International Journal of Physical Sciences Vol. 6(12), pp. 2921-2926, 18 June, 2011
Available online at http://www.academicjournals.org/IJPS
DOI: 10.5897/IJPS11.197
ISSN 1992 - 1950 ©2011 Academic Journals

Full Length Research Paper

A new method for image encryption via standard rules OF CA and logistic map function

Soheil Fateri[1] and Rasul Enayatifar[2]

[1]Islamic Azad University, Babol Branch, Babol, Iran.
[2]Islamic Azad University, Firuzkooh Branch, Firuzkooh, Iran.

Accepted 25 February, 2011

In this paper a hybrid model of cellular automata and chaotic signal is proposed for image encryption. In this method, 8-bits mask is used for changing the pixel gray level of main image. Every bit content is 0 or 1. For changing each pixel gray level, value of each bit of the mask is selected by one of the 256 cellular automat standard rules. One of the 256 cellular automat standard rules is determined by chaotic signal. Studying the obtained results of the performed experiments, high resistance of the proposed method against brute-force and statistical invasions is obviously illustrated.

Keywords: Image encryption, cellular automata, chaotic function.

INTRODUCTION

Together with the rapid rate of multimedia products and vast distribution of digital products on internet, protection of digital information from being copied, illegal distribution is of great importance each day. To reach this goal, various algorithms have been proposed for image encryption (Mitra et al., 2006; Chang and Yu, 2002; Enayatifar and Meybodi, 2009; Rotermanm and Porat, 2007). Recently, due to the widespread use of chaotic signals in different areas, a considerable number of researchers have focused on these signals for image encryption (Alsultanny, 2007; Yen and Guo, 2000; Li and Zheng, 2002; Kwok and Tang, 2007; Behnia et al., 2007). One of the most important advantages of chaotic signals is their sensitivity to the initial conditions and also their noise-like behavior while being certain. In Alsultanny (2007), the method of moving pixels is proposed for image encryption. In Yen and Guo (2000), an algorithm is proposed which is based on a key for the encryption of the image (CKBA[2]). In this method a chaotic signal is utilized to determine the amount of gray scale of the pixels. Later researches have shown that the aforesaid method is not securing enough (Li and Zheng, 2002).

*Corresponding author. E-mail: f_mirzaei62@yahoo.com

In this paper a hybrid model of cellular automata and chaotic signal is proposed for image encryption. In this method, 8-bits mask is used for changing the pixel gray level of main image. Every bit content is 0 or 1. For changing each pixel gray level, value of each bit of the mask is selected by one of the 256 cellular automat standard rules. One of the 256 cellular automat standard rules is determined by chaotic signal.

Cellular automata

Cellular automata were introduced by Ulam and von Neumann (Neumann, 1966). They have been progressively used to model a great variety of dynamical systems in different application domains (Preston and Duff, 1984; Wolfram, 1985).

A cellular automaton is basically a computer algorithm that is discrete in space and time and operates on a lattice of sites (in our case, pixels). A (bi-dimensional, deterministic) cellular automaton (CA) is a triple A = (S;N;δ); where S is a nonempty set, called the state set, N $\subseteq Z^2$ is the neighborhood, and $\delta : S^N \rightarrow S$ is the local transition function (rule); the argument of δ indicates the states of the neighborhood cells at a given time, while its value the central cell state at the next time.

In order to define a neighborhood in a standard way we can use some norms h on R^2 such that N = $B_h(0, r) \cap Z^2$ (where Bh(0, r) is the ball of radius r ≥ 1). The most common neighborhoods are:

(i) Von Neumann neighborhood using the norm:

$$R^2 \ni x \to h(x) := |x|_1 = |x_1| + |x_2| \in R_+, x = (x_1, x_2).$$

(ii) Moore neighborhood attached to the norm:

$$R^2 \ni x \to h(x) := |x|_\infty = max\{|x_1|, |x_2|\} \in R_+, x = (x_1, x_2).$$

A cellular automaton, A = *(S;N;δ)* is said to be symmetric if the value of the local rule is constant on symmetric inputs, that is:

$$\delta(s_1, s_2, \dots, s_{|N|}) = \delta(s_{\alpha(1)}, s_{\alpha(2)}, \dots, s_{\alpha(N)}),$$

for every $s_1, s_2, \dots, s_N \in S$ and $\sigma \in S_N (the\ permutation\ group\ of\ |N| degree)$.

