AENSI Journals

Advances in Environmental Biology

ISSN-1995-0756 EISSN-1998-1066

Journal home page: http://www.aensiweb.com/AEB/

An Efficient Fingerprint Image Encryption Algorithm

[1]Hossein Malekinezhad and [2]Hossein Ebrahimpour-Komleh

[1] PhD student, University of Kashan
[2]Faculty Member, University of Kashan

ARTICLE INFO

Article history:
Received 15 April 2014
Received in revised form 22 May 2014
Accepted 25 May 2014
Available online 15 June 2014

Keywords:
Image Encryption, Block Permutation, Wavelet Transform, Fingerprint Image

ABSTRACT

In this paper, we propose a fingerprint image encryption algorithm based on permutation and diffusion operations in wavelet domain in order to enhance the protection of fingerprint-based systems against replay attacks. These attacks have been identified and located in different points by Ratha *et al*. First, one-level Lifting Wavelet Transform Integer-to-Integer is performed to the original fingerprint image. The approximation and details sub-bands are then partitioned into blocks and permuted using a permutation key. After that, for each sub-band the Rubik's cube principle presented in (Loukhaoukha *et al*., 2012) is applied. Then, the values of rows and columns of the modified sub-bands are changed using XOR operator. Finally, the encrypted image is constructed by ordering the encrypted sub-bands. Experimental tests and security analysis have been carried out on three fingerprint images, taken from Fingerprint Verification Competition, "FVC 2000" database. The obtained results clearly show the robustness of the proposed encryption algorithm against common attacks, namely exhaustive, differential and statistical attacks and also reveal the high security level achieved by the proposed algorithm.

To Cite This Article: Hossein Malekinezhad and Hossein Ebrahimpour-Komleh., An Efficient Fingerprint Image Encryption Algorithm. ***Adv. Environ. Biol., 8(11),*** *1232-1238, 2014*

INTRODUCTION

Our society is becoming increasingly dependent on new technologies such as computers and mobiles. However, the use of these technologies may not be safe unless they are equipped with reliable authentication mechanisms in order to ensure that only authorized persons are allowed to access and use these technologies. Usually, authentication is achieved through some information such as passwords or PINs (knowledge-based) or some possessed means such as ID cards or badges (token-based). However, these ways are not sufficient to reliably authenticate persons especially with the use of more sophisticated tricks by hackers to overpass these traditional means. Recently, biometrics, which means the use of physiological or behavioral traits of a person to confirm his identity, has been introduced in many applications. This increasing interest in biometrics is justified by the fact that the uniqueness of an individual arises from his physiological or behavioral characteristics such as fingerprint, retinal and iris scanning, hand geometry and facial recognition with no passwords or numbers to remember (Jain *et al*., 2005). Among biometric systems, fingerprint systems are the most mature, extensively studied and widely deployed biometric systems because of their easy access, low price sensors and relatively good performance (Wu. C., 2007). Also, fingerprints are considered legitimate proofs of evidence in courts of law all over the world.

As with many interesting and powerful development of technology, there are concerns about fingerprint systems (biometric systems, in general). The biggest concern is the security aspect, where the overall reliability of the system is meant here, rather than the authentication/identification results accuracy. Several researchers show the existence of many threats and attacks that may affect the security and the integrity of biometric-based systems (Ratha *et al*., 2001), (Maltoni *et al*., 2003), (Uludag *et al*., 2004). The problems that may arise from the attacks on such systems are raising concerns as more and more biometric systems are deployed. Image encryption algorithms are possible solutions that can be used to increase the security of the fingerprint images (biometric data, in general).

In this paper, an efficient image encryption algorithm with the architecture of combining permutation and diffusion is proposed, in order to enhance the security of fingerprint-based systems against replay attacks. First,

Corresponding Author: Hossein Malekinezhad, PhD student, University of Kashan
E-mail: hmalekinezhad@grad.kashanu.ac.ir

one-level Lifting Wavelet Transform Integer-to-Integer is performed to original image. The approximation and details sub-bands are then partitioned into blocks of size L x L, which are permuted using a permutation key. After that, for each sub-band the Rubik's cube principle presented in (Loukhaoukha *et al*., 2012) is applied. Then, the XOR operator is applied separately for rows and columns of the modified sub-bands. Finally, the encrypted image is constructed by the encrypted sub-bands. Experiments were carried out on three fingerprint images taken from Fingerprint Verification Competition,"FVC2000" database. The obtained results show that the proposed algorithm is very robust to common attacks and achieves a high security level. The paper is organized as follows: Section II presents an overview of biometric image encryption schemes. In section III, the possible points in biometric systems where attacks may occur are briefly described. The proposed image encryption algorithm for fingerprint images is explained in section IV. Experiments were carried out in section V to evaluate the robustness of the proposed algorithm. The security analysis is provided in section VI. Finally, conclusions are drawn in section VII.

