Chaotic Image Encryption Based On Discrete Wavelet

Amirhoushang Arab Avval[1] **, Jila Ayubi**[2]

[1] **Department of electrical and electronic engineering of Sistan and Baluchestan university, Zahedan, Iran**
amirhoushang.arab@gmail.com
[2] **Department of electrical engineering, Meraj Higher Education Institute, Salmas, Iran**
Jila.ayubi@gmail.com

Abstract

In this paper, a digital image encryption algorithm based on discrete wavelet transform and chaos theory is referred. The value of the discrete wavelet transformation coefficient matrix was encrypted and the scrambled by adjusting chaos sequence. The proposed algorithm is described in detail. To illustrate the effectiveness of the proposed scheme, some security analysis are presented. The cryptosystem speed is analyzed and tested as well. Results of the various types of analysis are encouraging and it can be concluded that the proposed image encryption technique is suitable choice for practical applications.

Keywords: *Image Encryption, Wavelet Transform, Chaos, Chaotic Maps, High Security.*

1. Introduction

With the rapid growth of multimedia production systems, electronic publishing and widespread dissemination of digital multimedia data over the Internet, protection of digital information against illegal copying and distribution has become extremely important. The wavelet transformation and the chaos theory are now the hot spot of the research in the nonlinear scientific field, the combination of the two will have its potential advantages in non-linear problems [1]. Organically combining the chaos sequence and the existing encryption algorithm result in the chaotic encryption technology is considered to be a promising new encryption algorithm [2]. Recently, along with the rapid development of theory and application of chaos, many researchers are now focusing on the chaotic cryptography. A lot of image encryption schemes based on chaos theory have been presented [3]–[8]. These applications have been motivated by the chaotic properties such as ergodicity and sensitive dependence on initial conditions and system parameters, in addition to complex dynamics and deterministic behaviors.

2. DWT

Discrete Wavelet Transform (*DWT*) is a multiresolution analytical approach of time-frequency and can describe partial characteristics of time and frequency domains. The basic thought is to decompose the image to sub images with different space and frequency, then, the coefficient is processed. According, to S.Mallatfs pyramid algorithm shown in Fig.1, the image after wavelet decomposition is divided into four bands: horizontal direction, vertical direction, diagonal direction and low frequency part which can be decomposed on and on. The wavelet transformed image has three high frequency bands *LHi, HLi ,HHi*(*i* = 1, 2, 3) and a low frequency band LL3; the main energy is concentrated in the low frequency part with a few in horizontal, vertical and diagonal parts.

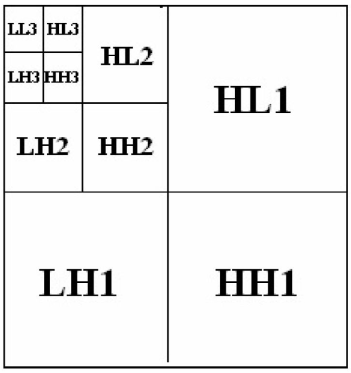

Figure. 1 The three-level decomposition of mage.

3. CHAOS

Logistic map is one of the simplest chaotic maps, which is determined by equation (1)

$$x_k = \mu x_k (1 - x_k) \qquad (1)$$

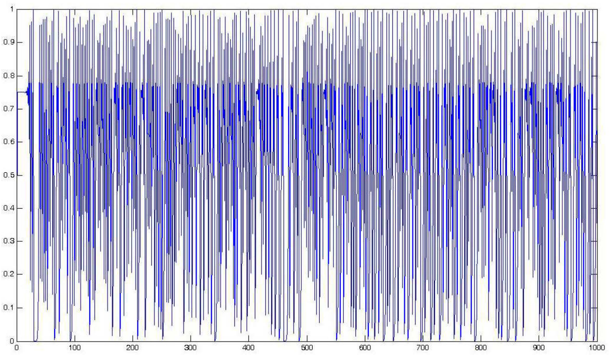

Figure. 2 Chaotic behavior of logistic map with X_0=0.24 and μ=3.99999.

Where $0 \leq \mu \leq 4$, $0 < x_{k+1} < 1$.When 3.5699456≤μ< 4,the map is in the chaotic states, and the sequence produced by logistic map is random and sensitive to original value. Moreover all the orbits of the logistic map are dense in the range of the map [0, 1]. Fig.2 shows the plot of x_k vs k for $x_0 = 0.24$ and $\mu = 3.99999$ after 1000 iteration.