Chaotic signal

Chaos is a phenomenon that occurs in definable nonlinear systems which are highly sensitive to initial values, and trend to show random-like behavior. If such systems satisfy the conditions of Liapanov exponential equation, it will continue to be in the chaotic mode. The main reason why these signals are utilized in image encryption is the definability of the system while being random-like; this caused the output of the system seem random to the invaders. Since it is definable by the encrypted, it is decodable. The advantages of these functions are studied in two parts:

(a) Sensitivity to the initial value: This means that minor variation of the initial values can cause considerable differences in the next value of the function, that is when the initial signals varies a little, the resulting signal will differ significantly.
(b) Random-like behavior: In comparison with the generators of ordinary random numbers, in which the series of generated random numbers are capable of regeneration, the random-number-generation methods utilized in chaotic function algorithms are able to regenerate the same random numbers, having the initial value and the transform function.

Equation (1) is one of the most well-known signals to have random-like behavior and is known as Logistic Map Signal.

$$X_{n+1} = rX_n(1 - X_n) \quad (1)$$

The Logistic Map Signal will have a chaotic behavior in case the initial value is $X_0 \in (0,1)$ and $r = 3.9999$ In Figure 2, the signal behavior with initial value is $X_0 = 0.5$ and $r = 3.9999$ can be seen.

The proposed method

In this method, value of 8-bits mask will be XOR with value of each pixel in base binary of main image. So the pixel gray level of main image is changed. Content of mask for each pixel get a new value that it determine with a hybrid model of cellular automata and chaotic signal.
The initial value of 8-bits mask is determined with 80-bits key. After that for determine new value of mask per state, one of the 256 standard rules is used. On the other hand rule number is determined with Logistic Map Chaotic Signal.

Step 1: Choose 80-bits key for determine initial value of chaotic signal and 8-bits mask:

$$K_0, K_1, \dots, K_9 (ASCII) \quad (2)$$

In this key, K_i determines an 8-bit block of the key. The binary form of the mentioned key is as follows:

$$K = \begin{pmatrix} K_{01}, K_{02}, K_{03}, K_{04}, K_{05}, K_{06}, K_{07} \\ K_{08}, \dots\dots\dots\dots\dots\dots, K_{91}, K_{92}, K_{93} \\ K_{94}, K_{95}, K_{96}, K_{97} K_{98}, (\text{Binary}) \end{pmatrix} \quad (3)$$

The initial value is resulted by Equation (4).

$$X_0 = \begin{pmatrix} K_{01} \times 2^{79} + K_{02} \times 2^{78} + \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ K_{11} \times 2^{71} + K_{12} \times 2^{70} + \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ K_{n7} \times 2^1 + K_{n8} \times 2^0 \end{pmatrix} / 20^{80} \quad (4)$$

The initial value of 8-bits mask is shown below:

$$K_{00} \quad K_{01} \quad K_{02} \quad K_{03} \quad K_{04} \quad K_{05} \quad K_{06} \quad K_{07}$$

Step 2: The X_0 as Logistic Map initial value is used for determine one of the 256 rules of cellular automata. As seen in Figure 1, the variation range of the signal is [0, 1].This range is divide into *P* parts whose size is determines by:

$$\varepsilon = 1/P \quad (5)$$

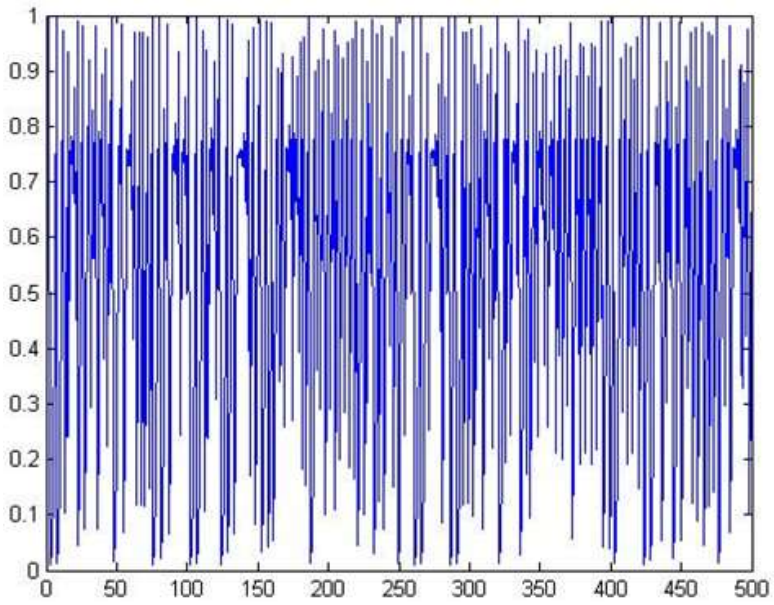

Figure 1. The chaotic behavior of Signal (1) in its 500 iterations.

