtar Branch, Shoushtar
Iran

Mojtaba khayt
Sama Technical and Vocational Training College
Islamic Azad University
Shoushtar Branch, Shoushtar
Iran

Sajjad Ghorbany Beram
Sama Technical and Vocational Training College
Islamic Azad University
Shoushtar Branch, Shoushtar
Iran

Abstract:

In this paper, an algorithm for image encryption using chaotic systems and techniques to change the pixel values are proposed for protecting digital images in an efficient and safe manner will be offered. In the proposed algorithm, the stochastic properties of chaotic Logistic system is used. To evaluate the performance of the proposed algorithm, we have implemented it in MATLAB using parameters such as visual analysis, key space analysis, histogram analysis. Implementation results show that the proposed algorithm, the algorithm is efficient and safe.

1. INTRODUCTION

Cryptography is the science of code and secrets. It is an ancient art and it has been used for several centuries amang commeders, informers and others to protect the message amang them and to keep the messages privately. When we are dealing with the data safety, we need the identity sender and receiver of the message and also we should make sure about the content of message has not been manipulated. These three subjects, in other words, confidentiality, confirming the identity and generality are at the center of safety of modern data communication and can make use of cryptography. As a whole, this issue should be guaranteed that a message can only be decoded(read) by means of the people to whom the message has been sent and others are not allowed to read them. The method wich provides this issue is called cryptography[1,2,3].

2.CHAOS

Chaos is a phenomenon wich takes place in the definable nonlinear systems that have a lot of sensitivity against the primary conditions and their uasi randomized behavior suchlike systems satisfy the liapanof appearance they will be in a stable condition in the peak of chaos. The out put of this system is always under the effect of primary amounts of input. On the other hand prediction of this kind of signal is almost impossible with having the primary amounts and the physical appearance(shape) of this signal is similar to noise. The chaos environs have the following specifications:high sensitivity in relation to the primary conditions, exactness and lack of statistical prediction[4,5,6].

Formula1

$$X_{n+1}=r.xn(1-x_n)$$

x_n is the state variable being in the interval [0, 1] and r is system parameter which might have any value between 1 and 4. In this paper we have used the logistic function to generate the secret key.

3. THE PROPOSED METHOD

In this study an algoritm is presented which changes the order of pixels in the input image in a way that there will be very difference between the input and output image. At first we divide the input image into three sub-bands, namely red, green, blue to satisfy our expectation, and the current place of pixels is randomly changed into a place which is determined by means of fourmalu2,3. In order to change the mounts of the pixels which are fixed in new places with ane of the lines of table1 which is randomly assigned by fourmala4. table 1 includes 16 lines that each line with 4 valuable bits is xor with the pixels amounts.

Fourmalu2

$$X_{n+1}=(r.xn(1-x_n))*a \quad 1<a<\text{number of rows}$$

Fourmalu3

$$X_{n+1}=(r.xn(1-x_n))*b \quad 1<b<\text{number of columns}$$

fourmalu14

$$X_{n+1}=(r.xn(1-x_n))*c \qquad 1<c<16$$

a, b are selected so that the Chaos integer between 1 to Number of rows and 1 columns are generated, and c are determined by a number between one and sixteen production so that each execution of the scalar random selection row of table 1 is selected.

For example, if the pixel value 150 is a binary value of 10010110 is then based on the value of the Formula 4 comes a row of Table 1 is selected and a four digit value of number(10010110), XOR, and the new value replaces the pixel values of previous that is, if the number 14 is derived from the logistic map, 4MSB(most sign bit of number) with the number 150 (1001) with row 1 of table (1110), XOR is and result is 118(Figure1,2).

Table1

ROWES	XOR
0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001
10	1010
11	1011
12	1100
13	1101
14	1110
15	1111