4. THE ENCRYPTON AND DECRYPTION PROCEDURES

The proposed cryptosystem is a stream cipher algorithm based on logistic chaotic maps. The image encryption algorithm proposed in this paper consists of the following major steps:

- Step 1: First, image is transformed into matrix $I(i, j, 1 \rightarrow 3)$, ($1 \rightarrow R$, $2 \rightarrow G$ and $3 \rightarrow B$).
- Step 2: Each channel of image is transformed by discrete wavelet transform.
- Step 3: The Map (Eq (1)) is iterated 1000 times to avoid the transient effect using the initial condition $x0$, parameter of the elliptic functions k, and control parameter ®.
- Step 4: The result of 2^{rd} step is used to encrypt $I(i, j, 1)$ using the following equation

$$I(i, j, 1) = I(i, j, 1) + [\tilde{x}_f \ mod\ 256]$$

- Step 5: Then if matrix I is exhausted and K is equal to False, set K equal to true and matrix I equal to reverse values of matrix C and go to step 2, else if K is equal to True, transform the matrix C into $C_{n \times n}$ and output the cipher image.
- Step 6: Based on the initial conditions and amount of the control parameter, the keys then should be generated.
- Step 7: Steps 1 to 5 should be considered for each color mode.

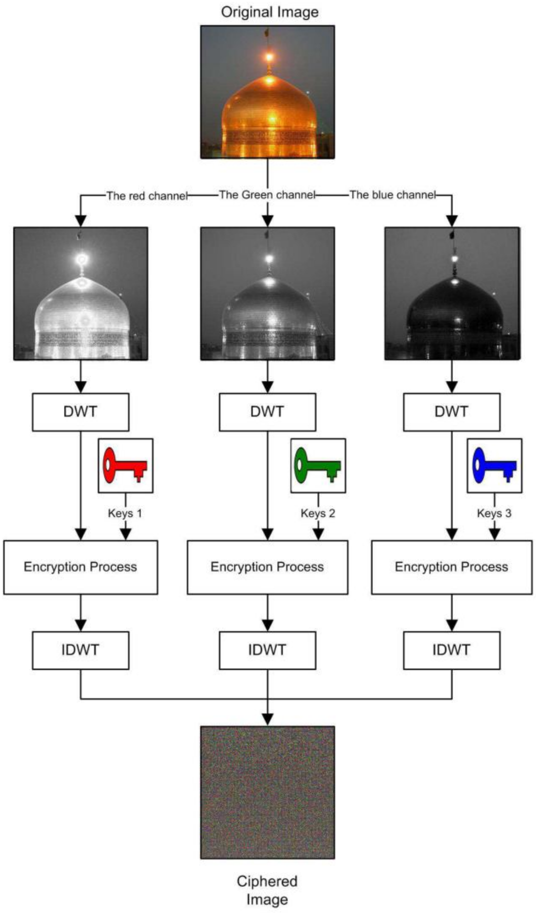

Figure. 3 Block Diagram.

In Fig (3) the block diagram of the proposed algorithm is presented. As the result of the control parameters of the chaotic maps are changed chaotically in each step, therefore the algorithm is so much sensitive to the plaintext and the keys, such that a very small change in the plain-image or the keys would lead to a totally different cipher-image. Since both decryption and encryption procedures have similar structure, they essentially have the same algorithmic complexity and time consumption. Fig (4) shows the flowchart of our proposed algorithm.

5. EXPERIMENTAL RESULTS

We provide some experimental results to illustrate the performance of the proposed chaotic cryptosystem. In order to test the efficiency of the proposed chaotic cryptographic scheme, we used the colored scale image "MASHHAD" with the size 512 × 512 pixels is used for this experiment (Fig. 5. a). The results of the encryption are presented in Fig. (5. b). As can be seen from the figures there is no patterns or shadows visible in the corresponding ciphertext. We have implemented the proposed algorithm using MATLAB programming language and observed the simulation results on a Pentium-IV 4.0 GHz with 2GB RAM and 300 GB hard-disk capacities. It seems that, encryption time in respect to the other cryptosystems such as is acceptable.

