Australian Journal of Basic and Applied Sciences, 5(8): 587-593, 2011
ISSN 1991-8178

Image Encryption using Cellular Automata and Arnold Cat's map

[1]Hasan Asadollahi, [2]Morteza Saberi Kamarposhti, [3]Ehsan Moosavian Jandaghi

[1,2]Department of Computer Science, Islamic Azad University, Firoozkooh Branch, Firoozkooh, Iran.
[3]Department of Computer Science, Islamic Azad University, Mashhad Branch, Mashhad, Iran.

Abstract: Nowadays, using Internet application and number of computer networks users are too numerous. And so many different digital images can be accessed on the Internet easily. As result, protection of data is very important. Image encryption has been important tools to prevent unauthorized data access. In this paper a new encryption method has been proposed based on cellular automata and CAT's map for encrypting digital image. The results show the value of the entropy is 7.9926. Consequently, by comparison with other methods, the mentioned method has a high security to avoiding attacks.

Key words: Image Encryption; CAT's map; Cellular Automata; Cryptography

INTRODUCTION

One of the advantages of using the Internet is accessing and processing to the different Images easily. Image encryption is necessary for avoiding unauthorized access to the data. Image encryption is one of the essential and important topics for the researcher and many methods have been done with them. In (Kuo-Liang Chung, Lung-Chun Chang, 1998) a new method has been proposed for encrypting binary Images. In (Chin-chen Chang *et al*., 2001) a new method has been proposed for encrypting Images with vector quantization methods. Quantization method is one of the common methods to encrypting images. Also digital signature has used for encrypting images in (Aloka Sinha, Kehar Singh *et al*., 2003) that the digital signature of pain-image has been added in to cipher-image. The 3D chaotic cat maps uses for symmetric image encryption (Guanrong Chen *et al.*, 2004). Recently, some of proposed algorithms are based on fractional wavelet transform and fractional Fourier transform (Karl Martin, *et al*., 2005; Linfei Chen, Daomu Zhao, 2005; Xiaogang Wang, Daomu Zhao, 2006; Xiaogang Wang, *et al*., 2006).

In (Tiegang Gao, Zengqiang Chen, 2008) a new total shuffling algorithm has been proposed for encrypting image that in this method the gray level has change too. In (Tiegang Gao, Zengqiang Chen, 2008; Yang *et al*., 2009) cryptosystems are based on chaotic map and operations algebraic that the results show chaotic maps usually guarantee security on data.

In this paper a new encryption method has been proposed by using cellular automata and CAT's map for encrypting digital image. The results show the proposed method has a high security to avoiding attacks.

In this paper at first, special properties of chaotic systems have been discussed then CAT's map has been defined. After that a proposed method will be described. Finally, some simulation outcomes to security analysis are given.

Special Properties of Chaotic Systems:

A chaotic system is totally nonlinear with pseudorandom behavior by definite range of values for the system parameters. Also responses or trajectories of system remain bounded in phase space. Such unstable state strongly depends of parameters value and path of initial conditions. The properties of dynamic chaotic have been described as follow:

Sensitivity to initial conditions:

Next states are predictable if initial conditions have accepted in a final system. Although long term prediction for chaotic systems is impossible but for special parameters values, two trajectories that are very close in initial time, have been diverged exponentially. As a result the initial information about the systems will be lost totally. Figure 1 shows the mentioned description.

Certainty:

Although chaotic functions are pseudorandom behaviors, they are completely certain. It means using correct calculation and accurate parameters have been generated similar chaotic series.

Corresponding Author: Hasan Asadollahi, Department of Computer Science, Islamic Azad University, Firoozkooh Branch, Firoozkooh, Iran.

