International Journal of the Physical Sciences Vol. 6(4), pp. 837-842, 18 February, 2011
Available online at http://www.academicjournals.org/IJPS
DOI: 10.5897/IJPS11.034
ISSN 1992 - 1950 ©2011 Academic Journals

Full Length Research Paper

Hybrid model of chaotic signal and complete binary tree for image encryption

Mehrzad Khaki Jamei[1], Rasul Enayatifar[2] and Hamid Hassanpour[3]*

[1]Islamic Azad University, Sari Branch, Sari, Iran.
[2]Islamic Azad University, Firuzkooh Branch, Firuzkooh, Iran.
[3]Department of Computer Engineering and Information Technology, Shahrood University of Technology, Shahrood, Iran.

Accepted 25 January, 2011

In this paper, a new method was proposed for image encryption using chaotic signals and complete binary tree. In this method, perfect binary tree was utilized for further complexity of the encryption algorithm, higher security and changing the amount of gray scale of each pixel of the original image. Studying the obtained results of the performed experiments, high resistance of the proposed method against brute-force and statistical invasions was obviously illustrated. Also, the obtained entropy of the method which is about 7.9931 is very close to the ideal amount of 8.

Key words: Chaotic signal, image encryption, complete binary tree.

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; Joshi et al., 2007; Roterman 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 the method of moving pixels is proposed for image encryption (Alsultanny, 2007). In an algorithm which was proposed, is based on a key for the encryption of the image ($CKBA^2$) (Yen and Guo, 2000). In this method, a chaotic signal was utilized to determine the amount of gray scale of the pixels. Later researches have shown that the aforesaid method was not securing enough (Li and Zheng, 2002).

*Corresponding author. E-mail: h.hassanpour@ieee.org.

In this paper, a new method was proposed for image encryption using chaotic signals and complete binary tree to make the encryption algorithm more complex and secure, in which the implementation of Max-Heap tree has caused that, even when the initial value of the chaotic function was revealed, the real amount of gray scale of each pixel cannot be accessed. In the following section, Max-Heap trees are primarily introduced in brief, and then the proposed method was analyzed. In the experimental results section, the functionality of this method was studied through some experiments. The reversibility of the method was studied in the next section and finally the conclusions were drawn.

Complete binary tree

In computer science, a binary tree is a tree data structure in which each node has at most two child nodes, usually distinguished as "left" and "right". Nodes with children are parent nodes, and child nodes may contain references to their parents. Outside the tree, there is often a reference to the "root" node (the ancestor of all nodes), if it exists. Any node in the data structure can be reached by starting at root node and repeatedly following references to either the left or right child.

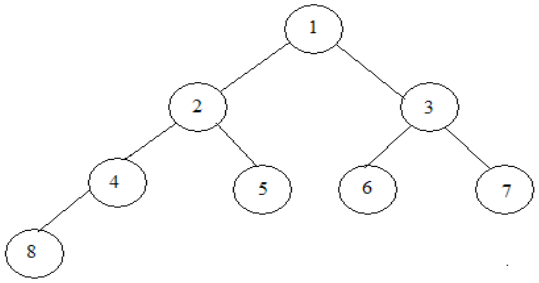

Figure 1. Complete binary tree.

A binary tree in which every level, except possibly the deepest, is completely filled. At depth n, the height of the tree, all nodes must be as far left as possible. For example in Figure1 a complete binary tree was shown.

Chaotic signal

The chaotic signals are like noise signals but they are completely certain, that is if we have the primary quantities and the drawn function, the exact amount will be reproduced. The advantages of these signals will be as follows (Kwok and Tang, 2007):

The sensitivity to the primary conditions

By this we mean a minor change in primary amount will cause a significant difference in subsequent measures. It means if we have a little change in the signal amount, the final signal will be completely different.

The apparently accidental feature

In comparison with productive accidental natural number in which the range of the numbers can not be produced again, the technique used for producing the accidental number in algorithm based on the chaotic function will prepare the ground that if we have the primary quantities and the drawn function, we can produce the numbers again.

The deterministic work

As the chaotic functions have the accidental manifest, they are completely exact. It means as we have the drawn function and the primary quantities we can produce and reproduce sets of numbers seemingly have no system and order. The equation 1 shows one of the most famous signals which has chaotic features and is known as the Logistic Map signal.

