Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi

Pamukkale University Journal of Engineering Sciences

PAJES

CHAOTIC IMAGE ENCRYPTION WITH RANDOM SHUFFLING OF DATA

RASTGELE VERİ KARIŞTIRMAYA DAYALI KAOTİK ŞİFRELEME

Murat AYDOS[1*], *Alper UĞUR*[2]

[1]Computer Engineering Department, Engineering Faculty, Hacettepe University, 06800, Ankara.
maydos@hacettepe.edu.tr
[2]Computer Engineering Department, Engineering Faculty, Pamukkale University, 20070, Denizli.
augur@pau.edu.tr

Geliş Tarihi/Received: 03.08.2012, Kabul Tarihi/Accepted: 12.03.2013 doi: 10.5505/pajes.2014.18209
*Yazışılan yazar/Corresponding author

Özet

Kişisel resim albümlerindeki resimler, çoklu video konferanslara ait elektronik yayın kareleri gibi değerli medya içeriklerinin güvenliği resim şifreleme yöntemleri ile sağlanır. Bu içeriklerin güvenli iletimi hızlı, verimli ve pratik olmak zorundadır. Bu nedenle; resim şifreleme teknikleri seçilirken sadece güvenlik değil, aynı zamanda bahsi geçen özellikleri sağlayacak şekilde seçilmelidir. Klasik metin tabanlı bilgi şifreleme yöntemlerinin resim şifrelemedeki yetersizliği ve verimsizliği sebebi ile literatürde bu amaç için önerilmiş şifreleme algoritmaları mevcuttur. Bu şifreleme yöntemlerinin çoğu kaotik algoritmalara dayanır. Son zamanlarda bu konudaki çalışmalar çoğunlukla kaotik algoritmaların zayıflıklarına odaklanmıştır ve beraberinde karmaşık yapıda kaotik haritalar oluşmuştur. Bu çalışmada, basitlik ve verimlilik özelliklerini kaybetmeksizin kaotik şifreleme yöntemlerinin zafiyetlerini ortadan kaldırmaya yönelik tek boyutlu kaotik şifreleme sistemlerinde gerçekleşen bir öz-köşegen kaotik şifreleme algoritması önerilmektedir.

Anahtar kelimeler: Kriptografi, Şifreleme, Kaotik resim şifreleme, Öz-Köşegen karıştırıcı.

Abstract

Security of valuable multimedia contents such as images in personal photograph albums, electronic publishing, frames of multicast video conference can be achieved by image encryption. Secure transmission of these contents is required to be rapid, efficient and practical. Hence, image encryption process must be chosen not only to satisfy the security goals but also to fulfill these requirements. Due to the inadequacy and inefficiency of conventional text based information encryption methods, researchers have proposed several encryption schemes. Many of them are based on chaotic algorithms. Recently, the studies are concentrated on some weaknesses of chaotic algorithms and most of the presented solutions came up with complex structured chaotic maps. In this paper, we present a self-diagonal shuffler mechanism embedded to one dimensional chaotic encryption system to overcome its leak points while keeping simplicity and efficiency properties.

Keywords: Cryptography, Encryption, Chaotic image encryption, Self-diagonal shuffler.

1. Introduction

Image encryption is an effective process to provide secure transfer of valuable digital multimedia contents such as personal photograph album, video conference and electronic publishing over insecure networks. The term "secure" corresponds to two aspects; accessibility of legitimated user and confidentiality of digital content. Further, Shannon describes a system "secure" if the system has confusion and diffusion properties [1].

The image encryption process can be defined as invisible altering operation of the content under the scope of this term. Briefly, a proper image encryption scheme should satisfy features: simplicity, having low computational cost, support for large key space, easy key generation (i.e. asymmetric encryption key pairs), sensitivity to system parameters and initial conditions (avalanche property), confusion and diffusion (properties of ideal cipher), zero correlation between plain and cipher image, faultlessly reversible (no data loss), being practical (real-time image transfer over Internet).