Related Works:

In recent years, a number of image encryption schemes have been proposed to secure biometric systems (Han *et al*., 2007), (Khan *et al*., 2007), (Alghamdi and Ullah, 2010), (Delong, 2010). In the case of fingerprint, Han *et al*. [10] have proposed a chaotic fingerprint image encryption approach. Their proposed approach consists in encrypting fingerprint images using a chaotic sequence obtained from multi-scroll chaotic attractors, where their initial values serve as private keys and are generated from the pixel distribution of the binary images of the captured fingerprints. However, the robustness of their cryptosystem have not been evaluated against exhaustive, differential and statistical attacks. Khan and Zhang [11] have proposed a fingerprint image encrypted system based on Fractional

Fourier transform to thwart the risks of non-liveness and retransmission of biometric image by an attacker.

Their proposed cryptosystem has not been tested against differential attacks and the performance of the encryption scheme has not been done. Recently, (Delong, 2010) has proposed a new fingerprint image encrypted based on chaotic system and Fractional Fourier transform. First, the fingerprint is encrypted using Fractional Fourier, then the confusion fingerprint is encrypted by using confusion matrix which is generated by chaotic system, and finally the encrypted fingerprint is obtained. However, no analysis against exhaustive and differential attacks has been provided.

Attacks On Biometric Systems:

Biometric systems are increasingly used in applications that need to verify or determine the identity of an individual. These systems have some advantages over traditional ones, especially the difficulty to copy, share, guess or regenerate biometric traits. Despite these advantages, biometric systems are vulnerable to specific attacks that can degrade their functionalities. Ratha *et al*. have identified eight possible points in a biometric system where attacks may occur. These attacks are illustrates in figure 1.

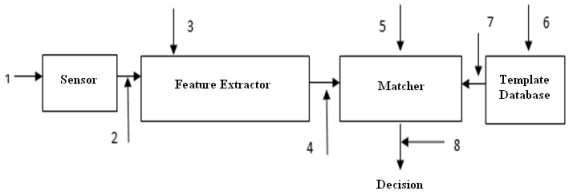


Fig. 1: Locations of possible attacks in a biometric system.

Tampering the presented biometric data (point 1): in this type of attacks, called also spoof attacks, a reproduction of the biometric trait is presented to the sensor. For examples, a presentation of a signature copy or a face mask.

Tampering with the transmitted biometric data (point 2): in this type of attacks, a previously intercepted genuine biometric data is replayed in the system without using the biometric sensor, such as the presentation of an old copy of a fingerprint image or the presentation of a previously recorded audio signal.

Attack on the features extraction module (point 3): in this attack, the features extraction module is replaced by a Trojan horse program that produces information chosen by the attacker. This attack is also known as substitution attack.

Tampering with the extracted features (point 4): in this attack, the data obtained by the extraction module are altered or replaced by other data, specified by the attacker. However, in practice, applying this attack is extremely difficult since the steps of the extraction parameters and similarity test are often inseparable.

Attack on the matcher module (point 5): in this type of attacks, an attacker replaces the matcher module by a Trojan horse program that generates a preselected score.

Alteration of the stored templates (point 6): biometric templates are stored either locally (smartcards) or remotely (central database). In this type of attacks, an attacker try to add, modify or remove one or more stored templates. And this may result in either authorizing access to an attacker or denying service to genuine users. For example, the template stored in the smart card and presented to the authentication system, is particularly vulnerable to this type of attacks.

Tampering with the transmitted templates (point 7): in this kind of attacks, the transmitted templates could be intercepted and altered by an attacker.

