RESEARCH ARTICLE OPEN ACCESS

Security Enhancement for Digital Images using Chaotic Maps

Prof. Swetha.T.N[1], Dr. S.Bhargavi[2], Dr. Sreerama Reddy G.M[3],Prof. Gangadhar.V[4]
1 (Asst. Professor, Dept of ECE, S.J.C.I.T, Chickballapur.)
2 (Professor, Dept of TCE, S.J.C.I.T, Chickballapur.)
3 (Professor, Dept of ECE, C.B.I.T, Kolar.)
4 (Asst. Professor, Dept of ECE, S.J.C.I.T, Chickballapur.)

Abstract:

The chaos based cryptographic algorithms have suggested some new and efficient ways to develop secure image encryption techniques. In this paper an algorithm for encryption & decryption of digital image using chaotic logistic map and Arnold cat map is discussed. The algorithm utilizes the good features of chaotic sequence related to cryptographic properties, such as pseudo-random, sensitivity to initial conditions and aperiodicity. The algorithm use logistic mapping to confusion the location of pixels in a digital image & Arnold cat map parameters are to be considered as secret keys for securing an image. Due to change of any secret keys the system produces undesired results at the receiver side. Finally experimental results along with statistical analysis including histogram analysis and correlation property show that presented algorithm has good desirable cryptography properties and is more secure technique against the unauthorized person.

Keywords - **Digital image, Image scrambling, Chaotic sequence, Logistic mapping, Arnold cat map**

1. Introduction:

In recent years, it is seen that chaos system plays significant role in image cryptography for secure transmission. The basic idea behind this is to convert the image, pixel by pixel, to chaotic map variables by iterating chaotic map using initial conditions. After a small number of iterations, a certain number of cycles and changing pixel positions using Arnold cat map, image becomes unpredictable. Image size, initial conditions, number of iterations, number of cycles and Arnold cat map parameters are to be considered as secret keys for securing an image. Due to change of any secret keys the system produces undesired results at the receiver side.

In last few years, basic ideas and theories behind chaos system have diverted the researcher`s mind towards the direction of cryptography. Cryptography is the study of mathematical techniques related to the aspects of the confidential information. The main purpose of cryptography is conversion of an original message into a cipher message and then recovers the message back in its original form. This process involves transformation of the original message into garbage message, so that unauthorized people cannot have access of secret message.

A number of different encryption techniques have been proposed by many researchers to provide the confidentiality of the message may be text, data, picture, video etc. Image is one of the most important styles for representation of information and more than 80% information we obtained is from vision. Due to high sensitivity of chaos systems to initial

Conditions and system parameters, it can be used for strong chaotic cryptosystems that makes them robust against any statistical attacks. Therefore, chaos system plays a great and significant role in cryptography system in many areas, including a database, Internet transaction, banking, software, online business and protection of communication channels.

During image encryption, chaotic map followed by Arnold cat map has also been introduced for secure strong image cryptography. Unlike chaotic map, Arnold cat map has different significance towards image pixels positions. As a result of the initial sensitivity and the unpredictability of outcome of the chaotic map, it is very difficult to attack the secure system effectively.

The wide use of digital images across the world in internet, wireless networks, military image database, medical imaging system and various other applications, require reliable, fast and robust security system to store and transmit digital images. In order to fulfill the security requirements of digital images, many image encryption approaches have been used. One of the recently and widely used approaches is the chaos based cryptography.

A lot of work is going on in developing the chaos based cryptosystems. In cryptography, the strength lies in choosing the keys, which are secret parameters, used in encryption. It should not be possible to guess the key by an intruder. The chaotic systems are very sensitive to initial conditions and system parameters. For a given set of parameters in chaotic regime, two close initial conditions lead the system into divergent trajectories. Therefore, an encryption/decryption scheme can be developed if the secret parameters are chosen as keys. Since the same parameters are used for encryption and decryption, the chaos scheme is symmetric. The parameters and the initial conditions form a key space thereby enhancing the security of the scheme. In recent years, the chaos based cryptographic algorithms have suggested some new and efficient ways to develop secure image encryption techniques in order to meet the demand for real-time image transmission over the communication channels. Chaos based image encryption methods are considered good for practical use because they have important characteristics like:

- They are very sensitive to initial conditions/system parameters,
- They have pseudo-random property and non-periodicity as the chaotic signals are usually noise-like, etc. All these characteristics make chaos an excellent and robust cryptosystem against any statistical attacks.