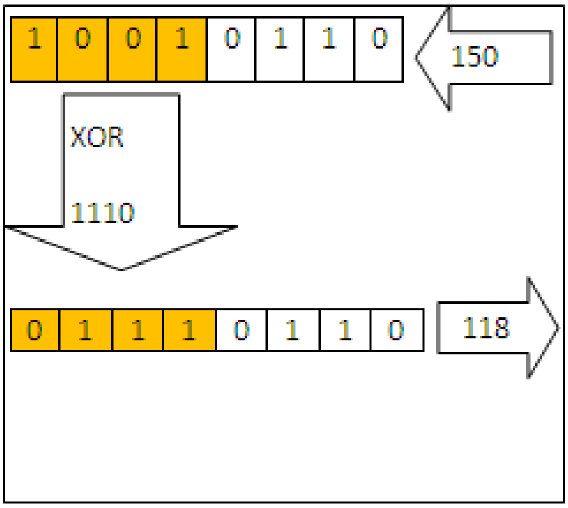

Figure1-change MSb of pixel with the selected rows

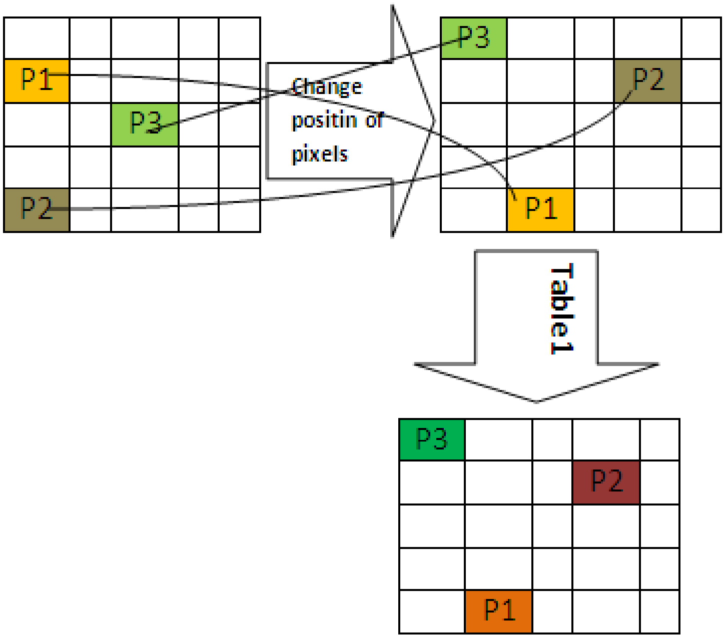

Figure 2-Flowchart of the data encryption process

The image is composed of pixels, the pixel values are in hiding and encryption technique for digital images. Change in the least significant bit[7,8,9] of a pixel, which is technically referred to as steganogeraphy[10,11,12](Figure 3).

As shown in Figure 4, we change a bit in the pixel values of images will not cause a visual change .in this paper we have used the change in the msb. As we see in Figure 5, this change is very real.
We also intend to change the values of the pixels in such a way that the basic shape vary.

