Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 8, Issue, 05, pp.31661-31664, May, 2016

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

ISSN: 0975-833X

RESEARCH ARTICLE

SENSITIVE ENCRYPTION USING KEY MATRIX WITH CHAOS SYSTEM

***Ilakkiya, A. and Dr. Pushpa Rani, M.**

Dept. of Computer Science, Mother Teresa Women's University, Madurai

ARTICLE INFO

Article History:
Received 23rd February, 2016
Received in revised form
25th March, 2016
Accepted 14th April, 2016
Published online 31st May, 2016

Key words:

Image compression, Encryption,
Arnold transform, Chaos system.

ABSTRACT

Recent developments of digital image production and applications have increases importance of digital image compression and security in today's world. The proposed method is developed to combine both compression and security of image. Compression is achieved by the removal of redundant data. Discrete Wavelet Transform (DWT) is a recently developed compression technique in image compression. The existing methods to encrypt images usually treat the whole matrix as the key which makes the key too large to distribute and memorize or store. To solve this problem, in this proposed method key controlled matrix is constructed using the logistic map and the Arnold transform is used for image location scrambling.

Citation: Ilakkiya, A. and Dr. Pushpa Rani, M. 2016. "Sensitive encryption using key matrix with chaos system", *International Journal of Current Research*, 8, (05), 31661-31664.

INTRODUCTION

During the last decade, the use of computer networks has grown enormously, and this growth continues unabated. Almost all networks are being installed, interconnected, and connected to the global internet. Through internet more and more information has been transmitted. The information is not only text, but also audio, image, and other multimedia. Image security has become an important topic in the current computer world. To solve those problems, the common method is image scrambling technology. In recent years, many researches of watermark preprocessing only confined to the location scrambling, and didn't guarantee the security. This paper puts forward an encryption algorithm combing Logistic chaos system and position scrambling system (Arnold transform), and reach a better effect. It can enhance the robustness of image encryption.

Compression

The goal of image compression is to reduce the amount of data required to represent a digital image to reduce the large storage capacity and transmission bandwidth. The Discrete wavelet transform (DWT) has gained widespread acceptance in signal processing and image compression.

****Corresponding author: Ilakkiya, A.***
Dept. of Computer Science, Mother Teresa Women's University, Madurai

The performance of discrete wavelet transforms based coding depends on the wavelet decomposition level and threshold value.

Threshold Coding Method

In level dependent threshold coding method, each transform coefficient is compared with a threshold. If it is smaller than the threshold then it is set to zero. If it is larger then it will be retained. Different threshold values for different decomposition level are used. By applying hard threshold the coefficients below this threshold level are zeroed, and the output after a hard threshold is applied and defined by this equation:

$$y_{hard}(t) = \begin{cases} x(t), |x(t)| > T \\ 0, other\ wise \end{cases} \quad \text{.....(1)}$$

Where x(t), the input signal and T is the threshold.

Logistic map

Chaos system is often used in cryptography due to its pseudo randomness and sensibility to the initial condition, the definition of Logistic map is

$$X_{n+1} = \mu X_n (1 - X_n),\ X_n \in (0,1) \quad \text{.....(2)}$$

It becomes chaotic when the parameter μ [3.57,4].

The proposed Image compression–encryption algorithm Chaos and Cryptography

The close relationship between chaos and cryptography makes chaos based cryptographic algorithms as a natural candidate for secure communication and cryptography chaos based encryption techniques are considered good for practical use as these techniques provide a good combination of speed, high security, complexity, reasonable computational overheads and computational power etc.

Characteristics on the chaotic maps

The characteristics of the chaotic maps have attracted the attention of cryptographers since it has many fundamental properties such as ergodicity, sensitivity to initial condition and system parameter, and mixing property, etc. Most properties are related to some requirements such as mixing and diffusion in the sense of cryptography. Therefore, chaotic cryptosystems have more useful and practical applications.

Logistic Map

The logistic map is a polynomial mapping (equivalently, recurrence relation) of degree 2, often cited as an archetypal example of how complex, chaotic behaviour can arise from very simple non-linear dynamical equations. The map was popularized in a seminal 1976 paper by the biologist Robert May, in part as a discrete-time demographic model analogous to the logistic equation first created by Pierre François Verhulst. Mathematically, the logistic map is written as:

$$X_{n+1} = r X_n\ 1 - X_n \quad \ldots\ldots\ldots\ldots\ldots\ldots(3)$$

where this nonlinear difference equation is intended to capture two effects.

- Reproduction where the population will increase at a rate proportional to the current population when the population size is small.
- Starvation (density-dependent mortality) where the growth rate will decrease at a rate proportional to the value obtained by taking the theoretical "carrying capacity" of the environment less the current population.