The combination of the chaotic theory and the cryptography is an important study field of the image encryption. Classical Arnold cat map can change the position of image pixel points through iteration, but these pixel points will return to the original position after iterating many times. It is obvious not enough to carry on the encryption by using it only. If the encrypted result with cat map is carried to Lu chaotic map to encrypt again, it can attain the purpose of confusion and diffusion through changing the pixel value of each point. The system security lies in the initial sensitivity of chaotic map. By using the Matlab to simulate, comparing with the encryption of single map, the method has the high improvement in anti-attacking.

Internet has changed our work efficiency and life style by astonishing speed, and the business organization and personal will pass the Internet or the other electronics medium to process bank business, send out an E-mail, shopping and transact more and more. However, these characteristics also make the safety of secret communication more important, information encryption is one of the valid paths among them.

The basic thought of encryption is confusing and diffusing original information. Traditional encryption ways such as DES, RSA have already matured, but they are not fit to all the information encryption. If encrypting image by the traditional ways, the relativity of the adjacent pixel points is very great and it is easily attacked by the statistical analysis. So the security of the system is dangerous. Combination of the chaotic theory and the cryptography is a method improves the encryption level.

The chaotic theory as a new subject only twenties years, but it already has access into many subjects rapidly, and becomes an important and advanced science. The chaotic theory has the initial sensitivity, the parameter sensitivity and the unpredictability etc, such as “butterfly-effect”. Appling these important characteristics to the information encryption have already became a hot research direction.

II 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.

A. Characteristics of 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 [15-16]. 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.

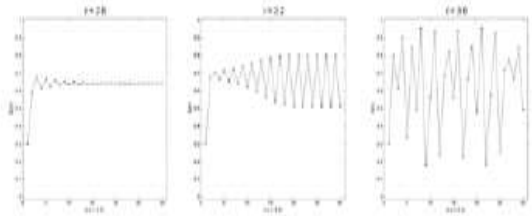
B. The logistic map and its analysis

One of the most known and widely used chaotic systems is the Logistic mapping. Logistic mapping is an ecosystem model which can be showed with a nonlinear repeated equation as follows:

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

where r is a system parameter lies between 0 to 4, X_n is map variable lies between 0 to 1, X_0 is the initial condition of the logistic map and n is number of iteration used for generating the iterative values. By varying the system parameter r, following behaviors are observed:

a. When the value of r lies between 0 to 1, the iterative values ultimately die, which are sovereign of initial condition.
b. When the value of r lies between 2 to 3, the iterative values first oscillate around some value and then finally stabilize on the same value as shown in Fig. 1(a).
c. When the value of r lies between 3 and 3.45 (approximately), the iterative values oscillate between two values forever, which are dependent on r as shown in Fig. 1(b).
d. When the value of r lies between 3.45 and 3.56 (approximately), the iterative values oscillate between four values.
e. As the value of r becomes greater than or equal to 3.57, this logistic map is converted into chaotic map, because a slight variation in the initial condition produces dramatically different iterative values over time, exhibit chaotic behavior and trajectory of these iterative values is called chaotic attractor, and hence the property of sensitive dependence which is a suitable condition for image encryption as shown in Fig. 1(c).[11]



a) iteration property when r = 2.8 b) iteration property when r = 3.2 c) iteration property when r = 3.8

Fig 1: Analysis of Logistic Map

C. Arnold Cat Map

Arnold cat map is a special type of chaotic map and it can be represented in matrix form as follow[9]:

$$\begin{bmatrix} x_{\varphi+1} \\ y_{\varphi+1} \end{bmatrix} = \begin{bmatrix} 1 & \varepsilon \\ \eta & \eta\varepsilon + 1 \end{bmatrix} \begin{bmatrix} x_{\varphi} \\ y_{\varphi} \end{bmatrix} mod(N) \qquad (2)$$