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

In which the X_n will get the numbers between [0,1], the signal shows three different chaotic features in three different range based on the division of the r parameter of which the signal feature will be as well by considering the $x_0 = 0.3$

1) If we have r € [0, 3], then the signal feature in the first 10 repetition showed some chaos and after that it was fixed (Behnia et al., 2007) (Figure 2a).
2) If we have r € [3, 3.57], then the signal feature in the first 20 repetition showed some chaos and after that it was fixed (Behnia et al., 2007) (Figure 2b).
3) If we have r € [3.57, 4], then the signal feature is completely chaotic (Behnia et al., 2007) (Figure 2c).

According to the given description and the research requirements for the complete chaotic features for image encryption, the logistic map chaotic signals with the primary values of $X_0 = 0.3$ and r € [3.57, 4] were used.

THE PROPOSED METHOD

In this method, a binary Max-Heap tree was made by non-repetitive random numbers from 0 to 255, with random order generated by the chaotic function of Logistic Map. This function needs an initial value to start out. To increase the level of security, an 80-bit key was used to generate the initial value of the signal (Equation 1). This key can be defined as an ASCII character of the form:

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

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

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

The initial value is resulted by Equation 4.

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

On the other hand as seen in Figure 2, the variation range of the signal is [0, 1]. This range was divided into *P* parts whose size is determines by:

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

Based on this segmentation, the range of the i^{th} part is determined by:

$$((l-1)\varepsilon, l\varepsilon) \quad (6)$$

In this method, *P* was 256 (the number of gray scales). In the

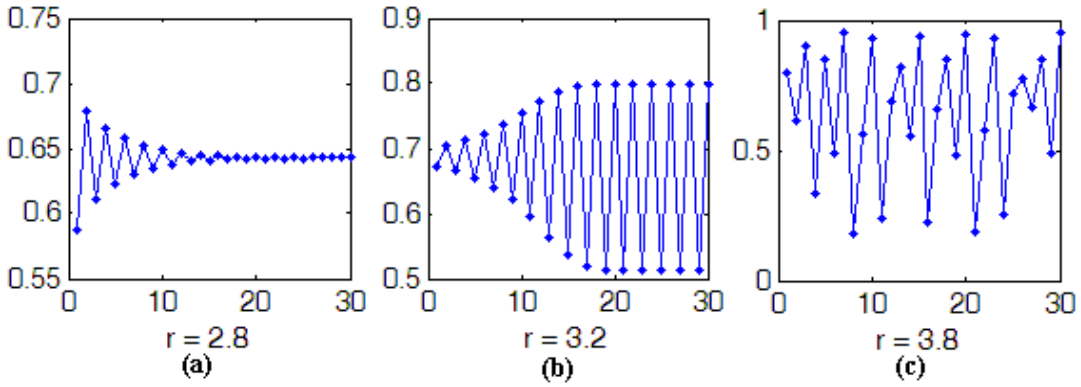

Figure 2. The logistic map chaotic signal with a). X_0=0.3, r € [0, 3], b) r € [3, 3.57], c) r € [3.57, 4].

following part, the range in which X_1 that was generated by Equation 1 and the initial value of X_0, will be determined. The number of this range was chosen as the first order, provided that this amount was not previously located in the range; this will continue as long as the signal magnitude is located in all *P* parts. Finally, non-repetitive random order will be generated in the range of (0.255) as:

$$Iteration = (it_1, it_2, \ldots, it_r) \quad (7)$$

Now, the first value of the iteration will be put into the root and the second one (based on the Max-Heap tree structure) in the tree; this will continue as long as all the numbers have filled the tree. Finally, a binary Max-Heap tree of 256 nodes will be generated in each node of which there is a unique number from 0 to 255. This tree was used to change the gray scale of the image pixels.

In the nest stage, 50% of the pixels of the first row of the image were selected by the use of Equation 1, Equation 2 (p = the image width) and the initial value of Xr (the last number generated by the chaotic signal in the last stage). The root of the tree generated in the previous stage replaces the first pixel of the next line. Knowing the tree structure, the children of the each node of the tree are put in a separate pixel of the image. Then, the value of each node is xored with the value of the pixel it is in. This will continue up to the last line. In this stage, three points are of great importance:

a) The position of the children of a node on the pixel is this way: if the node is in the position (x,y) of the image, the left-hand-side child is at (x+1,y-1) and the right-hand-side child is at (x+1,y+1).
b) In a pixel which contains more than one node, the value of all nodes and the value of the pixel are xored with each other (together) (nodes 15 and 10 as seen in Figures 3a and b).
c) The image is assumed to be a node. Figures 3a and b are examples of the proposed method, in which a 4×4 image and a complete binary tree of 6 nodes are considered.

In Figure 3b, by inserting the root on pixel 2 and assuming the image to be spherical, node 3 will be placed on pixel 12. The pseudo-code of the proposed method is as seen in Figure 4.