However, as a demographic model the logistic map has the pathological problem that some initial conditions and parameter values lead to negative population sizes. This problem does not appear in the older Ricker model, which also exhibits chaotic dynamics.

System Models

The system model contains 4 main modules.They are DWT, Key Matrix Generation, Arnold transform, Encrypted Image

DWT

A discrete wavelet transform is used to decompose the image.

KEY MATRIX GENERATION

Chaos system is used to create key matrix for encryption.

The Key matrix is constructed as a circulant matrix. The original row vector of the circulant matrix is controlled by the logistic chaos map. The steps are as follows

- A sequence with length 2N by logistic map with initial condition.
- X_{01} is generated; abandon the preceding N elements to obtain the sequence, which are used as the initial row vectors of the circulant matrices.
- The circulant matrix is constructed with the initial row vectors. To reduce the relevance among the column vectors, the first element of vector will be the result of multiplying by Λ, where 2 < i < M and Λ > 1, and the iteration:

$$\Phi\ i,1\ = \Lambda\ \Phi(i-1,N) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(4)$$
$$\Phi\ i,2{:}N\ = \Lambda\ \Phi(i-1,1{:}N-1) \quad \ldots\ldots\ldots\ldots\ldots(5)$$

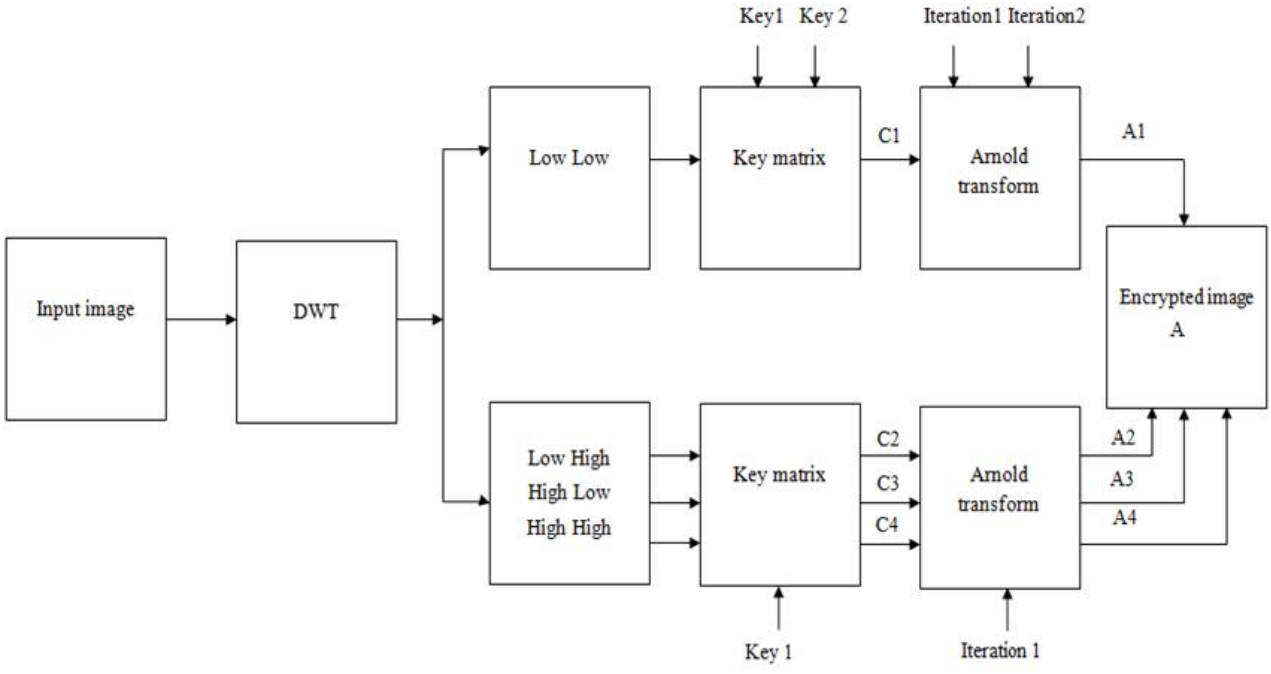


Fig. 1. Process of the encryption algorithm

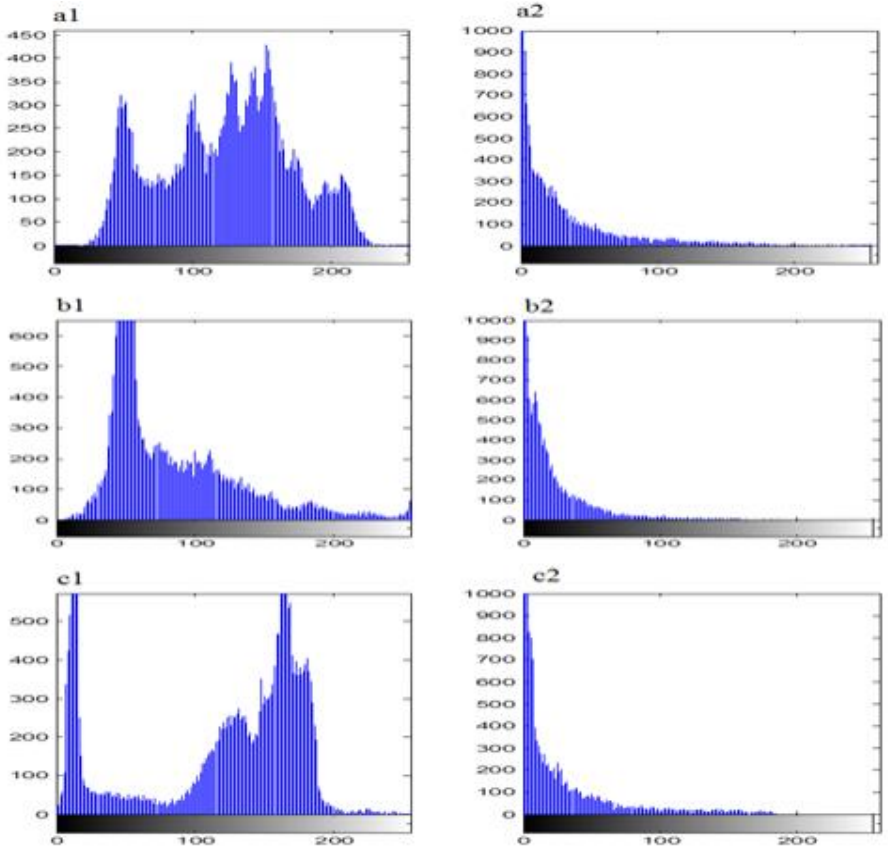