Where, are the pixel position of N x N image, Є, η are the constant parameters which are positive integers. The most important property of Arnold cat map is that it rearranges the position of image pixel, but after iterating a certain numbers it returns the same pixels position as before and thereby produces the original image. Let us consider, for image, when parameters Є =10, η =8 are given then it recovers the original pixels positions after being iterated 128 times, as shown in Fig. 1, [9]. These 6 pictures are the original image and the images which are iterated after 30, 60, 90, 120, 128 times. By varying the size of image and parameters η, ε, image can be recovered after different number of iterations. So size of the image and parameters of Arnold cat map may be treated as secret keys for image encryption. Due to a less number of secret keys and repeatability of original image Arnold cat map cannot be used for security system alone. So, for enhancing the security system it requires further processing.

III Chaos Based Chipper

The proposed image encryption algorithm has two major steps. Firstly, the correlation among the adjacent pixels is disturbed completely as the image data have strong correlations among adjacent pixels. For image security and secrecy, one has to disturb this correlation. To achieve this, the pixel values of the image are encrypted by employing a one-dimensional Logistic map, to provide more security against cryptanalysis we proposed a new block based image shuffling scheme using Arnolds Cat map in which the two control parameters η, Є of map are randomly generated through a key dependent chaotic sequences. The control parameters of Cat map are the control parameters of shuffling. The shuffling effect obtained after a number of iterations depends on these parameters.

A) Encryption Algorithm:

Encryption module is a simple block cipher with block size of 8-bit and 256-bit secret Key. The key is used to generate a pad that is then merged with the plaintext a byte at a time.

Step 1: For the encryption, First divide the original (plain) image pixels into blocks of 8-bits & i^{th} blocks can be represented as

$$P = P1P2P3P4 \ldots\ldots\ldots Pi \qquad (3)$$

Step 2: The proposed image encryption process utilizes an external secret key of 256-bit long. Further, the secret key is divided into blocks of 8-bit each, referred as session keys.

$K = K1K2K3K4$ .....$K64$ (in hexadecimal) (4)

here, *Ki* 's are the alphanumeric characters (0–9 and A–F) and each group of two alphanumeric characters represents a session key. Alternatively, the secret key can be represented in ASCII mode as

$K = K1K2K3K4$ .....$K32$ (in ASCII) (5)

here, each *Ki* represents one 8-bit block of the secret key i.e. session key.

Step 3: The initial condition ($X\ 0$) for the chaotic map and the initial code $C0$ are Generated from the session keys as

$$R = \sum_{i=1}^{32}([Ki]) \quad (6)$$

$$X_0 = R - \lfloor R \rfloor \quad (7)$$

$$C0 = \sum_{i=1}^{32}[Ki]\ mod\ 256 \quad (8)$$

Here *Ki* , ⌊ ⌋ , and M1 are, respectively, the decimal equivalent of the i^{th} session key, the floor function, and mapping from the session, key space, all integers between 0 and 255, into the domain of the logistic map, all real numbers in the interval [0,1].

Step 4: Read a byte from the image file (that represent a block of 8-bits) and load it as Plain image pixel *Pi.*

Step 5: Encryption of each plain image pixel *Pi* to produce its corresponding cipher image pixel *Ci* can be expressed mathematically as:

$$C_i = \left(P_i + M2\left[\sum_{i=1}^{\#_i} rX_i(1-X_i)\right]\right) \bmod 256 \quad (9)$$

Where *Xi* represents the current input for logistic map and computed as:

$$X_i = [X_{i-1} + C_{i-1} + K_i] \quad (10)$$

$\#_i$ is the number of iteration of logistic map for its current input *Xi* and calculated as:

$$\#_i = K_{i+1} + C_{i-1} \quad (11)$$

And M2 maps the domain of the logistic map, [0,1],back into the interval [0,255].