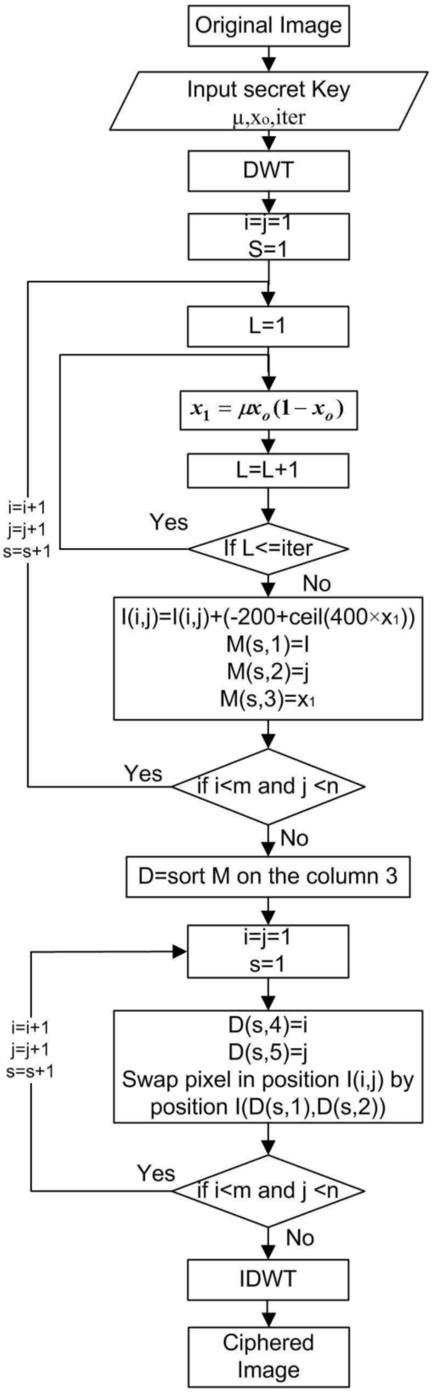

Figure. 4 Flowchart.

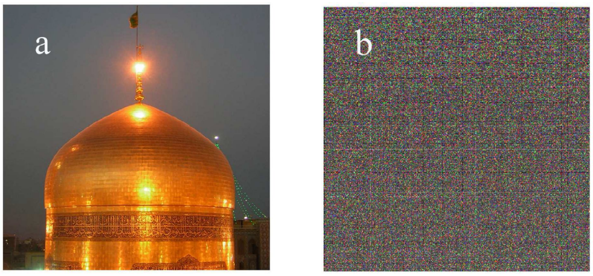

Figure. 5 (a) plain image (b) Cipher Image.

6. SECURITY ANALYS

When a new cryptosystem is proposed, it should always be accompanied by some security analysis. A good encryption procedure should be robust against all kinds of cryptanalytic, statistical and brute-force attacks. Here, some security analysis has been performed on the proposed scheme, including some important ones like key space analysis, statistical analysis, etc. The security analysis demonstrated the high security of the new scheme, as demonstrated in the following.

6.1 Statistical analysis

6.1.1 Histogram analysis

An image histogram illustrates that how pixels in an image are distributed by plotting the number of pixels at each color intensity level. By taking a (512×512) sized MASHHAD image as a plaintext, the histogram of the plaintext and corresponding ciphertext are shown in Fig(6-7).

We can see that the histograms of the original image and hence it does not provide any clue to employ any statistical analysis attack on the encryption image.

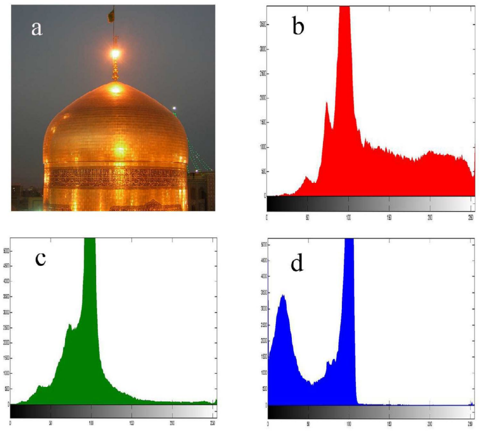

Figure. 6 The histogram of the plaintext(a) Plaintext (b) The red Channel (c) The green channel (d) The blue channel

