International Journal of the Physical Sciences Vol. 6(2), pp. 221-228, 18 January, 2011
Available online at http://www.academicjournals.org/IJPS
DOI: 10.5897/IJPS10.630
ISSN 1992 - 1950 ©2011 Academic Journals

Full Length Research Paper

Image encryption via logistic map function and heap tree

Rasul Enayatifar

Islamic Azad University, Firoozkuh Branch, Firoozkuh, Iran. E-mail: r.enayatifar@gmail.com.

Accepted 30 December, 2010

In this paper, a new method is proposed for image encryption using chaotic signals and Max-heap tree. In this method, Max-heap tree is 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 is 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: Image encryption, heap tree, logistic map.

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; Chin-Chen and Tai-Xing, 2002; Yalon and Porat, 2007; Yalon 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 (Yas Abbas, 2007; Yen and Guo, 2000; Li and Zheng, 2002; Kwok and Wallace, 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 Yas Abbas (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 secure enough (Li and Zheng, 2002). In this paper, a new method is proposed for image encryption using chaotic signals and Max-heap tree to make the encryption algorithm more complex and secure, in which the implementation of Max-heap tree has caused, even when the initial value of the chaotic function is revealed, the real amount of gray scale of each pixel cannot be accessed.

MAX-HEAP TREE

One of the special trees which is widely applied in computer sciences is Max-heap tree. This tree is a complete binary tree in which the initial value of each node is larger than or equal to the keys of its children.

Insertion of information in this tree is done as: the tree is always filled from left to right in the last line and then the next line. While inserting a new node, it is inserted in the far left empty space of the last line (not filled yet), so that the tree is always complete. Then the heapification is done, in which a node in the lowest point might be replaced by its parent as many times as it takes to be heapified. For instance, in case the insertion of 9 digits is as 5, 8, 2, 3, 4, 7, 9, 20, 14, the resulting Max-heap tree is shown in Figure 1.

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

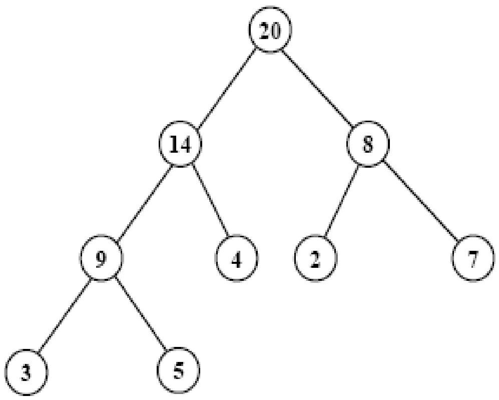

Figure 1. Max-heap tree.

encrypter, 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.

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

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, a binary Max-heap tree is 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 security, an 80-bit key is used to generate the initial value of the signal (Equation 1). This key can be defined as an ASCII character of the form:

$$\mathrm{K}_0, \mathrm{K}_1, \ldots, K_9(ASCII) \qquad (2)$$

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

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

The initial value is resulted by Equation (4).

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

On the other hand and as seen in Figure 2, the variation range of the signal is (0,1).This range is divide into P parts whose size is determines by:

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

Based on this segmentation, the range of the ith part is determined by:

$$((i - 1)\varepsilon, i\varepsilon) \qquad (6)$$

In this method, P is 256 (the number of gray scales). In the following part, the range in which X_1 that is generated by Equation (1) and the initial value of X_0, will be determined. The number of this range is 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:

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

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 is 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 are selected by the use of Equations (1) and (2) (p=the image width) and the initial value of X_r (the last number generated by the chaotic signal in the last stage). The root of the tree generated in the previous stage