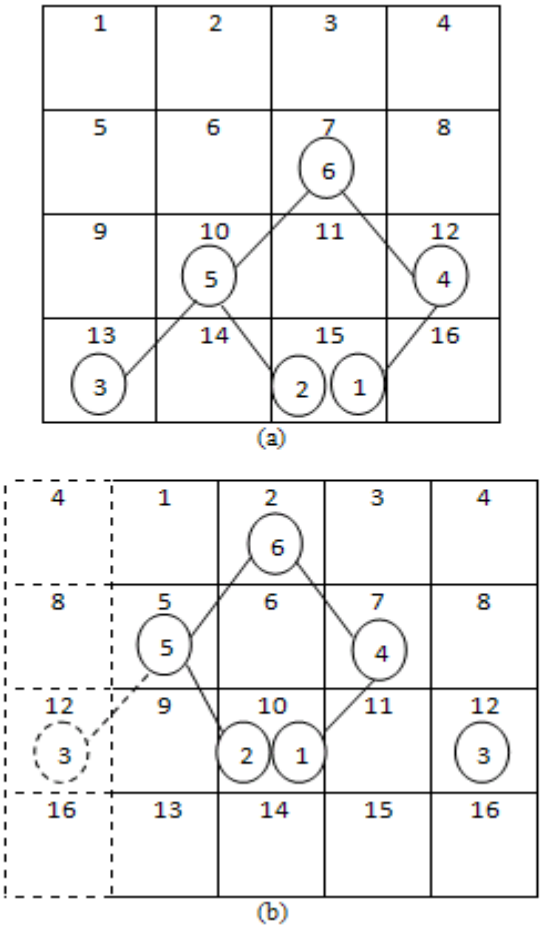

Figure 3a. The root is located in pixel 7. b, the root is located in pixel 2.

EXPERIMENTAL RESULTS

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

Initialize

$t = 0$, $r = 3.999$, $K = K_0, K_1, ..., K_9 (Ascii)$

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

While $t \neq 256$ ***do***

Repeat

$\text{Produce } X_{n+1} = r \times X_n \times (1 - X_n)$

$Number \leftarrow Round(X_{n+1} \times 255)$

Until $Number$ *exist in Iteration*

Inc(t)

$Iteration[t] \leftarrow Number$

endWhile

$CBTree \leftarrow \text{Create CompleteBinaryTree from Iteration}$

i=0 , j=0
While $i \neq \text{Image Hieght}$ ***do***
Count=0
While $Count \neq \frac{50}{100} \times \text{Image Width}$ ***do***
Repeat
$\text{Produce} X_{n+1} = r \times X_n \times (1 - X_n)$
$Number \leftarrow Round(X_{n+1} \times \text{Image Width})$
Until *Number exist* ***in*** *ImageWidthArray*
Inc(Count)
ImageWidthArray[Count]=Number
endWhile
Inc(i)
For *Num=1* ***to*** *Count*
j=ImageWidthArray[Num]
Xor(Image(i,j),CBTree Root)
CBT(CBTree,i,j)
endFor
endWhile

function *CBT(T,i,j)*
Xor(Image(i+1,j-1), CBT (T->left,i+1,j-1))
Xor(Image(i+1,j+1),CBT(T->Right,i+1,j+1))
endFunction

Figure 4. The pseudo-code of the proposed method.

Entropy analysis

The entropy is the most outstanding feature of the randomness (Young, 1995). Information theory is a mathematical theory of data communication and storage founded by Claude E. Shannon in 1949 (Shannon, 1949). There is a well-known formula for calculating this entropy:

$$H(S) = \sum_{i=0}^{2N-1} P(s_i) \log\left(\frac{1}{P(s_i)}\right) \quad (8)$$

where $P_{(si)}$ represents the probability of symbol *si* and the entropy is expressed in bits.

Actually, given that a real information source seldom transmits random messages, in general, the entropy value of the source is smaller than the ideal one. However, when these messages are encrypted, their ideal entropy should be 8. If the output of such a cipher emits symbols with entropy of less than 8, then, there would be a possibility of predictability which threatens its security. The value obtained is very close to the theoretical value 8. This means that information leakage in the encryption process is negligible and the encryption system is secure against the entropy attack. Using the above-mentioned formula, we have got the entropy H(S) = 7.9931, for the source s = 256. Entropy for some Images is shown in Table 1.

Key space analysis

In Figure 5b, the encryption of the image for Figure 5a, using the encryption key of ABCDEF0123456789ABCD is seen. The encryption of the same image was also done using the keys BBCDEF0123456789ABCD and ABCDEF0123456789ABCE respectively as seen in Figures 5c and d.