Step 6: Repeat steps 4-5 until the entire image file is exhausted.

Step 7: After finishing all steps mentioned above, now pixels positions are changed according to Arnold cat map manner called encoded pixels for strong secure transmission, so that un-correlation between adjacent pixels would become increased.

B) Decryption Algorithm:

Decryption is very simple, the same pad is generated but this time un-merged with the cipher text to retrieve the plaintext. The decryption module receives an encrypted image (cipher image) and the 256-bit secret key and returns the original image (plain image).

In particular, the decryption module works in the same way as the encryption module but now the output is subtracted from the corresponding Cipher image pixel *Ci* providing the plain image pixel *Pi* . The output of the decryption module is the original image (plain image). Decryption of each cipher image pixel C_i to produce its corresponding plain image pixel P_i can be expressed mathematically as:

$$P_i = \left(C_i - M2\left[\sum_{i=1}^{\#_i} rX_i(1-X_i)\right]\right) \bmod 256 \quad (12)$$

C) Design Principles:

The basic concept is that the encryption of each part of the plain image depends not only on the key, but also on the previous cipher image. The use of feedback mechanism has two desirable benefits. The first benefit is that there can be no simple periodicity in the encrypted image (cipher image) because the encryption of each plain image pixel depends not only on the encryption key, but also on the previous cipher image pixel. The second benefit is that any changes in the plain image are cascaded forward throughout the cipher image, which means that two almost identical plain images will encrypt to completely different cipher images. This sensitivity to the plain image is also a plus to the security of the proposed system.

The proposed system makes heavy use of data dependent essentials. This appears for the current input of logistic map, which is data-dependent since it is computed as a function of the current session key K_i , previous computed cipher pixel C_{i-1} and previous logistic output. Also, the number of iterations # for the chaotic logistic map is data-dependent since it is computed as a function of current session key K_{i+1} and previous computed cipher pixel C_{i-1} . As we encrypt each new block, i , the counter used to keep track of the current session

key, is incremented. The output of the logistic map is then merged with the plaintext to give the cipher text.

IV Performance Analysis:

A) Test, Verification and Efficiency:

Results of some experiments are given to prove its efficiency of application to digital images. We use the gray-scale images--Lena of size 256 x 256, gray-scale (0-255) as the original images (plain images) and the secret key "12345789012345678912345678901 2" (in ASCII) is used for encryption whose size is 256-bit. The encrypted images are depicted in Fig 2(b). As shown, the encrypted images (cipher images) regions are totally invisible. The decryption method takes as input the encrypted image (cipher image), together with the same secret key "12345789012345678912345678901 23" (in ASCII). The decrypted images are shown in Fig 2(c). The visual inspection of Fig 2 shows the possibility of applying the proposed system successfully in both encryption and decryption. Also, it reveals its effectiveness in hiding the information contained in them.

a) Original image b) Encrypted image c) Decrypted image

Figure 2: Lena's Plain image/Cipher image

B) Security Analysis and Test Results:

A good encryption procedure should be robust against all kinds of cryptanalytic, statistical and brute force attacks. In this section, we discuss the security analysis of the proposed system such as key space analysis, statistical analysis to prove that the Proposed cryptosystem is secure against the most Common attacks [16,17].

1) Key space analysis

For a secure image cryptosystem, the key space should be large enough to make the brute force attack infeasible. The proposed system has 2^{256} different combinations of the secret key. An image cipher with such a long key space is sufficient for reliable practical use. In the proposed system, a chaotic logistic map is employed which is sensitive on the initial condition. The initial condition for logistic map is calculated from the secret key. Additionally the number of iterations supported by the logistic map module is between 0 and 767, as cipher pixels take values in the interval [0,512] and the session keys take values in the interval [0,255].