Alteration of decisions (point 8): in this type of attacks, the final decision (yes or no) is altered. The risk of this attack is high because even if the system is a high authentication performance, it becomes useless by this type of attacks.It is worth mentioning that attacks at points 2, 4, 7 and 8 are also referred to as replay attack. In the literature, several security techniques have been proposed to thwart these attacks. For instance, some physical properties such as blood pressure or conductivity can be exploited to thwart simple attacks at the sensor. To secure the biometric system against attacks at points 5, 6, and 7, it has been proposed to have the matcher and the template database reside at a secure location. Cryptography has also been proposed to prevent replay attacks, i.e. attacks held at points 2, 4, 7 and 8.

Image Encryption Algorithm:

The proposed image encryption algorithm that operates in the wavelet domain, is based on blocks permutation and Rubik's cube principle. Let I be a gray-scale fingerprint image of size M x N, in which the pixels values range from 0 to 255. The image encryption process comprises the following steps:

1) Apply one-level Lifting Wavelet Transform Integer-to-Integer to decompose the image I into four sub-bands (i.e. LL, LH, HL and HH).
2) Generate randomly the column vector K_R and row vector K_C of length L.
3) For each sub-band *SB* where *SB* $\in$ {LL, LH, HL, HH } :

a) Divide the sub-band SB into blocks of size L x L.
b) Permute all the sub-band blocks by using a permutation key P_{SB}.
c) For each block k of the sub-band SB:
i) Compute the sum of all elements in the row i, denoted by $\Sigma_{Row(i)}$.
ii) Row i is right circular shifted by $K_R(i)$ positions if $\Sigma_{Row(i)}$ Modulo 2 is equal to 0, otherwise, the row i is left circular shifted by the same position.
iii) Compute the sum of all elements in the column j, denoted by $\Sigma_{column(j)}$.
iv) Column j is up circular shifted by $K_C(j)$ positions if $\Sigma_{column(j)}$ Modulo 2 is equal to 0, otherwise, the column j is down circular shifted by the same position.
d) The steps 3a, 3b and 3c are the confusion process, which are repeated for n_1 rounds for sub-band LL to produce modified sub-band, denoted by m_{LL} and n_2 rounds for LH, HL and HH sub-bands to get the modified sub-bands, denoted by m_{LH}, m_{HL}, and m_{HH} respectively.
4) For each block *k* of a modified sub-band m_{SB}, where $m_{SB} \in \{m_{LL}, m_{LH}, m_{HL}, m_{HH}\}$:
a) Apply the bitwise XOR operator to each row with the vector K_C according to following rule:
$m_{SB1}(2i - 1, j) = m_{SB}(2i - 1, j)$ XOR with $K_C(j)$,
$m_{SB1}(2i , j) = m_{SB}(2i - 1, j)$ XOR with $K_{C1}(j)$.
b) Using vector K_R, the bitwise XOR operator is applied to each column of the matrix m_{SB1} according to following rule:
$m_{SB2}(2i - 1, j) = m_{SB1}(2i - 1, j)$ XOR with $K_R(j)$,
$m_{SB2}(2i , j) = m_{SB1}(2i - 1, j)$ XOR with $K_{R1}(j)$.

Note that, K_{C1} and K_{R1} are obtained by flipping the vector K_C left to right and flipping the vector K_R up to down, respectively.

5) The steps 3 and 4 are repeated *m* rounds.
6) The encrypted image I_E is constructed by grouping and ordering the encrypted sub-bands.

The decryption stage is the inverse process of the above steps. The encrypted image IE is firstly divided into four sub-bans, which correspond to the encrypted sub-bands. Next, each sub-band is divided into blocks of size LxL. After that, for each block the steps 4b and 4a are applied to get the modified sub-band mSB, respectively. Then, the steps 3(c)iii, 3(c)iv, 3(c)i and 3(c)ii are applied successively to the modified sub-band mSB. After that, each decrypted sub-band is rearranged according the permutation key PSB. Finally, the one-level inverse Lifting Wavelet Transform Integer-to-Integer is performed to get the original image.

Experimental Results:

To demonstrate the efficiency and the security of the proposed image encryption algorithm, a number of tests have been carried out, using three real fingerprint images of size 448 x 480, presented in figure 2, which have been randomly selected from Fingerprint Verification Competition "FVC 2000, DB3" database.

(a) Image 22_6 (b) Image 46_2 (c) Image 88_1

Fig. 2: Original Images.