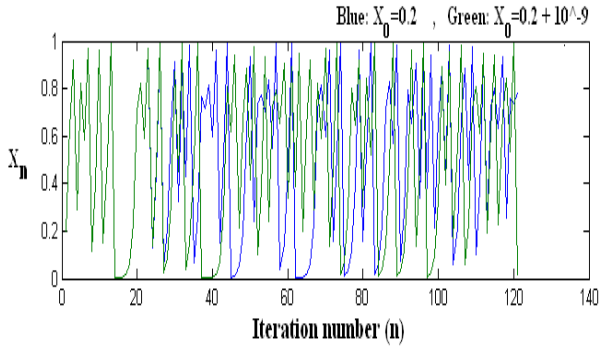


Fig. 1: Great sensitivity to little initial condition changing in chaotic series.

Statistically Non-Predictable:

Because the chaotic series have pseudorandom behaviors, generated series or numbers have not related way to each other with any statistical methods. It means, for the cryptosystems, any different statistical methods cannot reduce number of numerous chaotic sequence keys seriously and immediately.

Ergodic property:

A trajectory in phase space has Ergodic property if it closes to its initial condition completely. Trajectory of chaotic system can supply the mentioned properties. The inherent property shows that the system will be bounded to the goal in space. The goal is a set of points that has named absorber. The density of points is not changeable in during time and the mentioned property is very necessary to encryption.

Mixing:

Mixing is one of systems properties that a small interrupt in initial condition propagate in total phase space at changing asymptotes time. An interrupt, in a chaotic system, has propagated in part of phase space in initial condition that it has limited the trajectory by the asymptotes as result, each area has generated from other area of phase space.

Arnold CAT's map:

In this section, Arnold Cat has been described. The map defines as follow:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = A \begin{bmatrix} x_n \\ y_n \end{bmatrix} \pmod N = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \pmod N$$

Where p and *q* are positive integer and *det(A)=1*

The proposed method:

In the proposed method has used two stages to image encryption. In first stage, the position of image pixels has shuffled based on CAT's map. In second stage, generated map has used for changing the gray level of pixels separately. In the proposed method, a 120 bits key has used for encrypting image.

$$Key = K_{119}K_{118}.....K_1K_0$$

At first, the key has divided into even and odd parts.

$$KeyOdd = K_{119}K_{117}.....K_3K_1$$

$$= KO_{59}KO_{58}.....KO_1KO_0$$

$$KeyEven = K_{118}K_{116}.....K_2K_0$$

$$= KE_{59}KE_{58}.....KE_1KE_0$$

Then values x_0 and y_0 have obtained for initial condition based on CAT's map as follow:

$$x_0 = \frac{\left[KE_{59} \times 2^{59} + KE_{58} \times 2^{58} + ... + KE_0 \times 2^0\right]}{2^{60}}$$

$$y_0 = \frac{\left[KO_{59} \times 2^{59} + KO_{58} \times 2^{58} + ... + KO_0 \times 2^0\right]}{2^{60}}$$