Text based information encryption methods like DES, AES, RSA etc. are not convenient for real time image encryption. The methods deprive adequate confusion and diffusion properties between plain and cipher image pixels.

One of the solutions to satisfy these requirements is chaotic image encryption method. Chaotic properties such as ergodicity, quasi-randomness, sensitivity dependence on initial conditions and system parameters, topological transitivity motivated chaotic encryption as an alternative for traditional encryption methods [2].

The purpose of this paper is to design a new algorithm to handle all the requirements of a well enough image encryption process. In this work, we embedded a self-diagonal shuffle to one-dimensional chaotic system. This improvement provides not only simplicity but also has acceptable security level for applications. In addition, the self-diagonal shuffle puts a solution forward to window frame security weakness problem of multimedia contents.

The rest of the paper is organized as follows; in Section 2 we give a brief background information about chaotic image encryption. We propose a new chaotic image encryption algorithm with self-diagonal shuffler in Section 3. In Section 4, we present security analysis and experimental results. Finally, we conclude the paper with Section 5.

2. Background Information and Related Works

Chaos theory describes the behavior of certain nonlinear dynamical systems that under certain conditions exhibit a phenomenon known as chaos. The dynamical systems consist of a set of possible states, with a rule that determines the present state in terms of past states. The states described by chaotic maps have domain (input) space equal to their range (output) space. The complex structure and initial value dependency of chaotic systems make chaotic maps suitable for image encryption [3].

In order to transmit images over insecure channels, a variety of encryption processes have been proposed [5-17]. They could be classified into three major types: position permutation, value transformation and visual transformation [4]. Chaotic system based encryption is one of the branches of visual transformation type. There were several ideas using chaotic systems for both text and image encryption [9-17].

In 1998, chaos cryptography on text based encryption approach has been declared by Baptista, [9]. He encrypted a plain text with sequences of chaotic iterations based on a simply one dimensional chaotic map. In the same year, Fridrich, [10] used two dimensional standard Baker map for encryption purposes.

Baptista insisted on one-dimensional systems having advantages of computational efficiency and simplicity over other high-dimensional chaotic systems, whose dynamics reconstruction might be difficult. Successive researches exposed that some of the one-dimensional chaotic systems have drawbacks and leak points in security; therefore, these systems are not self-sufficient with regard to their small key space and low security level [11, 12].

Multi-dimensional chaotic cryptosystems have been proposed to be an alternative for one-dimensional chaotic cryptosystems; unfortunately, they have faced a tradeoff to satisfy security requirements or having simplicity and efficiency properties of one-dimensional chaotic cryptosystems.

Yen and Guo's BRIE, [13] is one of the proposed methods that strengthens one-dimensional chaotic systems; it is based on pseudo-random binary sequence controlled bit recirculation of pixels. Recently, in Gao, H. et al's [14] scheme used nonlinear chaotic map to overcome the major weaknesses . It satisfies uniform distribution property with structural parameters and initial value is used as encryption key in chaotic cryptosystem.

There are some other methods that use extra dimension as a solution to the problem. In 2004, Chen G. et al., [15] proposed a symmetric image encryption; a two-dimensional chaotic map is generalized to three-dimensional form to design a real-time secure image encryption scheme. This approach employs three-dimensional map to shuffle the position of image pixels and uses another chaotic map to confuse the relationship between the encrypted and its original image.

Afterwards, Gao, T. and Chen, Z., [16] proposed a new total shuffling algorithm differs from two-dimensional or three-dimensional chaotic cryptosystems. The algorithm uses a kind of shuffling matrix to shuffle the position of the pixels and the states by a combination of Lorenz and Chen's chaotic system.

In this section we briefly described background information and related works on chaotic image encryption. In the following section, we emphasize our approach to chaotic image encryption process.

3. Chaotic Image Encryption Algorithm with Self-Diagonal Shuffler

In this section we propose Chaotic Image Encryption Algorithm with Self-Diagonal Shuffler (CIEA-SDS), it is a one-dimensional chaotic map and a self-diagonal shuffle function that satisfies security, simplicity and efficiency.