Based on this segmentation, the range of the i[th] part is determined by:

$$((i-1)\varepsilon, i\varepsilon) \tag{6}$$

GivenX_0, first value is generated with Logistic Map in attention *P*=255(the number of cellular automata rules).

$$X_n = Round(P \times X_{n-1}) \tag{7}$$

Value obtained for X_n is used as number of cellular automata rules.

Step 3: Given rule for all bits of mask is executed simultaneously so the mask is determined with new value. This value will be XOR with first pixel of main image. Finally, the new value replaced with old value in main image. For all pixels of main image, Steps 2 and 3 is executed.

In conclusion, the all pixels gray level of main image is changed to new value.

EXPERIMENTAL RESULTS

A proper encryption method must be resistant and secure to various types of invasion, such as cryptanalytic invasions, statistical invasions and brute-force invasions. In this study, besides the efficiency of the proposed method, it is studied in terms of statistical and sensitivity analyses, in case of key changes. The results show that the method stands a high security level against various types of invasions.

Key sensitivity analysis

In Figure 2b, the encryption of the image for Figure 2a, using the encryption key of 'ABCDEF0123456789ABCD' is seen. The encryption of the same image is also done using the keys 'ABCDEF0123456789ABCE' and 'ABCDEF0123456789ABBD', respectively seen in Figures 2c and 2d.

In order to compare the obtained results, the average of correlation coefficient (horizontal, vertical and diagonal) of some specific points is calculated for each pair of encrypted images (Table 1). The obtained results show that this method is sensitive to even small changes of the key.

For instance, the effect of the change in a pixel of the original image on the encrypted image was measured using two standards of NPCR and UACI (Enayatifar and Meybodi, 2009; Fateri et al., 2010); NPCR is defined as the variance rate of pixels in the encrypted image caused by the change of a single pixel in the original image. UACI is also defined as the average of these changes. These two standards are as follows:

$$NPCR = \frac{\sum_{ij} D(i,j)}{W \times H} \times 100\%$$

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\% \tag{8}$$

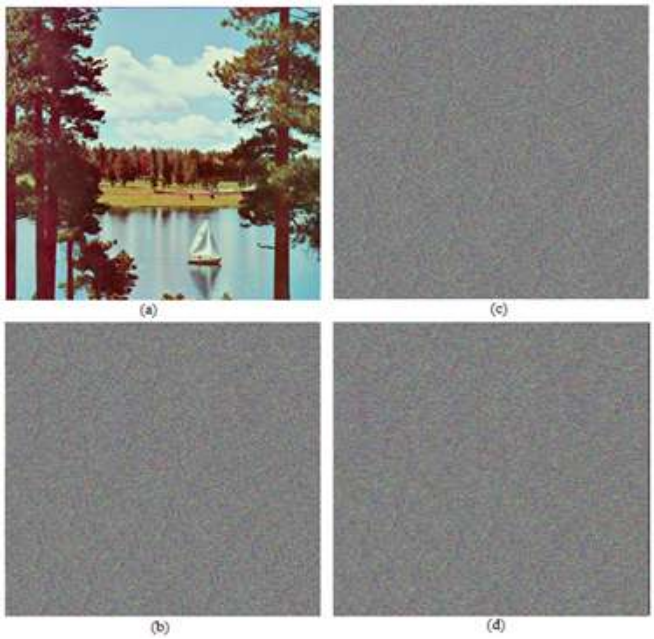

Figure 2. (a) Main image, (b) encryption with 'ABCDEF0123456789ABCD, (c) encryption with 'ABCDEF0123456789ABCE', (d) encryption with 'ABCDEF0123456789ABBD'.

Table 1. The average of correlation coefficient (horizontal, vertical and diagonal) of some specific points for each pair of the images.

encrypted image	Figures 2b and 2c	Figures 2c and 2d	Figures 2b and 2d
correlation coefficient	0.0019	0.0009	0.0011

where H and W are respectively the length and width of the images, and C_1 and C_2 are two encrypted images of two images which are different in one pixel. D is defined as:

$$D(i,j)=\begin{cases}1 & if \quad C_1(i,j)=C_2(i,j)\\ 0 & otherwise\end{cases}$$

The obtained values of an image with the size 256×265 are as follows: NPCR = 0.49%, UACI= 0.42%

The value obtained in Table 1 clearly shows that this method is resistant to differential attacks.