As a general requirement for image encryption scheme, the encrypted image must be almost totally different from its original form. In general, two measures are used to quantify this difference. The first one is the number of pixels change rate (NPCR), which indicates the percentage of different pixels between two images. The second one is the unified average changing intensity (UACI), which measures the average intensity of differences pixels between two images [14]. Let I be the original image and IE be its encrypted version, both images are of size M x N and let I (i , j) and IE(i , j) be the pixels values of the original and the encrypted images at location (i , j), respectively. The above mentioned measures are defined by the following equations:

$$NPCR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)}{M \times N} \times 100\%$$

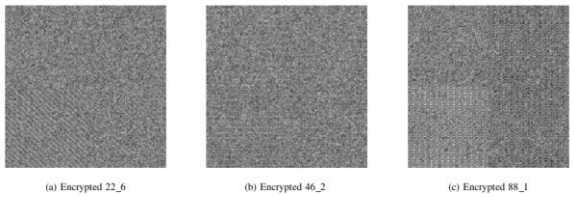
$$\text{with : } D(i,j) = \begin{cases} 0 & \text{if} \quad I(i,j) = I_E(i,j) \\ 1 & \text{otherwise.} \end{cases}$$

$$UACI = \left[\sum_{i=1}^{M}\sum_{j=1}^{N} \frac{|I(i,j) - I_E(i,j)|}{255}\right] \times \frac{100\%}{M \times N}$$

To build a near ideal image encryption algorithm, NPCR values must be greater than 99% and UACI values must be around 33%. Table 1 gives the NPCR and UACI values for the original images and their encrypted versions, which are presented in figure 3. As can be seen, the obtained NPCR values are above 99.6% for all test images and these values clearly show that the pixels positions have been randomly changed. Also, we can say that the obtained UACI values are within an acceptable range.

Table 1: Difference measures between original and encrypted images.

Image	NPCR (in %)	UACI (in %)
Image 22_6	99.61	31.30
Image 46_2	99.60	31.50
Image 88_1	99.65	31.94



(a) Encrypted 22_6 (b) Encrypted 46_2 (c) Encrypted 88_1

Fig. 3: Encrypted Images of Figure 2.

Security Analysis:

An ideal cryptosystem should resist to all kinds of known attacks, especially exhaustive, differential and statistical attacks. In the following, an analysis of the performance of the proposed algorithm against the above mentioned attacks is provided.

A. Exhaustive attack:

1) Key space analysis: To obtain an image encryption scheme with a high security level, the key space should be large enough to make any exhaustive attack ineffective. The key space involves the confusion and diffusion processes. The proposed encryption algorithm uses the following parameters: initial value L and secret keys: KR, KC, PSB, m, n1 and n2. In our simulation, these parameters are set as follows: L = 16, KR and KC are integer vectors of size L = 16 having values between 0 and 255, so the key space SKR = SKC= 25516. PSB is a vector of size 225, so its key space SPSB is equal to 225!. Iteration round m and confusion round n1 for LL sub-band are equal to 2 and confusion round n2 for other sub-bands is set to one. Thus, the total key space, without considering SPSB, is $S = SKR \times SKC \times m \times n1 \times n2 \approx 1039$.

As suggested by (Alvarez and Li, 2006), the key space must be greater than 2100. In order to obtain sufficient security against exhaustive attack. This requirement is respected in our cryptosystem.

Key sensitivity analysis: A good image encryption scheme should have a high key sensitivity, which means that a slight modification in encryption or decryption keys should lead to a completely different encrypted or decrypted images. In order to illustrate the key sensitivity of the proposed algorithm, two tests have been carried out. In the first test, the original image 46_2 is encrypted using the key K1 and the same image is encrypted using the key K2, which differs from K1 by only one digit. Then, the difference between the encrypted images, presented in figure 4, is evaluated by the NPCR and the UACI measures. The obtained results are 98.1194 % for the NPCR and 27.8536 % for the UACI. These results clearly show the high sensitivity of the proposed encryption algorithm to slight changes of the encryption key.

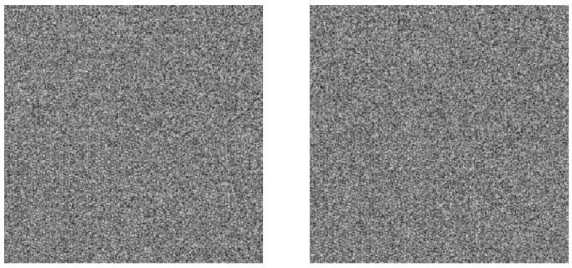


Fig. 4: Encrypted Image using Key K1 (left Image) and Encrypted Image Using Key K2 (Right Image).