2) Statistical Analysis:

It is well known that many ciphers have been successfully analyzed with the help of statistical analysis and several statistical attacks have been devised on them. Therefore, an ideal cipher should be robust against any statistical attack. To prove the robustness of the proposed system, we have performed statistical analysis by calculating the histograms and the correlations of two adjacent pixels in the plain image/cipher image.

i) Histograms analysis

To prevent the leakage of information to an opponent, it is also advantageous if the cipher image bears little or no statistical similarity to the plain image. An image histogram illustrates how pixels in an image are distributed by graphing the number of pixels at each color intensity level. We have calculated and analyzed the histograms of the several encrypted images as well as its original images that have widely different content. One typical example among them is shown in Fig.3(b). The histogram of a plain image contains large spikes. These spikes correspond to color values that appear more often in the plain image. The histogram of the cipher image as shown in Fig.3(d), is more uniform, significantly different from that of the original image, and bears no statistical resemblance to the plain image. It is clear that the histogram of the encrypted image is fairly uniform and significantly different from the respective histograms of the original image and hence does not provide any clue to employ any statistical attack on the proposed image encryption procedure.

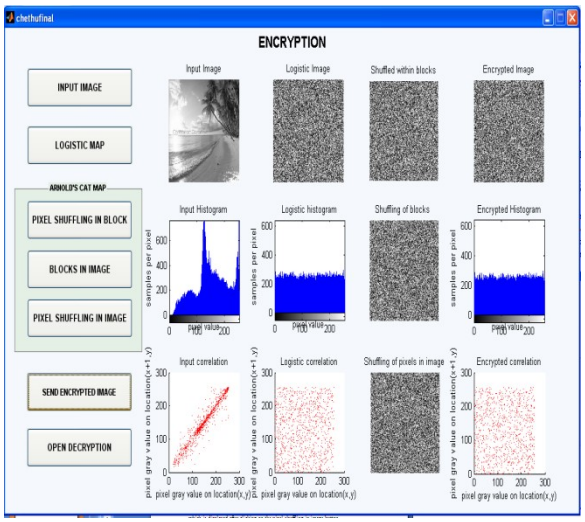


Figure 3 (Vertically): Original image, Histogram of original image, Correlation coefficient of original image , Encrypted image , Histogram of encrypted image, Correlation coefficient of encrypted image

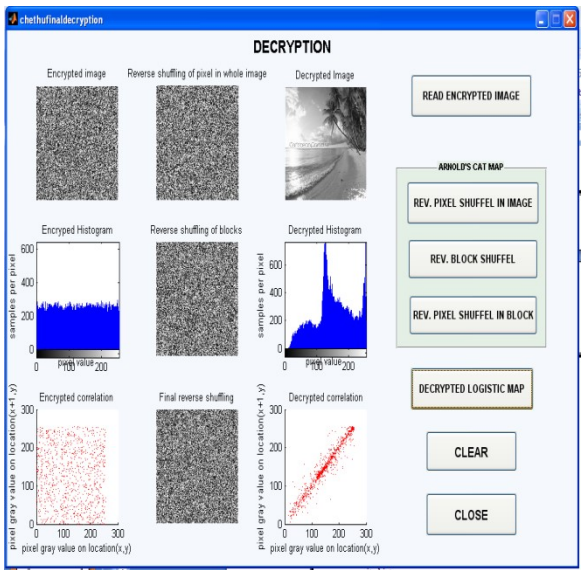


Figure 4 (Vertically): Cipher image, Histogram of cipher image, Correlation coefficient of Cipher image , Decrypted image , Histogram of decrypted image, Correlation coefficient of decrypted image

i) Correlation coefficient analysis

In addition to the histogram analysis, we have also analyzed the correlation between two vertically adjacent pixels, two horizontally adjacent pixels and two diagonally adjacent pixels in plain image/cipher image respectively. The procedure is as follows: First, randomly select 1000 pairs of two adjacent pixels from an image. Then, calculate their correlation coefficient using the following two formulas:

$$\mathrm{cov}(x, y) = E(x - E(x))(y - E(y)) \quad (13)$$

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (14)$$

Where x and y are the values of two adjacent pixels in the image. In numerical computations, the following discrete formulas were used:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} xi \quad (15)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (xi - E(x))^2 \quad (16)$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N} (xi - E(x))(yi - E(y)) \quad (17)$$