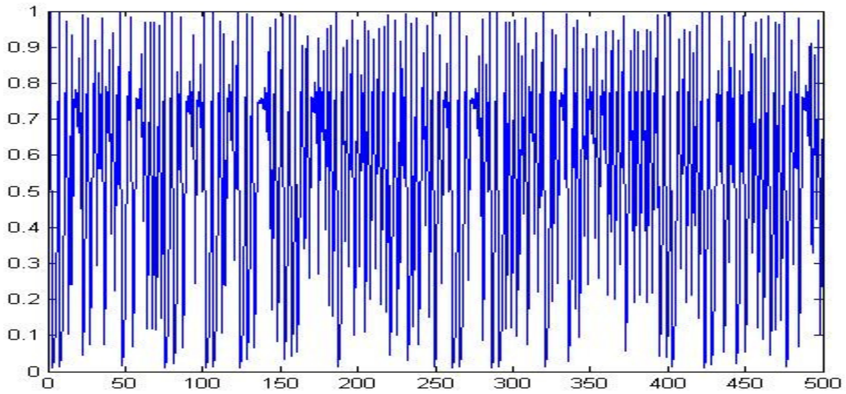

Figure 2. The chaotic behavior of signal (1) in its 500 iterations.

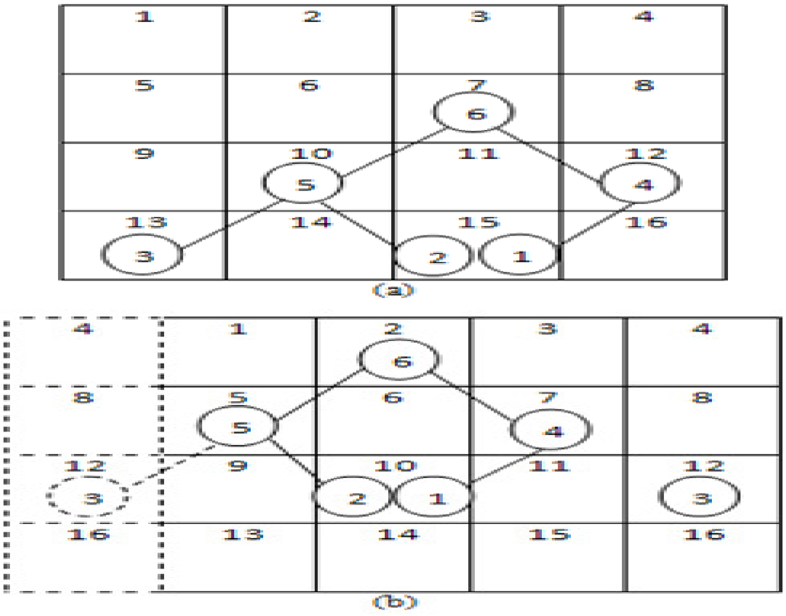

Figure 3. (a) The root is located in pixel 7 (b) The root is located in pixel 2.

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 in Figures 3a and 3b).

(c) The image is assumed to be a node. Figures 3a and 3b are examples of the proposed method, in which a 4×4 image and a Max-heap 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 seen in Figure 3.

Experimental results

A proper encryption method must be resistant and secured to various types of invasion, such as cryptanalytic invasions, statistical invasions and brute-force invasions.

Here, 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.

Histogram analysis

Histogram shows the numbers of pixels in each gray scale of an image. In Figure 5, 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 4, 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 1 and Figure 6a and b).