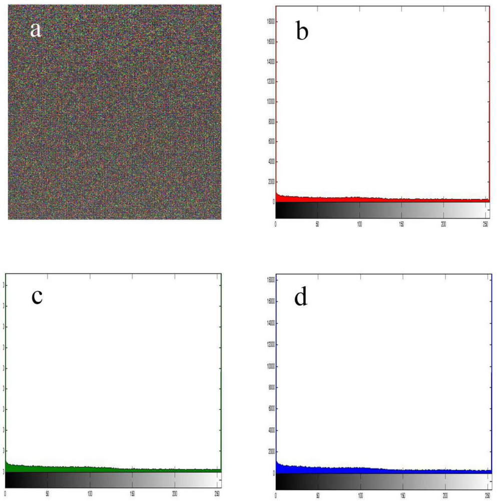

Figure. 7 The histogram of the Ciphertext: (a) Ciphertext (b) The red Channel (c) The green channel (d) The blue channel

6.1.2 Correlaton of two adjacent pixels

We have also analyzed the correlation between two vertically, two horizontally, and two diagonally adjacent pixels in MASHHAD cipher image.) To analyze the correlation of the adjacent pixels, we have used Eq. (7) to calculate the correlation coefficients in horizontal, vertical and diagonal directions [9]:

$$C_r = \frac{N\sum_{j=1}^{N}(x\times y)-\sum_{j=1}^{N}x_j\times\sum_{j=1}^{N}y_j}{(N\sum_{j=1}^{N}{x_j}^2-(\sum_{j=1}^{N}x_i)^2)\times(N\sum_{j=1}^{N}{y_j}^2-(\sum_{j=1}^{N}y_i)^2)} \qquad (2)$$

Where *xj* and *yj* are the value of the adjacent pixels in the image and N is the total number of pixels selected from the image for the calculation. We randomly choose 1000 image pixels in the plain image and the ciphered image respectively to calculate the correlation coefficients of the adjacent pixels in horizontal. The correlation coefficients of the adjacent pixels in vertical and in diagonal are calculated and listed in Table 1. It demonstrates that the encryption algorithm has covered up all the characters of the plain image and shows good performance of balanced 0 - 1 ratio.

Table 1: CORRELATION COEFFICIENT OF TWO ADJACENT PIXELS IN TWO IMAGES

Direction	Plain Image	Encrypted image
Horizontal	0.9110	0.0051
Vertical	0.9372	0.0046
Diagonal	0.9021	0.0074

6.2 Information entropy

The entropy (such as KS-entropy, information entropy) is the most outstanding feature of the randomness [10], [11] Information theory is a mathematical theory of data communication and storage founded in 1949 by Claude E. Shannon. To calculate the entropy *H(s)* of a source *s*, we have:

$$H(s)=\sum_{i=0}^{2N-1}P(s_i)\log_2\frac{1}{P(s_i)} \qquad (3)$$

Where *P*(*si*) represents the probability of symbol *si*. 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 entropy should ideally be 8. If the output of such a cipher emits symbols with an entropy of less than 8, then there exists a predictability which threatens its security. We have calculated the information entropy for encrypted image Fig. 2(b):

$$H(s)=\sum_{i=0}^{255}P(s_i)\log_2\frac{1}{P(s_i)}=7.53$$

The obtained value is very close to the theoretical value 8. Apparently, comparing it with the other existing algorithms, such as [12], the proposed algorithm is much more closer to the ideal situation. This means that information leakage in the encryption process is negligible, and so the encryption system is secure upon the entropy attack.

7. Plaintext Sensitivity Analysis (Differential Analysis)

In order to implement known plain text attack, chosen plaintext attack and more advanced adaptive chosen plaintext attack, an adversary attempts to make a slight change, usually one pixel, in the plain image and compare the cipher images (corresponding to very similar plain images and obtained by the same key) to extract some meaningful relationship between plain image and cipher image, which further facilitates in determining the secret key [13], [14].