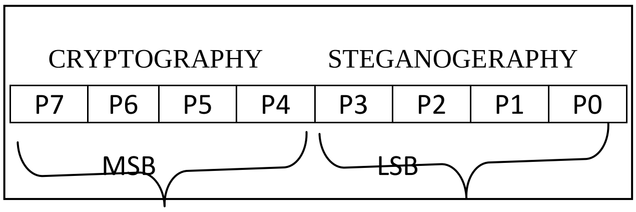

Figure 3

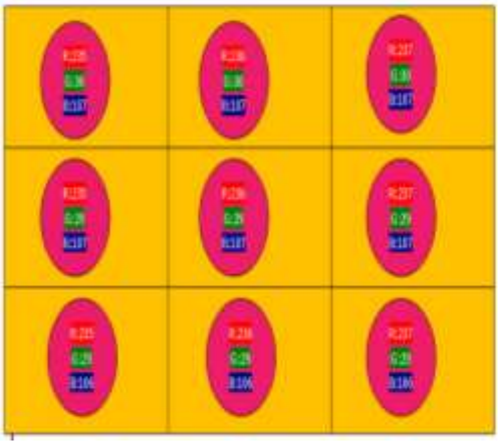

Figure4.change of LSB bits of pixel

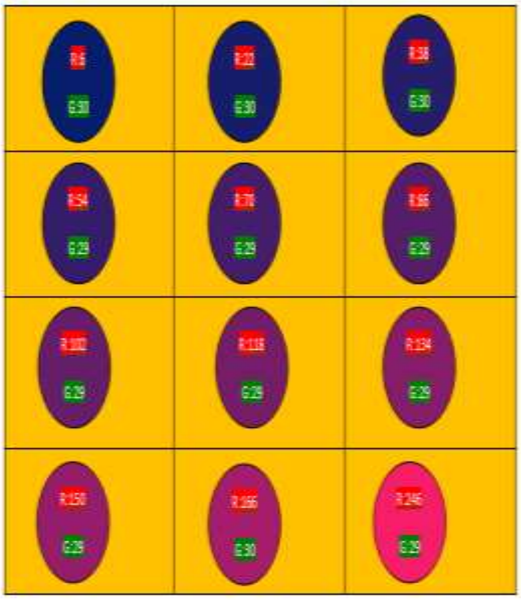

Figure5.change of MSB bits of pixel

A. Encryption algorithm

1) The original image into three sub-bands of red, green and blue break

2) change position of pixel(row and column) based on the logistic map.

3) Changing the pixel values given in Table 1.

4. IMPLEMENTATION

A method of good cryptography must be resistant against difference kinds of code-detection and statistical attacks. In the continuation the suggested algoritm will be analysis, the analysis of sensitivity of this method in relation to key changing, the analysis of The key space and **histogram**.

A. THE HISTOGRAM CHART

it is a kind of method of examining the encoded image of observation, a good cryptography algoritm should arrange the image in such a way that its specifications not to be specifiable. Also, no kind of information in the encoded image by comparing the encoded image with the main image should be observed. The main image and the encoded image should be seprate visually. The analysis of histogram expresses that pixels are distributed. In the images by means of drawing the observations numbers of the light severity. However we con not find the major image by prossessing the chart. In cryptography the greater difference between the main image histogram and encoded image will cause the safer algoritm. As it come be clearly seen in Figure6, Figure7, Figure8 and Figure 9 , that the histogram of cryptography image is totally different from the main image histogram. This problem increases th risk of possibility of statistical attacks. The analysis of random of randomization:an algoritm should have certain suitable probable features such as good distribution, high complexity and efficiency in order to have more security.