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

$$r_{xy} = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{8}$$

where,

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

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.

```
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
        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
$MHTree \leftarrow$ Create Max - Heap Tree from Iteration
$i=0\ ,\ j=0$
While $i \neq Image\ Hieght$ do
   Count=0
   While $Count \neq \frac{50}{100} \times Image\ Width$ do
      Repeat
         Produce $X_{n+1} = r \times X_n \times (1 - X_n)$
         $Number \leftarrow Round\ (X_{n+1} \times Image\ Width)$
      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),MHTree Root)
      MaxHeap(MHTree,i,j)
   endFor
endWhile

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

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

Information 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:

$$H(S) = \sum_{i=0}^{2N-1} P(s_i)\log\left(\frac{1}{P(s_i)}\right) \tag{9}$$

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

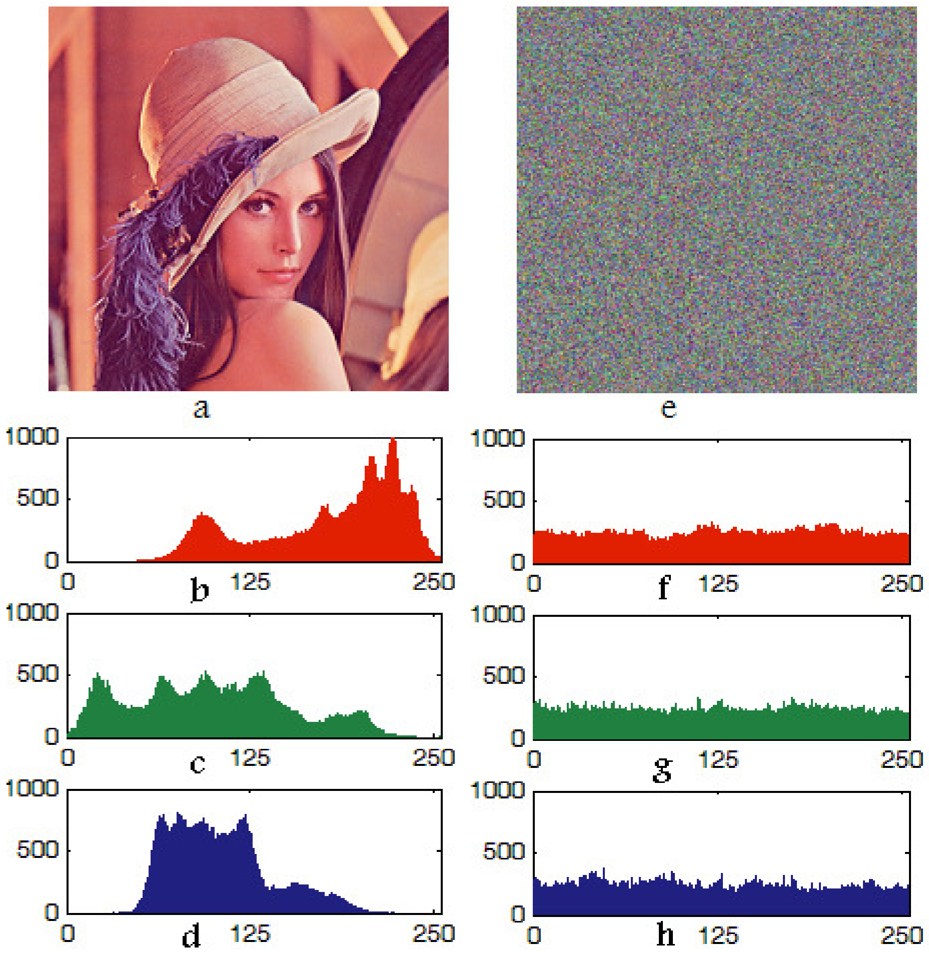

Figure 5. (a) the main image, and (b), (c) and (d) respectively show the histogram of the lena image of size 256×256 in red, green and blue scales, and (e) shows the encrypted image using the key, ABCDEF0123456789ABCD in a 16-scale. (f), (g) and (h) show the histogram of the encrypted image in red, green and blue scales.

Table 1. Correlation coefficient of two adjacent pixels in two images plain ciphered.

Pixels	Plain	Ciphered
Horizontal	0.9412	-0.0051
Vertical	0.8611	0.0078
Diagonal	0.8378	-0.0009

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.

Key space analysis

In a proper method, key should have enough space so that the method is resistant against brute-force invasions. In the proposed method, there can be 2^{80}(≈1.20893×10^{24})

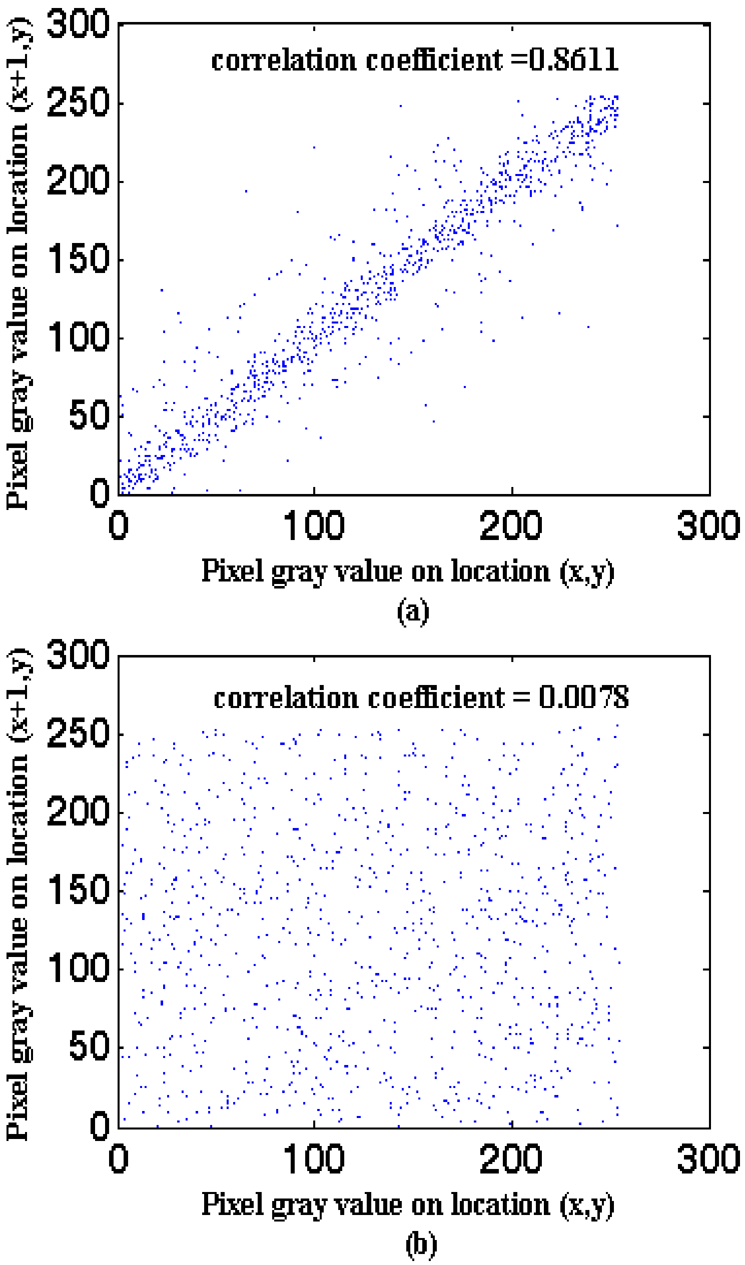

Figure 6. (a) Correlation analysis of plain image; (b) Correlation analysis of ciphered image.

different combinations of keys. Scientific results have shown that this number of key combinations is sufficient for a proper resistance against brute-force invasions.

Key space analysis