The second test aims at evaluating the sensitivity of the key in decryption process. In this test, the encrypted image 4a is decrypted using a correct key K1and wrong key K2 , that differs from the correct one by one digit. The decrypted images are presented in figure 5. As it can be noticed, decrypting the image using a wrong key leads to a completely different image from the original one. Based on the results of the two tests, we can conclude that the proposed algorithm is robust against exhaustive attacks.

Fig. 5: Decrypted Image Using Correct Key (left Image) and Decrypted Image Using Wrong Key (right Image).

B. Differential attack:

To resist the differential attack, the encryption algorithm should be very sensitive to small changes introduced to the original image. In other words, it generates a completely different encrypted image when the original image is slightly altered. In order to verify the robustness of the proposed algorithm against this attack, a randomly selected pixel from each test image is changed by only one bit to obtain a modified image. Then, the original images and their modified versions are encrypted using the same key. The NPCR and UACI measures

are used to evaluate the difference between the encrypted images. The obtained results, given in Table 2, show the big difference between the encrypted images, and hence, confirming the robustness of the proposed algorithm against the differential attack.

Table 2: NPCR and UACI of encrypted images.

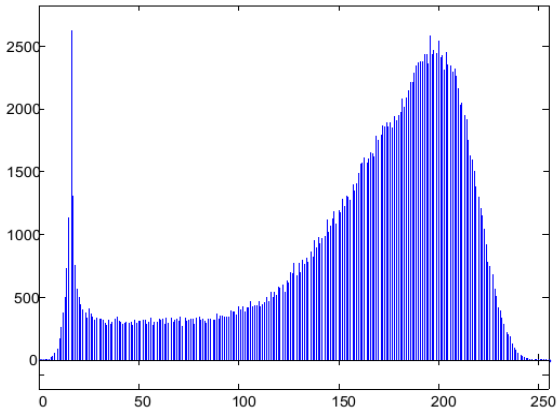
Image	NPCR (in %)	UACI (in%)
Image 22_6	98.34	29.76
Image 46_2	98.56	29.51
Image 88_1	98.79	29.66

C. Statistical analysis:

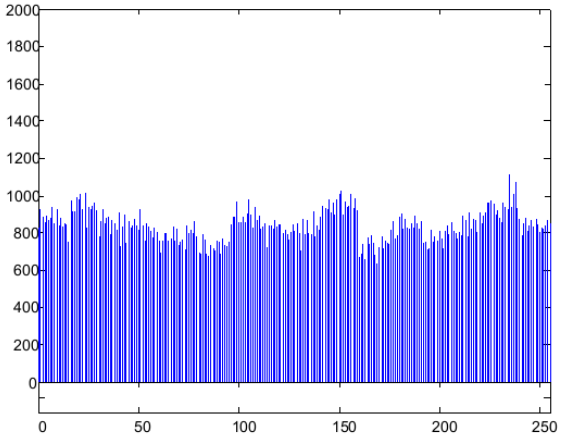
In his work (Shanon, 1949) published in 1949, Shannon stated that: "It is possible to solve many kinds of ciphers by statistical analysis ". So, he proposed two methods based on confusion and diffusion in order to counteract powerful attacks based on statistical analysis. In order to prove the security of the proposed algorithm against statistical attacks, two statistical tests have been performed.

Histogram:

An ideal image cryptosystem should generate scrambled images with a uniform his-togram. Figure 6 depicts the histogram of original image 46_2 (Figure 2b), and the histogram of its encrypted image (Figure 3). It is clear from the histogram of encrypted image that the pixels of the encrypted image are uniformly distributed.



a) Original Image Histogram



b) Encrypted Image Histogram

Fig. 6: Histogram of Original and Encrypted Images.