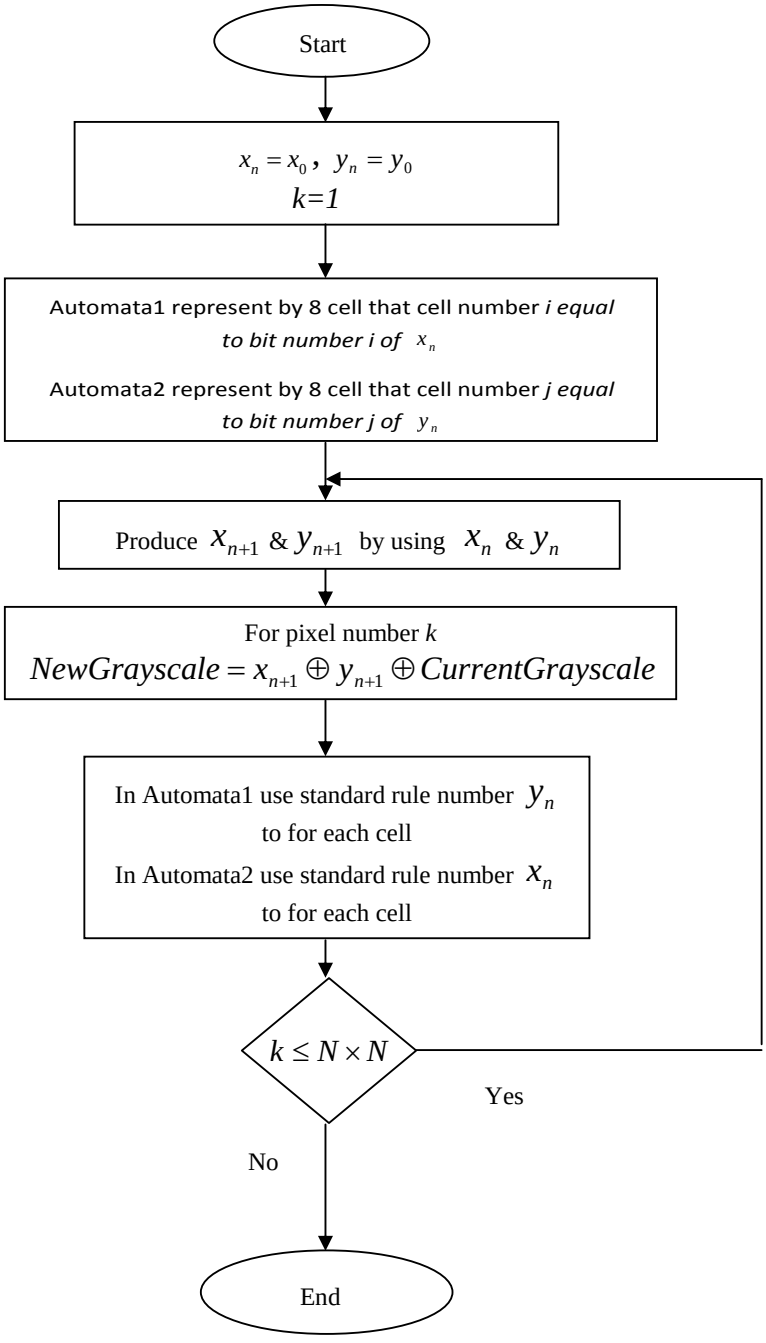


Fig. 2: The proposed algorithm for changing gray level in the image.

For encrypting an image by dimensions $N \times N$, two matrixes will be generated as follow:

$$X = \left[x_N x_{N-1} .....x_1\right]$$

$$Y = [y_N\, y_{N-1} \ldots\ldots\ldots\ldots\ldots y_1]$$

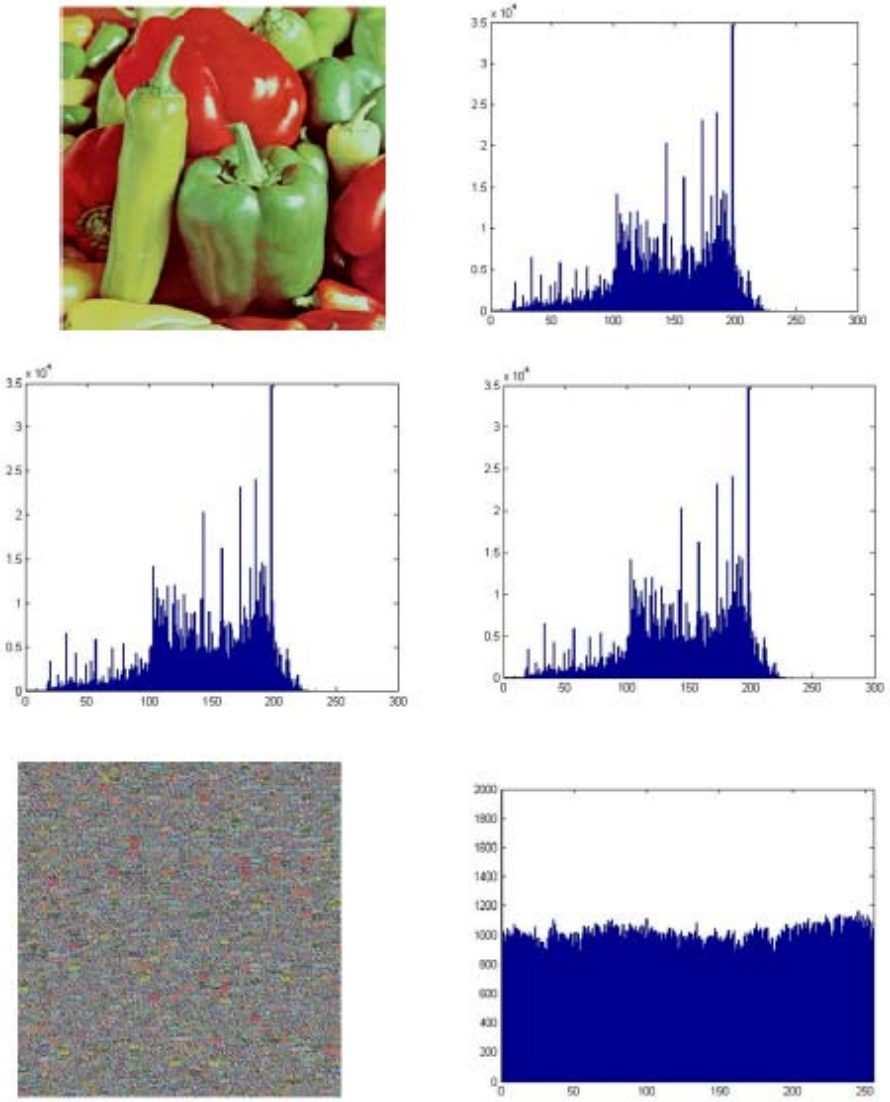
A Look Up Table matrix will be generated By using two generated matrixes as follow:

$$LUT = \begin{bmatrix} X_0, Y_0 & X_0, Y_1 & & X_0, Y_N \\ X_1, Y_0 & \cdots & \cdots & X_1, Y_N \\ \vdots & & & \\ X_N, Y_0 & \cdots & \cdots & X_N, Y_N \end{bmatrix}$$

For shuffling, corresponding points in the image have shuffle by corresponding points in LUT matrix. Figure 2 shows the changing gray level algorithm in the image.

Experimental results:

At first, the proposed method has been tested on pepper image that the pepper image is the most famous image to testing in image processing. The results and histogram of the pain-images and cipher-images have been illustrated in figure 3. The histogram of cipher-image is near flat that it shows the proposed method has a good efficiency.



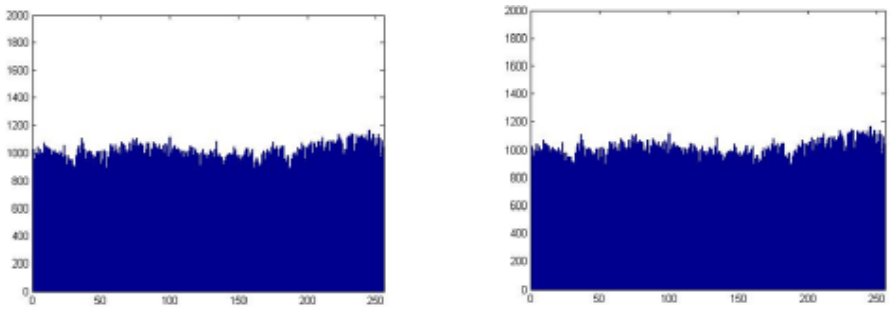


Fig. 3: Histogram of the plain images and ciphers images.