3.1 Chaotic Map

CIEA-SDS is a symmetric image encryption algorithm using a simple one-dimensional logistic map. This chaotic map is formerly used by Baptista, [9] for encryption purposes.

Logistic map is defined as;

$$x_{n+1}=(x_n.\beta)(1-x_n). \tag{1}$$

Where $x_n \in(0,1)$ and $\beta\in(3.57, 4.0)$. The parameter β in the equation is the chaotic behavior control parameter. Between these intervals, the logistic map has chaotic system characteristics. The chaotic interval of logistic map can be seen obviously in Figure 1. It should be noted that, white vertical zones on the figure are also out of the chaotic interval.

The logistic map is used to generate encryption key, chaotic data sequence and initial diagonal of plain image.

3.2 Self-Diagonal Shuffler (SDS)

The two main purposes of self-diagonal shuffler (SDS) are to provide diffusion of cipher data and to increase the confusion level. SDS operates on diagonal sliced image data according to the coordinates which are determined from encryption key value.

The SDS procedure on plain image (for instance 250x250 Lena) is as follows;

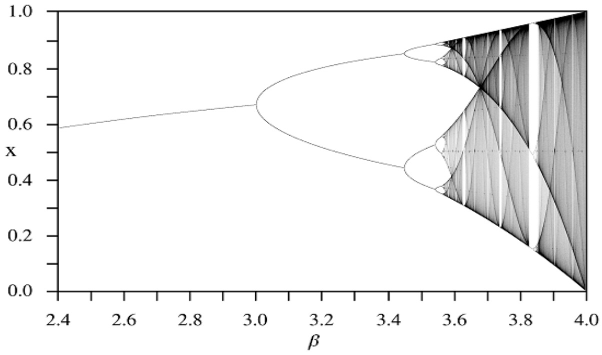


Figure 1. Logistic map.
(http://en.wikipedia.org/wiki/Logistic_map)

SDS firstly determines the initial coordinate (IC), and IC determines initial diagonal of the plain image. Then, with respect to initial diagonal, the plain image will be processed diagonally in counter-clockwise order.

The IC is calculated from chaotic map selected for encryption. As mentioned before, the logistic map is used in our scheme. The IC(x,y) is derived from the first 6 significant digits of x71 value. The modulo 250 of the first triple digit will be initial row coordinate (ICx) and the modulo 250 of the last triple digit will be initial column coordinate (ICy).

The IC(x,y) calculation is done only once for whole image encryption process.

The IC also determines the initial plain data block to be encrypted. The plain image is diagonally encrypted according to this reference point. To clarify the SDS, the encryption process is demonstrated in Figure 2.

IC(x,y) points to the pixel F. F'=Enc(F), F' will be the first pixel of cipher image. The following pixel K (the diagonal neighbor of F) will be the following pixel of cipher image. And the following pixel to be encrypted will be the pixel P (the diagonal neighbor of K) and so on. The diagonal encryption (SDS) will end when cipher image is done.

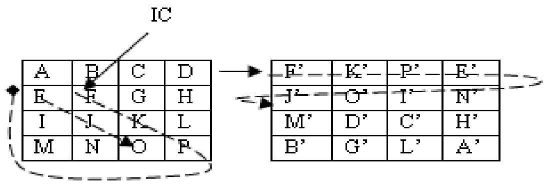


Figure 2. The SDS operation.

For the case IC (8, 83), the pixel at coordinate (8, 83) is encrypted and the (0, 0) coordinated pixel of cipher image is obtained. The coordinate of the following pixels will be (9, 84) and this will bring out the (0, 1) coordinated pixel of cipher image. This iteration will continue up to the encryption of (7, 82) coordinated pixel and will be completed at (249, 249) coordinated pixel of cipher image.

The decryption operation is quite similar to the encryption. After the IC calculation from the symmetric key, the cipher image will be decrypted row by row and the plain image is obtained diagonally from the IC. For the given example above, the (0, 0) coordinated pixel will be decrypted and plain image (8, 83) pixel will be obtained.