Two common measures, NPCR and UACI, are used to test the influence of one-pixel change on the whole image encrypted by the proposed algorithm. NPCR stands for the number of pixels change rate while, one-pixel of plain image is changed. The unified average changing intensity (UACI) measures the average intensity of differences between the plain image and ciphered image. For calculation of NPCR and UACI, let us assume two ciphered images (*C*1 and *C*2) whose corresponding plain images have only one-pixel difference. The grey-scale values of the pixels of the ciphered image *C*1 and *C*2 at grid (i,j) are labeled as *C*1(i,j) and *C*2(i,j), respectively. Take a bipolar array, D, with the same size as image *C*1 or

*C*2. Then, D (i, j) is determined by *C*1 (i, j) and *C*2(i,j). So, if *C*1(i,j) = *C*2(i, j) then D(i,j) = 1; otherwise, D(i, j) = 0. NPCR and UACl are defined through the following formul as:

$$NPSR = \frac{\sum_{ij} D(i, j)}{W \times H} \times 100 \qquad (4)$$

$$UACI = \frac{1}{W \times H}\left[\sum_{j,j} \frac{c_1(i, j) - c_2(i, j)}{255}\right] \times 100\,\% \qquad (5)$$

Where W and H are the width and height of *C*1 or *C*2. We have done some tests on the proposed scheme (color image of size 512×512) to find out the extent of change produced by one-pixel change in the plain image. The results show that the proposed algorithm can survive differential attack. (See Table 2)

Table 2: PLAINTEXT SENSITIVITY ANALYSIS

Differential analysis	**Red**	**Blue**	**Green**
UACI	49.7%	58.1%	68.3%
UPCR	18.8%	19.6%	22.5%

8. CONCLUSION

In this paper, a new chaotic cryptosystem base on wavelet transform for color images has been proposed. The proposed cryptosystem has passed some basic common security tests. After these attacks, it is concluded that the lack of security, along with the low operation speed, may discourage the use of this scheme for secure applications.

References

[1] You Rong-Yi. Study on phase-space reconstruction of chaotic signal based on wavelet transform [J]. Acta Physica Sinica,2004,53(9):2882-2888.

[2] Nikolaids, Athanasios ,Asymptotically optimal detection for additive watermarking in the DCT and DWT domains[J].IEEE Transaction Image Processing,2003,12(5):563-571.

[3] Fridrich J, Bifur JI. Chaos 8 (6) (1998) 1259.

[4] Yen JC,Guo JI, A New Chaotic Key-Based Design for Image Encryption and Decryption, in: Proceedings IEEE International Conference on Circuits and Systems, vol. 4, 2000, pp. 4952.

[5] Li S,Zheng X, Cryptanalysis of a Chaotic Image Encryption Method,Scottsdale, AZ, USA, 2002, in: Proceedings IEEE International Symposium on Circuits and Systems, vol. 2, 2002, pp. 708711.

[6] Beldhouche F,Qidwai U, Binary Image Encoding Using 1D Chaotic Maps, in: IEEE Annual Technical Conference, 11 April 2003, pp. 3943.

[7] Mao Y,Chen G, Chaos-Based Image Encryption, Handbook of Computational Geometry for Pattern Recognition, Computer Vision, Neurocomputing and Robotics, Springer-Verlag, Berlin, 2003.

[8] Chen G,Mao Y,Chui C.k, Chaos Solitons Fractals 21 (2004) 749.

[9] Behnia S, Akhshani A, Mahmodi H, Akhavan A. Chaotic Cryptographic scheme based on composition maps. Int J Bifurct Chaos 2008;18:251-61.

[10] De Santis, A. F. Anna, Lisa. & Masucci, Barbara. [2006] secure key assignment schemes,” Discrete applied mathematics 154, 234-252.

[11] Li W. On the Relationship between Complexity and Entropy for markov Chains and Regular Languages. Complex Systems 1991;5:381-99.

[12] Behnia S, Akhshani A, Mahmodi H, Akhavan A. A novel algorithm for image encryption based on mixture of chaotic maps. Chaos, Solitons &Fractals 2008;35:408-19.

[13] Mao Y, Chen G, Lian S. A novel fast image encryption scheme based on 3D chaotic baker maps. Int J Bifurct Chaos 2004;14:3613-24.

[14] Bluman AG. Elementary statistics : a step by step approach. McGraw-Hill, Boston, 1997.