In Figure 7b, the encryption of the image for Figure 7a, using the encryption key of ABCDEF0123456789ABCD is seen. The encryption of the same image is also done using the keys BBCDEF0123456789ABCD and ABCDEF0123456789ABCE, respectively seen in Figures 7c and 7d.

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 2). 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 (Chen et al., 2004;

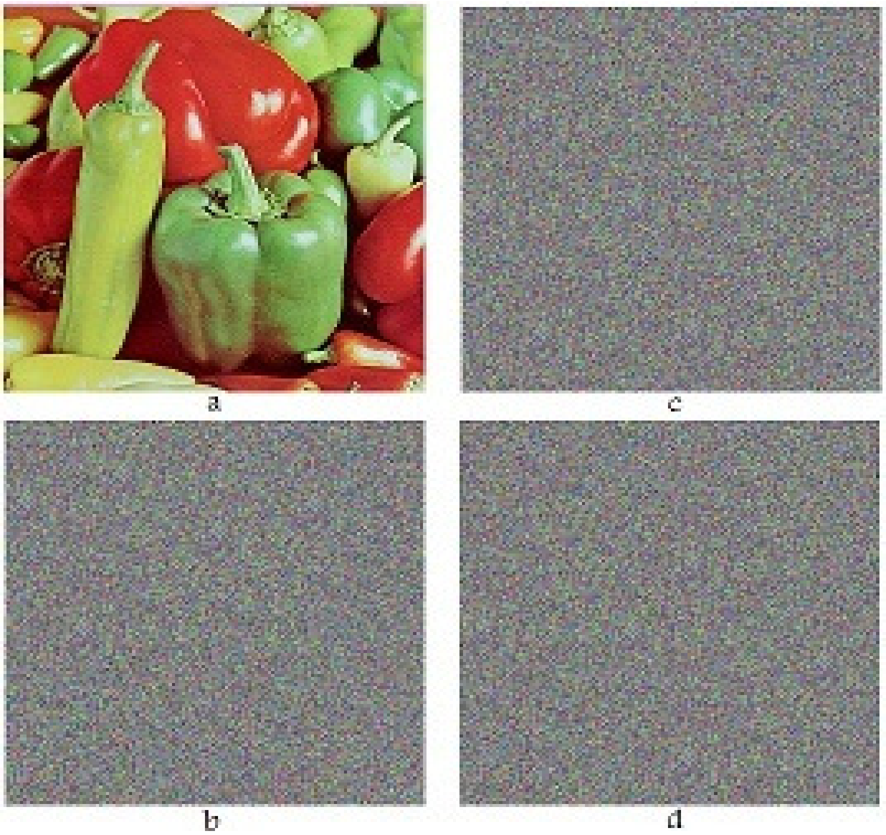

Figure 7. The result of image encryption for an image (a): using the encryption key of ABCDEF0123456789ABCD in b, the encryption keys BBCDEF0123456789ABCD and ABCDEF0123456789ABCE, respectively seen in c and d.

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

Encrypted image (Figure)	7b and 7c	7c and 7d	7b and 7d
Correlation coefficient	-0.0113	0.0011	-0.0074

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:

$$NPCR = \frac{\Sigma_{ij} D(i,j)}{W \times H} \times 100\% \qquad (10)$$

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

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:

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

The obtained values of an image with the size 256×265 are as follows: NPCR = 0.429%, UACI = 0.329%.

The value obtained in Table 2 clearly shows that this method is resistant to differential attacks.

Decoding an encrypted image

One of the vitalities of an image encryption method is its reversibility of the encrypted image to the original one. Using the proposed method, decoding an encrypted image takes place as follows: As mentioned earlier, one of the significant properties of chaotic functions is that, having the initial value and the transform function, the series of the numbers generated by the function can be regenerated. In this paper, having the key, the initial value of the chaotic function can be generated; therefore, the required series of numbers for the generation of Max-heap tree is provided. Then, the last generated value by the chaotic function of the previous stage is used to choose the first pixel of the first line. Unlike the encryption method, the tree is not transformed on the chosen pixel; instead, the position of the pixel is saved in the PosPixel series. Then the position of the second pixel of the first line is determined by the chaotic function. Thereby, the position of half of the pixels of the first line is saved in PosPixel. This will continue through the last line, where the following series is produced:

$$PosPixel \;=\left(\begin{matrix} (1,1),(1,2),...,\left(1,\dfrac{n}{2}\right) \\ (2,1),(2,2),...,\left(2,\dfrac{n}{2}\right) \\ ....\;..........\;... \\ (n,1),(n,2),...,\left(n,\dfrac{n}{2}\right) \end{matrix}\right)_{n\times\frac{n}{2}}$$

In PosPixel, in each element of ij, I determines the row number and j the normalized form of the first generated number by the Logistic Map in the range of (0, n). In the next step, the pixel in the position of the last value of PosPixel, (n, n/2), is used as the first pixel to be transformed and gone under Xored operation (as explained earlier). This will continue up to the first value of the PosPixel series, (1, 1). And finally, the decoded image is regenerated.

Conclusions

In this paper, a new method of image encryption has been proposed, which utilizes chaotic signals and the 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 high entropy of the method (7.9931) shows the capabilities of the proposed method.

REFERENCES

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

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

Chin-Chen C, Tai-Xing Y (2002). Cryptanalysis of an encryption scheme for binary images, Patt. Recognit. Lett., pp. 1847–1852.

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

Li S, Zheng H (2002). Cryptanalysis of a Chaotic Image Encryption Method. Scottsdale, AZ, USA. Proc. 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 FM, Prasanna SRM (2006). A New Image Encryption Approach using Combinational Permutation Techniques. Int. J. Comput. Sci., pp. 1306-4428.

Shannon CE (1949). Communication theory of secrecy systems. Bell Syst. Tech. J., 28: 656-715.

Yalon R, Moshe P (2007). Color image coding using regional correlation of primary colors, Image Vision Comput., pp. 637–651.

Yas AA (2007). Random-bit sequence generation from image data. Image Vision Comput., pp. 1178-1189.

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

Young LS, Branner B, Hjorth P (1995). (Eds.), NATO ASI Series, Kluwer Acad. Publ., p. 293.