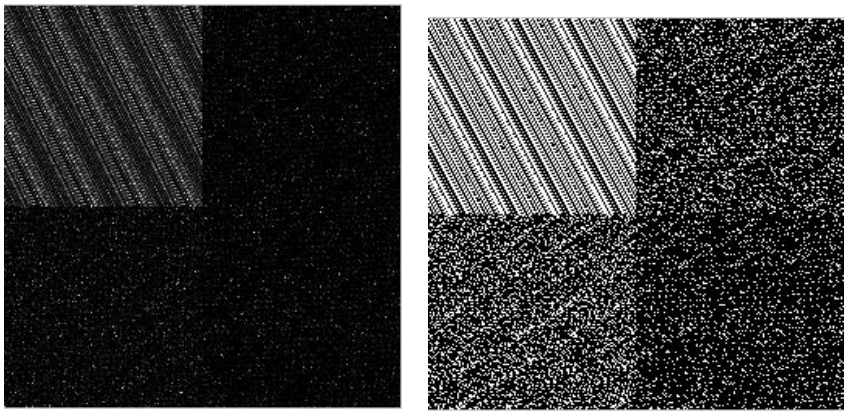


Fig. 2. Histogram: (a1) Lena; (a2) encrypted Lena; (b1) Cameraman; (b2) encrypted Cameraman; (c1) Peppers; and (c2) encrypted Peppers

(a) Input Lena image

(c) Encrypted image with key (x_{01} = 0.11 and x_{02} = 0.23)



(c) Encrypted image with key (x_{01} = 0.11 and x_{02} = 0.23 + 10^{-16})

(d) Difference between two encrypted images (b) and (c).

Fig. 2. Sensitivity of Chaos system

Arnold Transform

The pixels of the blocks are scrambled by Arnold transform.

EXPERIMENTAL ANALYSIS AND RESULTS

Histogram

The image histogram is often used to analyze the performance of the image encryption algorithm. It is the best when the values in the histogram of the encrypted image are fairly uniform in distribution or the second best when the histograms of different encrypted images are similar to each other. Fig. 5(a1), (b1) and (c1) are the histograms of Lena, Cameraman and Peppers, respectively. And Fig. 5(a2), (b2) and (c2) are the histograms of their encrypted images, correspondingly. The histograms of the two original images are obviously different from each other, while their encrypted images have similar histograms. After a large number of parallel experiments, shows that the histograms of the cipher texts of different original images are similar to Fig. 5(a2), (b2) and (c2). That is to say, the proposed algorithm can frustrate the statistical analysis attack.