3.3 The Algorithm

The proposed algorithm is a symmetric encryption algorithm that uses the same key for encryption and decryption purposes. This section of the paper includes definition of the chaotic image encryption algorithm steps and its flow chart (Figure 3).

- Step 1: The logistic map parameters; β and x^0 compose the encryption key. Set encryption key from chaotic interval of logistic map.
- Step 2: Do 70 times of chaotic iteration (1) and obtain the decimal fraction x70.
- Step 3: If the encryption process is finished then go to step 6; otherwise call the chaotic iteration once. For example, the first occurrence of step 3,x71 double value will be generated. The algorithm uses only its first 15 significant digit.
- Step 4: Divide the 15 digits into five triple digits. The first and second triple digits are used for the SDS to calculate initial coordinates. For the remaining triple digits, Do mod 256 operations. At the end of the step 4, 3 bytes of chaotic data and the IC for the SDS are generated.
- Step 5: Do the XOR operation using the 3 bytes of chaotic data and 3 bytes of image data which is taken according to the SDS. At the end of step 5, 3 bytes of cipher image is generated.
- Step 6: Pass the encrypted image through the insecure network.
- Step 7: Pass the encryption key through the secure network.
- Step 8: End.

4 Application, Security Analysis and Comparison

In this section we present experimental results and analysis of the proposed algorithm. Statistical analysis, information entropy and correlation analysis, key space and the effects of using SDS to the security are discussed in details.

The E_{key} = (α, x_0) = (3.9999995, 0.987654321012345), encryption key pair is used. In key sensitivity analysis, x_0'=0.987654321012346 value is used for wrong encryption key pair (Figure 4).

The performed experiments were done on 1.70 GHz Intel Pentium (IV), 512 MB memory and 40 GB HDD capacities.

It can be seen from Figure 4, decrypted image is clear and decryption performed without any corruption. It also presents the key sensitivity; the minor change in decryption key causes major difference on the decrypted image.

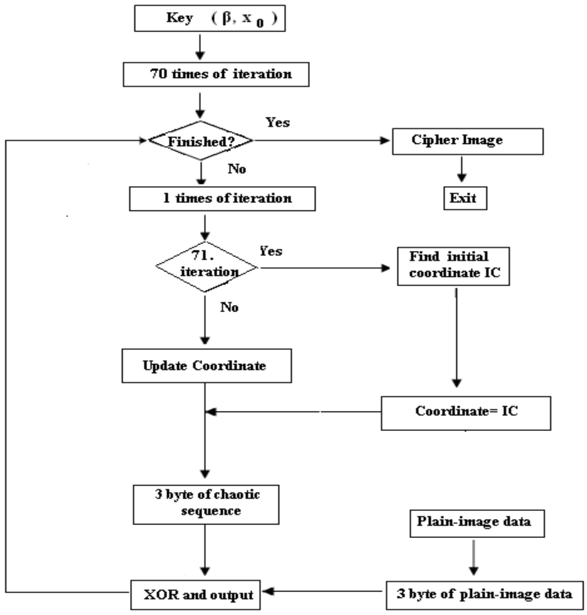
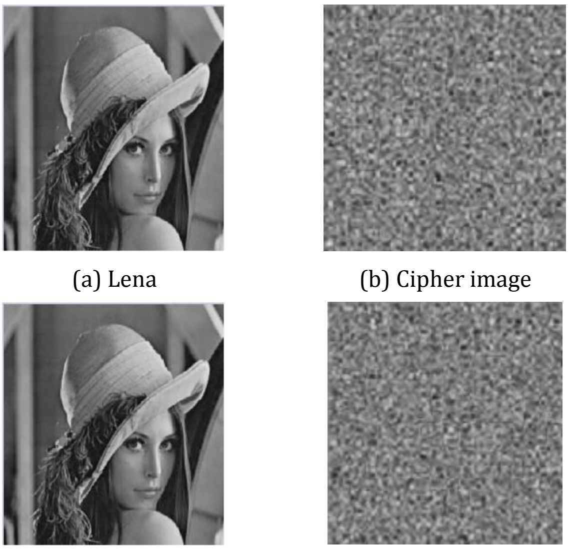


Figure 3. Flow-chart of the algorithm.