Information entropy:

Information entropy is a mathematical theory for storing and making relation between data. It presented in year 1949 with Claude E Shannon. One of the most famous equations about information entropy is as follow:

$$H(S)=\sum_{i=0}^{2N-1}P(s_i)\log\left(\frac{1}{P(s_i)}\right)$$

Where N is number of gray level in image (in 8 bits image equal 256) and $P(s_i)$ is a event probability of gray level i_{th}. The value of probability will be 8 if the images have been made random completely. The mentioned value is ideal value. Whatever the obtained value be more near to 8, it means the method is less predictable. As result, the method is a more secure. In the proposed algorithm, the value of obtained result is 7.9926. It is very near the ideal value. The result shows, the proposed method is a good method to avoiding attacks.

To stability testing of the proposed method, we have used 4 images that can be seen in figure 4 and the results of test have shown in figure 5.

Fig. 4: Selected image for stability testing.

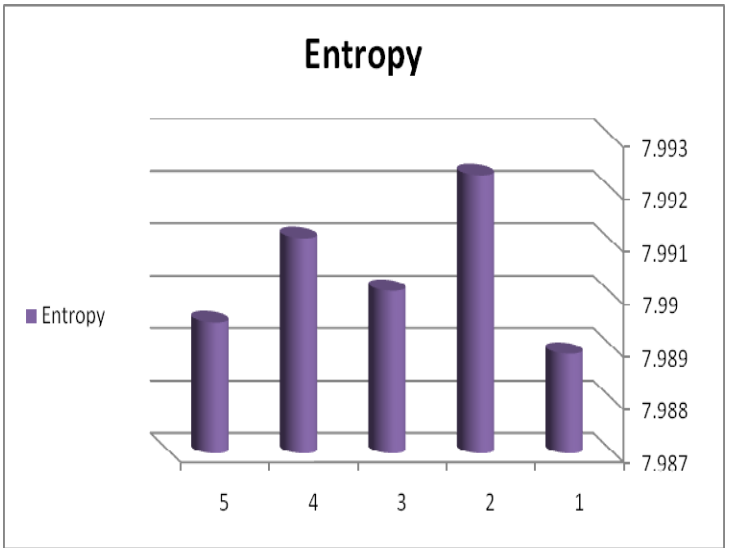


Fig. 5: The obtained entropy by testing on images in figure 4

Correlation coefficient:

In this section, the horizontal, vertical and diametric coefficients have been examined between pixels of the images. For this purpose, 2048 pairs of adjacent pixels have been selected randomly. They should be selected horizontally, vertically and diametrically. By using the follow equation, the correlation coefficient for each pair of pixel has been calculated.

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x_i))^2$$

$$\mathrm{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x_i))(y_i - E(y_i))$$

$$r_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

The results have shown in figures 6 and 7.

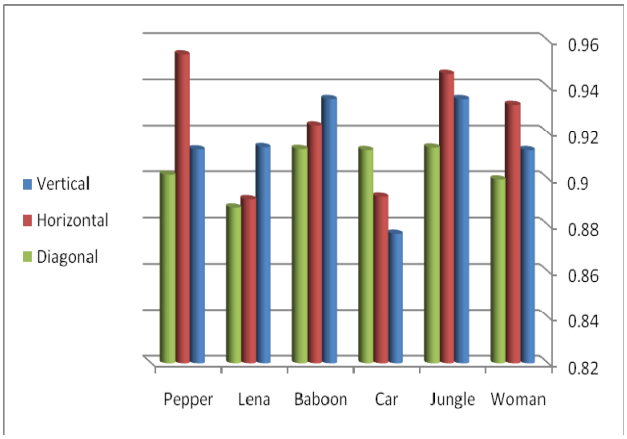


Fig. 6: Values of horizontal, vertical and diametric correlation coefficients for the six selected image.