Sensitivity Analysis

An ideal image encryption procedure should be sensitive with respect to both the secret key and plain image. The change of a single bit in either the secret key or plain image should produce a completely different encrypted image. To prove the robustness of the proposed method, we will perform sensitivity analysis with respect to both key and plain image.

Key Sensitivity Analysis

High key sensitivity is required by secure image cryptosystems, which means that the cipher image cannot be decrypted correctly although there is only a slight difference between encryption or decryption keys. This guarantees the security of the proposed method against brute-force attacks to some extent. For testing the key sensitivity of the proposed image encryption procedure, we have performed the following steps:

- An original image in Fig. (a) is encrypted by using the secret key x_{01} =0.11 and x_{02} = 0.23 and the resultant image is referred as encrypted image A as shown in Fig. (b).
- The same original image is encrypted by making the slight modification in the secret key i.e. x_{01} =0.11 and x_{02} = 0.23 + 10^{-16} and the resultant image is referred as encrypted image B as shown in Fig. (c).
- Finally, the difference between the encrypted images A, and B are compared is shown in Fig. (d).

It is clear that the encrypted images even though these have been produced by using slightly different secret keys. Key sensitivity analysis shows that changing one bit in encryption key will

Conclusion

By using the key controlled circulant matrix using chaos system, the proposed method is secure. By using Arnold transform the compressed and encrypted image is scrambled, the security is enhanced further. The proposed encryption algorithm combines both Arnold transformation and Logistic chaos system. The encrypted image is analysised from the histogram, the key sensitivity and the correlation of adjacent pixels, shows that the proposed method resist to different attacks. Since the algorithm used the number of Arnold transformation and the initial value of Logistic chaos system as the key, the key space is big, and have a strong sensitivity.

REFERENCES

Bhargava, B., Shi, C. and Wang, S. Y. 2004. “MPEG video encryption algorithms,” Multimedia Tools and Applications, vol. 24, no. 1, pp. 57–79.

Chu Hui Lee and Zheng Wei Zhou, 2012. “Comparison of Image Fusion based on DCT-STD and DWT-STD,” IMECS Vol I, March 14-15, Kong Kong.

Cohen, A. and Kovacevic, J. 1996. “Wavelets: the mathematical background,” Proceedings of the IEEE, vol. 84, no. 4, pp. 514–522.

Hennelly, B.M., Sheridan, J.T. 2003. Image encryption and the fractional Fourier trans-form. Proc SPIE – Int Soc Opt Eng, 5202:76–87

Karen Lees, 2002. “Image compression using Wavelets,” Report of M.S.

Locker Gnome, 2011, “Real World Application of Image Compression,” http://www.lockergnome.com/nexus/ windows/2006/12/25/real-world-applications-of- image compression/ [accesed 11 Dec 2011].

Lu, P., Xu, Z.Y., Lu, X., Liu, X.Y. 2013. “Digital image information encryption based on compressive sensing and double random-phase encoding technique.” *Optik-Int J Light Electron Opt*, 124:2514–8.

Nanrun Zhou, Aidi Zhang, Fen Zheng, Lihua Gong, 2014. “Novel image compression–encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing,” Optics & Laser Technology 62, 152–160.

Pavan Kumar Goswami, Namita Tiwari, Meenu Chawla, “Block Based Image Encryption Using Iterative Arnold Transformation,” *International Journal of Advanced Research in Computer Science and Software Engineering* 3(8), August - 2013, pp. 273-278

Pavan Kumar Goswami, Namita Tiwari, Meenu Chawla, “Block Based Image Encryption Using Iterative Arnold Transformation”, *International Journal of Advanced Research in Computer Science and Software Engineering* 3(8), August - 2013, pp. 273-278

Rafael, C. Gonzalez, Richard, E. Woods. 1992. Digital Image Processing (2nd edition), NJ:Prentice Hall

Swastik Das and Rashmi Ranjan Sethy, “A Thesis on Image Compression using Discrete Cosine Transform and Discrete Wavelet Transform,” Guided By: Prof. R. Baliarsingh, dept of Computer Science & Engineering, National Institute of Rourkela.

Takanori, N., Bahram, J. 2000. Optical encryption system with a binary key code. *Appl Opt*, 39:4783–7.

Wangsheng Fang1, Lulu Wu1,Rong Zhang1, 2012. “A Watermark Preprocessing Algorithm Based on Arnold Transformation and Logistic Chaotic Map,” Advanced Materials Research Vols. 341-342, pp 720-724

****