(a) Lena

(b) Cipher image

(c) Decyrpted image

(d) Decrypted image with wrongkey (x0')

Figure 4. CIEA-SDS Encryption process and key sensitivity on Lena image.

4.1 Statistical analysis

The proposed algorithm provides uniformity distribution property for the diffusion effect. Statistical analysis on plain image and cipher image histograms are demonstrated in Figure 5.

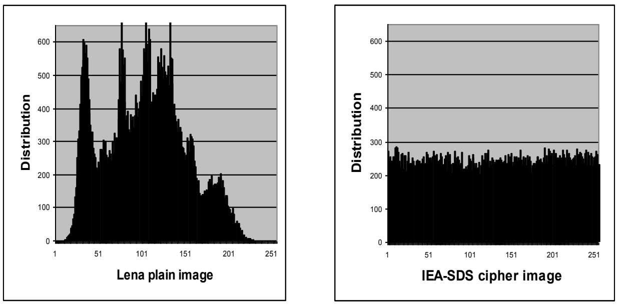


Figure 5. Histograms of image data.

4.2 Information entropy

Shannon [1], defined entropy value as a measure of the average information content associated with a random outcome. The entropy H (m) of an information set m is;

$$H(m) = \sum_{i=0}^{2N-1} P(m_i)\log_2 \frac{1}{P(m_i)} . \qquad (2)$$

P (mᵢ): probability of m_i, N: number of information set.

The entropy H(m) will be 8.0 when 2^8 distinct information have same probability of existence in source sets. The 8.0 value is the optimal value of information entropy, corresponding truly random source. At the end of the encryption process; information set entropy should be close to this optimal value. The larger distance of entropy to the optimal value 8.0 causes weak security as it increases predictability of the plain image from cipher image.

In case of entropy being less than 8, predictability of the plain image from the cipher image will increase and threat the security [1, 11].

The entropy value of CIEA-SDS on Lena cipher image is 7. 99676, which is very close to the optimal value. So that this quite small information leakage in the encryption process is negligible and the process is supposed to be robust against the entropy attacks.

4.3 Correlation analysis of Two Adjacent Pixels

To avoid statistical cryptanalysis of the cipher image, the proposed algorithm is examined under correlation tests. This test is done with randomly selected 1000 pairs of two adjacent vertical, horizontal and diagonal pixels from plain image and cipher image and the results are given in Figure 6.

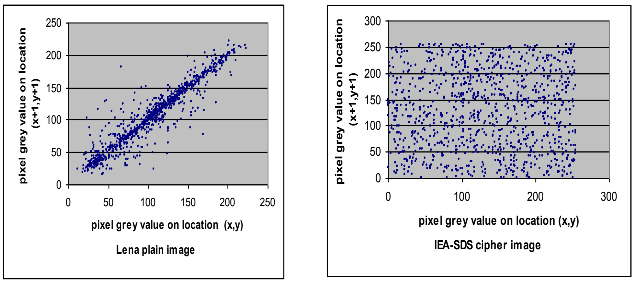


Figure 6. The correlation analysis of the two diagonally adjacent pixels images.

Correlation coefficients may change between -1 and 1. If there is strong relationship between the adjacent values, the correlation coefficient tends to be 1, and if there is no relationship between the adjacent values, the correlation coefficient is 0 or very low. To make sense, crosscheck of the corresponding correlation coefficients with Gao H. et al., [10] is also given in Table 1.

As mentioned in Section II, Gao, H. et al used a nonlinear chaotic map as;

$$x_{n+1} = \lambda . tg(\alpha . x_n).(1- x_n)\ \beta, \quad x_n\ (0,1),\ n = 0,1,2,... \qquad (3)$$

to satisfy uniform distribution property. It is clear that embedded SDS provides a qualitative distribution on cipher image with simpler chaotic map (1).