Histogram analysis

Histogram shows the numbers of pixels in each gray scale of an image. In Figure 3, the original image is seen in Frame (a) and the histogram of the image in red, green and blue scales are seen in Frames (b), (c) and (d), respectively. Also, in Frame (e), the encrypted image (using key 'ABCDEF0123456789ABCD' in a 16-scale) can be seen. In Frames (f), (g) and (h), the histogram of the encrypted image in red, green and blue scales can be seen, respectively. As seen in Figure 3, the histogram of the encrypted image is totally different from that of the original one, which restricts the possibility of statistical invasions.

Correlation coefficient analysis

Statistical analysis has been performed on the proposed image encryption algorithm. This is shown by a test of the correlation between two adjacent pixels in plain image and ciphered image. We randomly select 1000 pairs of two-adjacent pixels (in vertical, horizontal, and diagonal direction) from plain images and ciphered images, and calculate the correlation coefficients, respectively by using the following two formulas (Table 2 and Figure 4(a) and (b)):

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

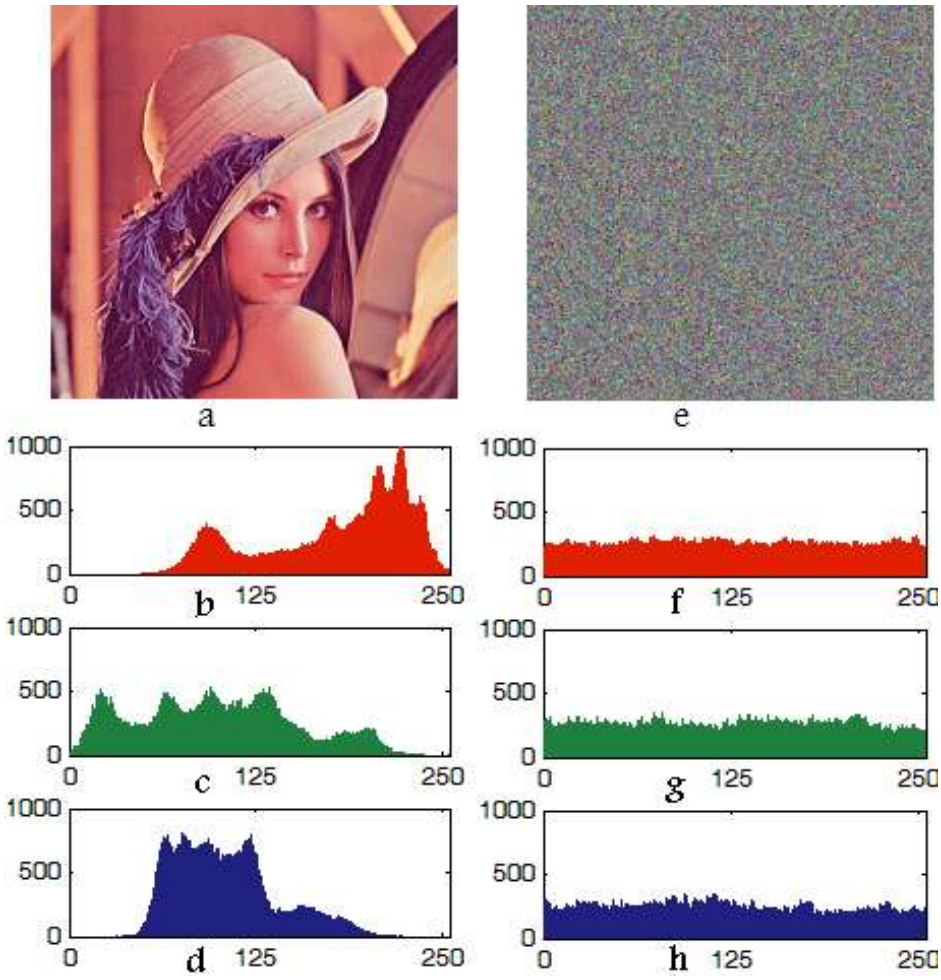

Figure 3. (a) The main image, and (b), (c) and (d) respectively show the histogram of the lena image of size 256×256 in red, green and blue scales, and (e) shows the encrypted image using the key, ABCDEF0123456789ABCD in a 16-scale. (f), (g) and (h) show the histogram of the encrypted image in red, green and blue scales.

Table 2. Correlation coefficient of two adjacent pixels in two images plain ciphered.

	Plain	Ciphered
Horizontal	0.9311	0.0251
Vertical	0.9255	0.0247
Diagonal	0.9126	0.0172

$$r_{xy} = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (9)$$

where,

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

Here, E(x) is the estimation of mathematical expectations of x, D(x) is the estimation of variance of x, and cov (x, y) is the estimation of covariance between x and y, where x and y are grey-scale values of two adjacent pixels in the image.