Correlation of adjacent pixels:

It is well known that, in general, any chosen pixel in an image is more likely to be strongly correlated with its adjacent pixels. However, a secure image encryption algorithm must produce an encrypted image having low correlation between adjacent pixels. In order to test the correlation of adjacent pixels, we have randomly

selected N = 10000 pairs (vertical, horizontal and diagonal) of adjacent pixels from the original and the encrypted images separately. Then, the correlation coefficient of each pair is calculated. The result are shown in Table III. Analyzing these results, we can see that the correlation coefficients of the adjacent pixels of the encrypted images are very small (≈ 0). Relying on these results and the results obtained from the histogram test, one can conclude that the proposed algorithm possesses high security against statistical attacks.

Table III: Correlation coefficients of pairs of adjacent pixels.

Image	Horizontal	Vertical	Diagonal
22_6	0.92	0.92	0.87
Encrypted 22_6	0.006	-0.01	0.006
46_2	0.88	0.92	0.80
Encrypted 46_2	-0.007	0.01	0.008
88_1	0.94	0.92	0.90
Encrypted 88_1	0.01	0.03	0.03

Conclusion:

In this paper, a fingerprint image cryptosystem based on blocks permutation and Rubik's cube principle in wavelet domain is proposed in order to enhance the security of fingerprint-based systems against replay attacks, which may occur in different points as stated by (Ratha *et al*., 2001). First, one-level Lifting Wavelet Transform Integer-to-Integer is performed to original image. The approximation and details sub-bands are then partitioned into blocks of size LxL, which are permuted using a permutation key. After that, for each sub-band the Rubik's cube principle presented in [9] is applied. Then, the XOR operator is applied separately for rows and columns of the modified sub-bands. Finally, the encrypted image is constructed by the encrypted sub-bands. Experimental tests and security analysis have been carried out on real fingerprint images and the obtained results demonstrates the robustness of the proposed image algorithm against exhaustive, differential and statistical attacks.

REFERENCES

[1] Ratha, N.K., J.H. Connell and R.M. Bolle, 2001. Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal, 40(3): 614-634.
[2] Fingerprint Verification Competition, "FVC 2000," http://bias.csr.unibo.it/fvc2000/databases.asp, Nov. 2012.
[3] Jain, A.K., R. Bolle and S. Pankanti, 2005. Biometrics: Personal Identification in Networked Society. Kluwer Academic Press.
[4] Wu, C., 2007. Advanced feature extraction algorithms for automatic fingerprint recognition systems. Ph.D. thesis, University Of New York at Buffalo.
[5] Ratha, N.K., H.H. Connell and R.M. Bolle, 2001. An Analysis of Minutiae Matching Strength. In Proceedings of The 3rd International Conference on Audio and Video Based Biometric Person, 2091: 223-228.
[6] Maltoni, D., D. Maio, A.K. Jain and S. Prabhakar, 2003. Handbook of Fingerprint Recognition. Springer, New York.
[7] Uludag, U., S. Pankanti, S. Prabhakar and A.K. Jain, 2004. Biometric Cryptosystems: Issues and Challenges. Proceedings of the IEEE, 92(6): 948-960.
[8] Loukhaoukha, K., J.Y. Chouinard and A. Berdai, 2012. A Secure Image Encryption Algorithm Based on Rubik's Cube Principle. Journal of Electrical and Computer Engineering, 13.
[9] Han, F., J. Hu, X. Yu and Y. Wang, 2007. Fingerprint images encryption via multi-scroll chaotic attractors. Applied Mathematics and Computation, 185(2): 931-939.
[10] Khan, M.K. and J. Zhang, 2007. An Intelligent Fingerprint-Biometric Image Scrambling Scheme, 1141-1151.
[11] Alghamdi, A.S. and H. Ullah, 2010. A Secure Iris Image Encryption Technique Using Bio-Chaotic Algorithm. International Journal of Computer and Network Security, 2(2): 78-84.
[12] Delong, C., 2010. A Novel Fingerprint Encryption Algorithm Based on Chaotic System and Fractional Fourier Transform. In Proceedings of International Conference on Machine Vision and Human-Machine Interface, 168-171.
[13] Chen, G., Y. Mao and C.K. Chui, 2004. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons and Fractals, 21: 749-761.
[14] Alvarez G. and S. Li, 2006. Some basic cryptographic requirements for chaos-based cryptosystems. International Journal of Bifurcation and Chaos, 16(8): 2129-2151.
[15] Shannon, C.E., 1949. Communication Theory of Secrecy Systems," Bell System Technical Journal, 28(4): 656-715.