Table 1. Correlation coefficients of two adjacent pixels in two images.

	Lena image	Gao H. et al. cipher image	CIEA-SDS cipher image
Horizontal	0,9731	-0,01589	-0,01293
Vertical	0,9610	-0,06538	-0,0033
Diagonal	0,9308	-0,03231	-0,06128

The entropy and correlation analysis are also done on number of images of the USC-SIPI image database to confirm the robustness. A sample subset is given in Table 2. The encryption has been done using the secret key 0.987654321012345. Results of experiments suggest that entropy values are not far away from optimal value and the adjacent pixels on cipher image are distributed fairly.

Table 2. Sample subset of encryption scheme analysis done with 256x256 USC-SIPI images.

File name	Entropy	Correlation Coefficients
4.1.01	7.99645	0.003624
4.1.02	7.99651	0.005921
4.1.03	7.99592	-0.00372
4.1.04	7.99692	0.034011
4.1.05	7.99670	-0.00582
4.1.06	7.99677	0.01366

4.4 Key Space

The key space of the algorithm is limited to the defined intervals on the domain given in the previous section. The encryption key must be chosen between these chaotic intervals.

The iterative structure of the chaotic encryption algorithms-the number of chaotic iterations-also affects the number of possible encryption keys. The key space depends on the chosen chaotic map. As the small key space of the logistic map, the number of chaotic iteration on proposed algorithm is reduced to use the key space effectively. The algorithm is designed to allow different chaotic maps.

4.5 The effect of self-diagonal shuffler to the security

The chaotic interval sensitivity of secure encryption key is another important subject in chaotic encryption systems. The experiments to determine encryption key present that chosen key may not satisfy chaotic properties and desired security level [17].

Self-diagonal shuffler (SDS) provides partial security level to the presence of this problem in chaotic image encryption schemes. The effect of SDS embedded to a simple iterative chaotic encryption algorithm is obvious from Figure 7.

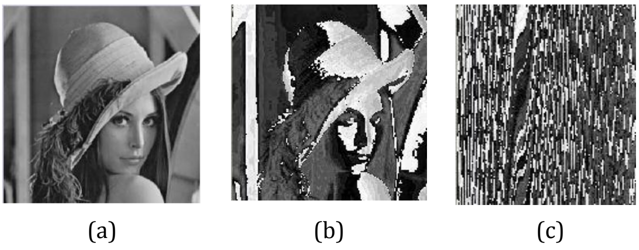


Figure 2. The weak key effect on plain image (a), (b) presents effect of simple chaotic encryption algorithm with E key (1.1, X0), (c) presents CIEA-SDS effect with same key.

As mentioned before, image encryption algorithm might provide a cipher image with minimal disclosure of information about plain image. Similar consecutive pixel blocks are not rare on delivered multimedia, and especially video streams occasionally have same plain window frame. These recurrent data blocks may expose information for encryption key and cipher image with plain image attacks. Adapting SDS mechanism will serve to the encryption algorithm by providing an average level of diffusion. In Figure 8, blank image with window frame and the SDS effect are given.

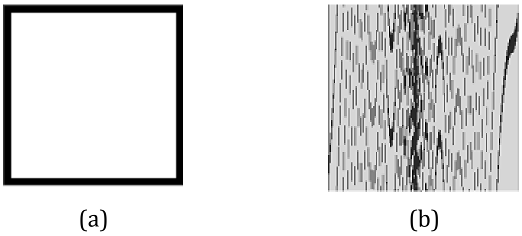


Figure 3. (a) Blank image with window frame;
(b) SDS effect on the frame.

The diffusion of the frame-recurrent data block-is obvious. It can be seen from correlation coefficients given in Table 2; SDS has positive effect on correlations of adjacent pixels. Although SDS enforcement slightly differs at horizontal adjacent pixels for the blank image, the vertical and diagonal correlation coefficient results are remarkable.

Table 3. Correlation coefficients of blank image and SDS effect.