Conclusions

In this paper, a new method of image encryption has been proposed, which utilizes chaotic signals and the

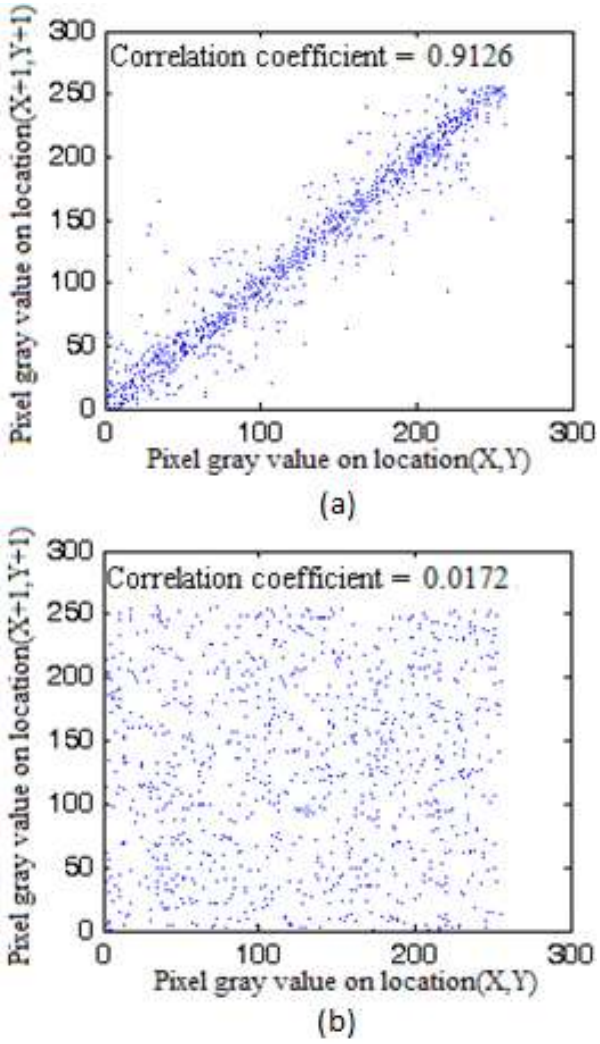

Figure 4. (a) Correlation analysis of plain image; (b) correlation analysis of ciphered image.

Max-Heap tree for higher complexity. As seen in the experimental results, this method shows a very proper stability against different types of invasions such as decoding invasions, statistical invasions and brute-force ones. The amount of NPCR and UACI shows the capabilities of the proposed method.

REFERENCES

Mitra A, Subba RYV, Prasanna SRM (2006). “A New Image Encryption Approach using Combinational Permutation Techniques”, Int. J. Comp. Sci., pp. 1306-4428

Chang C, Yu T (2002). “Cryptanalysis of an encryption scheme for binary images”, Patt. Recogn. Lett., pp. 1847-1852.

Enayatifar R, Meybodi RM (2009).” Image Hiding with Chaotic Logistic Map”, Int. Conf. Data Mining, Iran.

Rotermanm Y, Porat M (2007). “Color image coding using regional correlation of primary colors”, Image and Vision Comp., pp. 637-651.

Alsultanny YA (2007). “Random-bit sequence generation from image data”, Image Vision Comp., 1178-1189

Yen JC, Guo JI (2000). “A New Chaotic Key-Based Design for Image Encryption and Decryption”, Proceedings IEEE Int. Conf. Circuits Syst., 4: 49-52.

Li S, Zheng X (2002). “Cryptanalysis of a Chaotic Image Encryption Method”, Scottsdale, AZ, USA, 2002, in: Proceedings IEEE Int. Symp. Circuits Syst., 2: 708–711.

Kwok HS, Tang WS (2007). “A fast image encryption system based on chaotic maps with finite precision representation”, Chaos Solitons Fractals, pp. 1518-1529.

Behnia S, Akhshani A, Ahadpour S, Mahmodi H, Akhavan A (2007). “A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps”, Phys. Lett. A., 391-396

Neumann J (1966). Theory of Self-Reproducing Automata (edited and completed by Arthur Burks), University of Illinois Press.

Preston K, Duff MJB (1984). Modern Cellular Automata. Theory and Applications, Plenum Press, London,

Wolfram S (1985). "Cryptography with Cellular Automata", Proceedings Crypto., 85: 429-432.

Fateri S, Rasul E, Mohammad T (2010). “Image Encryption via Hybrid Model of Chaotic Signal and Genetic Operation”, International Conference on Cryptography, Iran.