Figure 6-original image

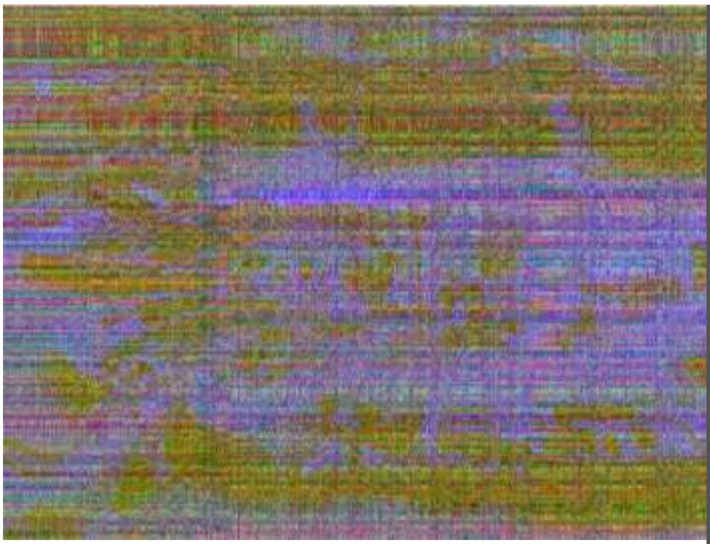

Figure7-encrypted image

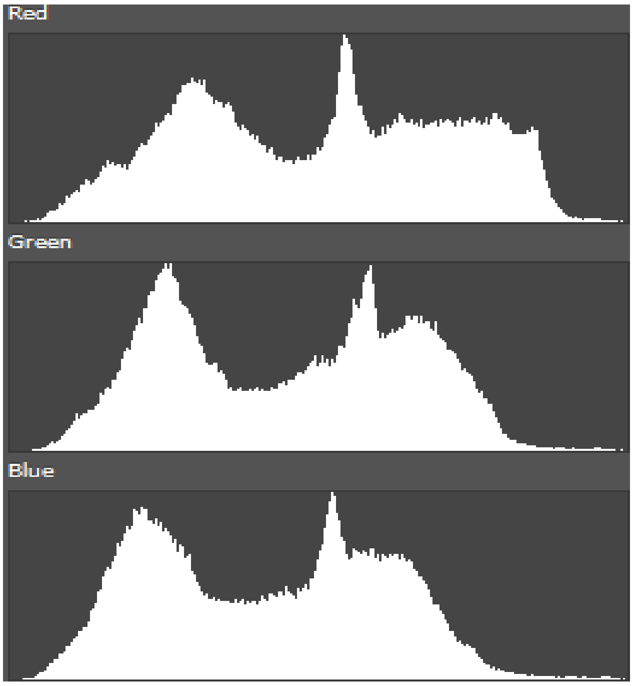

Figure8- histogram of original image

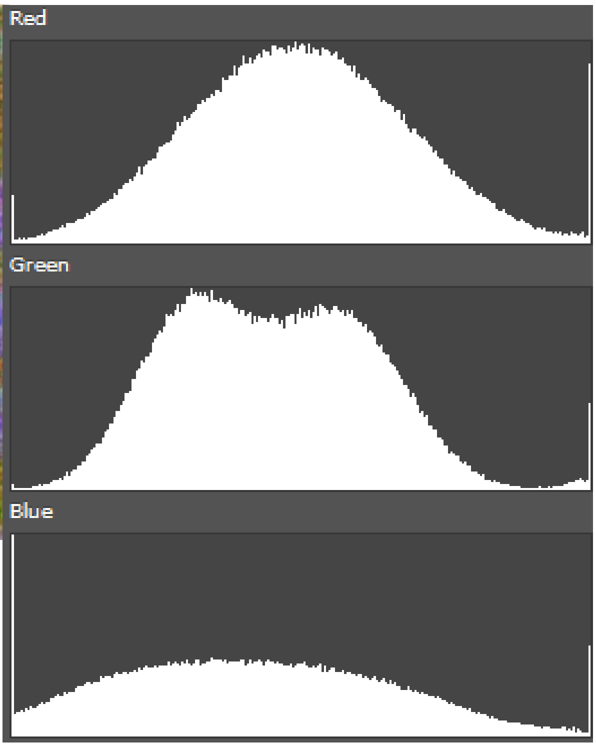

Figure9- histogram **of** encrypted image

B. THERE ARE VARIOUS WAYS IN ORDER TO CREATE RANDOM NUMBERS

Today, researchers have paied special attention to chaos systems. We applied logestic chaos system to make random number in this paper. Fourm1 shows one of most famous signals which has chaos behavior and it is called logestic map. While r[3.57 4] the behavior of system is generally like a chaos.

As a whole one ideal feature for an encrypted image is its sensitivity in relation with the partial changes in the main image, in other words changing one pixel. The invader tries to create some partial changes in the input images to observe the result changes in the secret image. By usig this method the meaningful relation between the main image and the encrypted image will be obvious. This activity itself made the key to be diagnosed and to be known in more simple way. one of the feauures of evaluating the cryptography algoritms is the analysis of sensitivity to the key[9]. Namely, making changes in the key should create a totally different encrypted image.to do this, it is enough to change the amounts of x,y,r in the suggested algoritm, as a result, regarding the feature of chaos environs which are related to the primary elements, the produced amounts change and the result of it is creating different encrypted images(Figure10,11).