In order to compare the obtained results, the average of correlation coefficient (horizontal, vertical and diagonal) of some specific points was calculated for each pair of encrypted images (Table 1). The obtained results showed 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 (Chen et al., 2004; Mao et al., 2004); 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:

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

$$UACI = \frac{1}{W \times H} \left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255} \right] \times 100\ \% \quad (9)$$

Table 1. Entropy of some Images.

Image	Lena	Peppers	House	Boat
Entropy	7.9931	7.9928	7.9912	7.9904

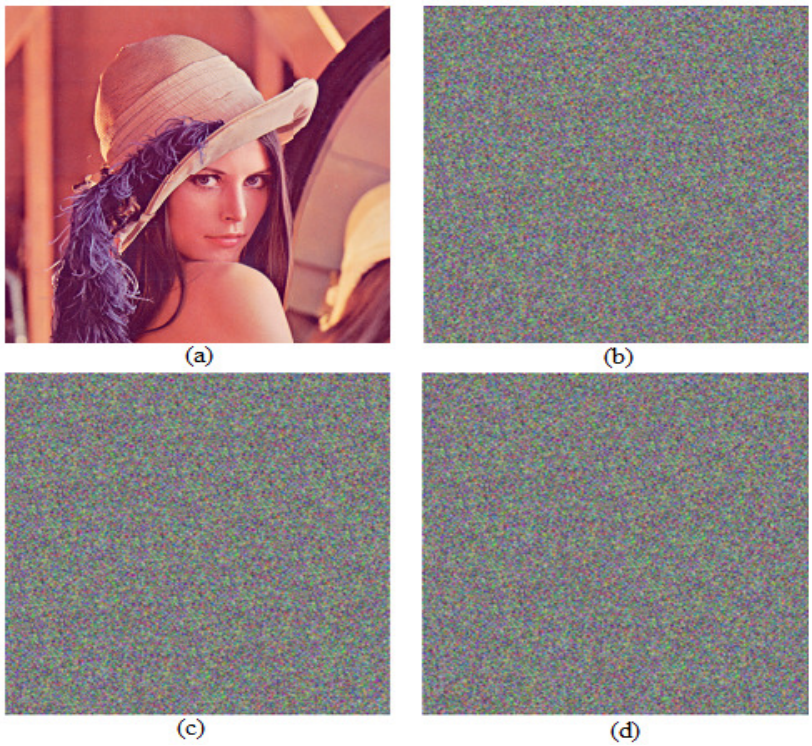

Figure 5. The result of image encryption for an image (Figure 7a): using the encryption key of ABCDEF0123456789ABCD in 7b, the encryption keys BBCDEF0123456789ABCD and ABCDEF0123456789ABCE, respectively seen in 7c and d.

Table 2. The average of correlation coefficient (horizontal, vertical and diagonal) of some specific points for each pair of the images.

Encrypted image-Fig	5b and c	5c and d	5b and d
Correlation coefficient	0.0020	0.0018	0.0013

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 = 0.432%, UACI = 0.347%.

The value obtained in Table 2 clearly showed that this method was resistant to differential attacks.

Conclusions

In this paper, a new method of image encryption has been proposed, which utilizes chaotic signals and the complete binary tree for higher complexity. As seen in the experimental results, this method showed a very proper stability against different types of invasions such as

decoding invasions, statistical invasions and brute-force ones. The high entropy of the method (7.9931) showed the capabilities of the proposed method.

REFERENCES

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

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

Chang C, Tai-Xing Y (2002). “Cryptanalysis of an encryption scheme for binary images”, Patt. Recognition Lett., 1847–1852.

Chen G, Mao YB, Chui CK (2004). “A symmetric image encryption scheme based on 3D chaotic cat maps”, Chaos, Solitons & Fractals, pp. 74-82.

Joshi M, Chandrashaker S, Singh K (2007). Color image encryption and decryption using fractional Fourier transform. Optics Commun., 811–819.

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

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.

Mao YB, Chen G, Lian SG (2004). “A novel fast image encryption scheme based on the 3D chaotic baker map”, Int. Bifurcat. Chaos, pp. 544-560.

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

Roterman Y, Porat M (2007). “Color image coding using regional correlation of primary colors”, Image Vision Computing, 637–651

Shannon CE (1949). Communication Theory of Secrecy Systems. Bell Syst. Tech. J., 28: 65.

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.

Young LS (1995). In: B. Branner, P. Hjorth (Eds.), NATO ASI Series, Kluwer Academic Publishers, p. 293.