	Blank image with window frame	SDS enforced image
Horizontal	0,945412	0,939174
Vertical	0,965323	0,063798
Diagonal	0,909794	0,09204

5 Conclusion

This paper has discussed on the improvement of one-dimensional chaotic map image encryption process. In spite of their computational efficiency and simplicity properties meeting fundamental requirements of image encryption, one-dimensional chaotic system is not self-sufficient with regard to its small key space and low security level in image encryption process.

The proposed algorithm CIEA-SDS is based on a one-dimensional chaotic map called logistic map. The logistic map has simple and practical structure with sensitivity to system parameters and initial conditions.

The key space weakness of logistic map is considered and number of chaotic iteration in CIEA-SDS is minimized without any compromise in security issues.

Information entropy and statistical analysis emphasized that CIEA-SDS provides zero correlation between plain image and cipher image.

Consequently, analysis clearly illustrate that CIEA-SDS is an appropriate algorithm for the secure image transmission.

6 References

[1] Shannon, C.E., Communication theory of secrecy systems, Bell Syst. Tech. J. Vol. 28, 1949.

[2] Wok, H.S.K., Tang, W.K.S., A fast image encryption system based on chaotic maps with finite precision representation, Chaos, Solitons & Fractals, V. 32, 1518-1529, 2007.

[3] Devaney, R.L., An Introduction to Caotic Dynamical Systems, Westview Press, 2003.

[4] Öztürk, İ., Soğukpınar, İ., Analysis and Comparison of Image Encryption Algorithms, International Journal of Information Technology, Vol. 1. No. 2, 108-111, 2004.

[5] Yen, Jiu-Cheng, and Guo, Jiu-In., "A new image encryption system and its VLSI architecture," IEEE Workshop on Signal Processing Systems, Taipei, pp. 430-437, 1999.

[6] Lian, S., Sun, J., Zhang, D. and. Wang, Z., "A selective image encryption scheme based on JPEG2000 Codec," in Proc. 2004 Pacific-Rim Conf. on Multimedia, in Springer Lecture notes in Computer Science, Vol. 3332, pp. 65–72, 2004.

[7] Lian, S., Sun, J., Wang, Z., "A Novel Image Encryption Scheme Based-on JPEG Encoding." IV . 217-220, 2004.

[8] Bourbakis, N. and Alexopoulos, C., "Picture Data Encryption Using SCAN Pattern," Pattern Recognization, Vol. 25, No. 6, pp. 567-581, 1992.

[9] Baptista, M.S., Cryptography with chaos. Physics. Letters. A Vol. 240, 1998.

[10] Fridrich, J., Symmetric ciphers based on two-dimensional chaotic maps, Int. J. Bifurcation and Chaos, Vol. 8, No. 6, 1259-1284, 1998.

[11] Wong, K. W., A fast chaotic cryptographic scheme with dynamic look-up table, Physics. Letters. A Volume 298, 234-242, 2002.

[12] Xiang, T., Liao, X., Tang, G., Chen, Y. and Wong, K.W., A novel block cryptosystem based on iterating a chaotic map, Physics Letters A, Volume 349, Issues 1-4, 2006.

[13] Yen, J.C., Guo, J.I., "An efficient hierarchical chaotic image encryption algorithm and its VLSI realization", IEE Proc. Vis. Image Process. 147, 167-175, 2000.

[14] Gao, H., Zhang, Y., Liang, S., and Li, D., A new chaotic algorithm for image encryption, Chaos, Solitons & Fractals, Vol. 29, Issue 2, 2006.

[15] Chen, G., Mao, Y., Chui, C.K., A symmetric image encryption based on 3D chaotic maps, Chaos, Solitons & Fractals, Vol. 21, 749-761, 2004.

[16] Gao, T., Chen, Z., Image encryption based on a new total shuffling algorithm, Chaos, Sol&Frac, 2007.

[17] Behnia, S., Akhshani, A., Mahmodi, H., Akhavan, A., A novel algorithm for image encryption based on mixture of chaotic maps, Chaos, Sol&Frac, 2006.