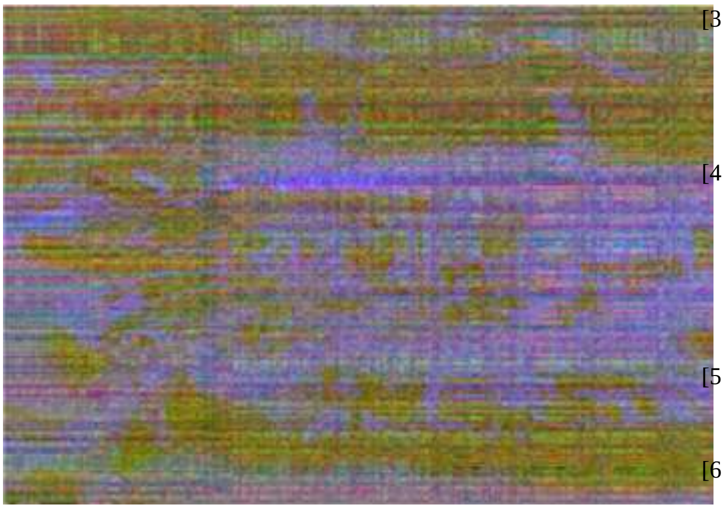

Figure10.image encrypted based on initial x_1,y_1,r_1

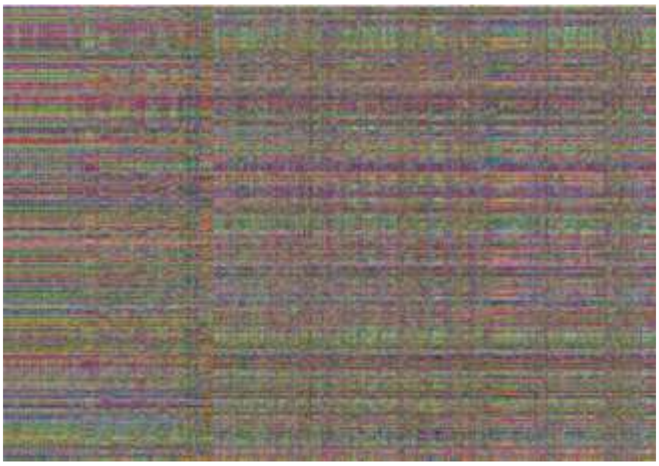

Figure11.image encrypted based on initial x_2,y_2,r_2

5. CONCLUSION

An algoritm for cryptography of image was introduced in this article. The suggested algoritm was evaluated by means of some exams to assess the efficacy of the algoritm. The result of visual tests and the analysis of histogram showed that there is not any obvious fiber in the encrypted images by suggested algoritm and there is no similarity between the main image and the encrypted image from the viewpoint of statistics. The result of the analysis of sensitivity to the key showed that the suggested algoritm is very sensitive regarding switching the key.

6. REFERENCES

[1] Shiguo Lian_, JinshengSun, Zhiquan Wang, "Security analysis ofa chaos-based image encryption algorithm", Elsevier, Physica A, Vol. 351, pp. 645–661,2005.

[2] B. Schneier, "Applied Cryptography Second Edition : protocols, algorithms, and source code in C", ISBN 9971-51-348-X, John Wiley & Sons,1996.

[3] Fethi Belkhouche, Uvais Qidwai, Ibrahim Gokcen, Dale Joachim, "Binary Image Transformation Using Two-Dimensional Chaotic Maps", IEEE, Proceedings of the 17th International Conference on Pattern Recognition (ICPR), 2004.

[4] Grummt, E., Ackermann, R.: Proof of Possession: Using RFID for large-scale Authorization Management. In: Mhlhuser, M., Ferscha, A., Aitenbichler, E. (eds.) Constructing Ambient Intelligence, AmI-07 Workshops Proceedings. Communications in Computer and Information Science, pp. 174, 182 (2008)

[5] Pecorra, L.M., Carroll, T. L.,"Synchronization in chaotic systems", Phys. Rev. Lett., Vol. 64, No. 8, pp. 821–824, 1990.

[6] Pareek, N.K., Patidar, V., Sud, K.K., "A Random Bit Generator Using Chaotic Maps", International Journal of Network Security, Vol. 10, No. 1, pp. 32-38, 2010.

[7] Mohammad Ahmad Alia, A.A.Y., Public–Key Steganography Based on Matching Method, in European Journal of Scientific Research.2010.p.209

[8] D. Bret, A detailed look at Steganographic Techniques,US:SANS institute, 2002.

[9] Belkacem, S. Dibi, Z. Bouridane, "Color Image Watermarking based on Chaotic Map", 14th IEEE International Conference of Electronics, Circuits and Systems, 2007.

[10] Masoud Nosrati , Ronak Karimi," A Survey on Usage of Genetic Algorithmsin Recent Steganography Researches", World Applied Programming, Vol (2), No (3), March 2012. 206-210,ISSN: 2222-2510,©2011 WAP journal. www.waprogramming.com

[11] Indradip Banerjee, Souvik Bhattacharyya, Gautam Sanyal," A Procedure of Text Steganography Using Indian Regional Language", J. Computer Network and Information Security, 2012, 8, 65-73 Published Online August 2012 in MECS (http://www.mecs-press.org/)

[12] Seyyed Amin Seyyedi, Rauf.Kh Sadykhov," Digital Image Steganography Concept and Evaluation", International Journal of Computer Applications (0975 – 8887) Volume 66– No.5, March 2013