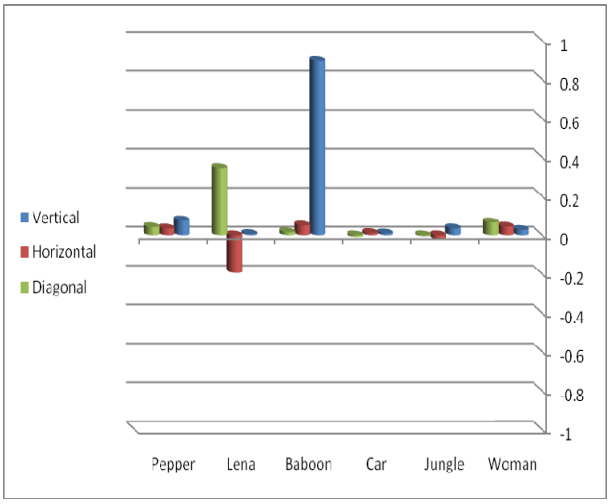


Fig. 7: Values of horizontal, vertical and diametric correlation coefficients for the six ciphers-images.

Conclusion:

In this paper a new image encryption method has been proposed based on cellular automata and Arnold CAT's map. As can be seen, experimental results show that the proposed method has a high security against several attacks.

ACKNOWLEDGMENT

This Research was supported by Islamic Azad University, Firoozkuh Branch.

REFERENCES

Aloka Sinha, Kehar Singh, 2003. A technique for image encryption using digital signature, Optics Communications, 218: 229-234.

Chin-chen Chang, Min-Shian Hwang, Tung-Shou Chen, 2001. "A new encryption algorithm for image cryptosystems", The Journal of System and Software, 58: 83-91

Fuyan Sun, Zongwang Lü, Shutang Liu, 2010. "A new cryptosystem based on spatial chaotic system", Optics Communications, 283: 2066-2073.

Guanrong Chen, Yaobin Mao, Charles K. Chui, 2004. "A symmetric image encryption scheme based on 3D chaotic cat maps", Chaos, Solitons and Fractals, 21: 749-761.

Huaqian Yang, Xiaofeng Liao, Kwok-wo Wong, Wei Zhang, Pengcheng Wei, 2009. "A new cryptosystem based on chaotic map and operations algebraic", Chaos, Solitons and Fractals, 40: 2520-2531.

Karl Martin, Rastislav Lukac, Konstantinos N. Plataniotis, 2005. "EfWcient encryption of wavelet-based coded color images", Pattern Recognition, 38: 1111-1115.

Kuo-Liang Chung, Lung-Chun Chang, 1998. "Large encrypting binary images with higher security", Pattern Recognition Letters, 19: 461–468.

Linfei Chen, Daomu Zhao, 2005. "Optical image encryption based on fractional wavelet transform", Optics Communications, 254: 361-367.

Reza Entezari-Maleki, Seyyed Mehdi Iranmanesh and Behrouz Minaei-Bidgoli, 2009. An Experimental Investigation of the Effect of Discrete Attributes on the Precision of classification Methods, World Applied Sciences Journal, Volume 7 (Special Issue for Computer & IT).

Seyed Amin Hosseini Seno, Rahmat Budiarto and Tat-Chee Wan, 2009. SHSDAP: Secure Hierarchical Service Discovery and Advertisement Protocol in Cluster Based Mobile Ad hoc Network, World Applied Sciences Journal, Volume 7 (Special Issue for Computer & IT).

Tiegang Gao, Zengqiang Chen, 2008. "Image encryption based on a new total shuffling algorithm", Chaos, Solitons and Fractals, 38: 213-220.

Xiaogang Wang, Daomu Zhao, 2006. "Image encryption based on anamorphic fractional Fourier transform and three-step phase-shifting interferometry", Optics Communications, 268: 240-244.

Xiaogang Wang, Daomu Zhao, Linfei Chen, 2006. "Image encryption based on extended fractional Fourier transform and digital holography technique", Optics Communications, 260: 449-453.

Zhi-Hong Guan, Fangjun Huang, Wenjie Guan, 2005. "Chaos-based image encryption algorithm", Physics Letters A 346: 153-157.