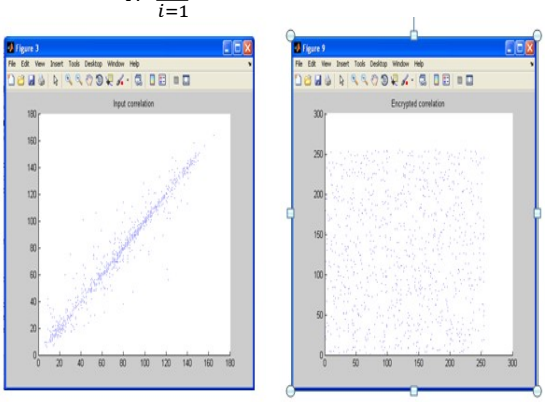


Fig 5: Two horizontally adjacent pixels correlation in pixel image/cipher image

This Fig. 4 shows the correlation distribution of two horizontally adjacent pixels in plain image/cipher image for the proposed system. The correlation coefficients are 0.9905 and 0.0308 respectively for both plain image/cipher image. Similar results for diagonal and vertical directions are obtained as shown in Table 1. It is clear from the Fig. 4 and Table 1 that there is negligible correlation between the two adjacent pixels in the cipher image. However, the two adjacent pixels in the plain image are highly correlated.

Direction of Adjacent pixels	Plain image	Cipher image
Horizontal	0.9910	0.0053
Vertical	0.9651	0.0289
Diagonal	0.9730	0.0102

Table 1: Correlation coefficients in plain image/ Cipher image for the sea image

V Conclusion

In this paper, a new way of image encryption scheme have been proposed which utilizes a chaos-based feedback cryptographic scheme using the logistic map and an external secret key of 256-bit. The robustness of the proposed system is further reinforced by a feedback mechanism, which leads the cipher to a cyclic behavior so that the encryption of each plain pixel depends on the key, the value of the previous cipher pixel and the output of the logistic map. We have carried out key space analysis, statistical analysis to demonstrate the security of the new image encryption procedure. According to the results of our security analysis, we conclude that the proposed system is expected to be useful for real-time image encryption and transmission applications.

References:

[1] W. Stallings., "Cryptography and Network Security: Principles and Practice," Prentice- Hall, New Jersey, 1999.
[2] Bruce Schneier, "Applied Cryptography – Protocols, algorithms, and source code in C," John Wiley & Sons, Inc., New York, second edition, 1996.
[3] N. Bourbakis and C. Alexopoulos , Picture data encryption using SCAN patterns. Pattern Recognition 25 6 (1992), pp. 567–581.
[4] Alexopoulos, C., 1989. SCAN, A language for 2-D sequential data accessing. Ph.D. Thesis, University of Patras, Greece.
[5] C.J. Kuo , Novel image encryption technique and its application in progressive transmission. J. Electron. Imaging 24 (1993), pp. 345–351.
[6] Chang, H.K., Liou, J.L., 1994. An image encryption scheme based on quadtree compression scheme. In: Proceedings of the International Computer Symposium, Taiwan, pp. 230–237.
[7] Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen, "A new encryption algorithm for image cryptosystems", The Journal of Systems and Software 58 (2001), 83-91
[8] Fridrich Jiri, Symmetric ciphers based on two dimensional chaotic maps, Int. J. Bifurcat Chaos 8 (1998) (6), pp. 1259–1284.
[9] J. Scharinger, Fast encryption of image data using chaotic Kolmogrov flow, J. Electronic Eng 7 (1998) (2), pp. 318–325.
[10] J.C. Yen, J.I. Guo, A new image encryption algorithm and its VLSI architecture, in: Proceedings of the IEEE workshop signal processing systems, 1999, pp. 430–437.
[11] J.C. Yen, J.I. Guo, A new chaotic key based design for image encryption and decryption, Proceedings of the IEEE International Symposium Circuits and Systems, vol. 4, 2000, pp. 49–52.
[12] S. Li, X. Zheng, X. Mou, Y. Cai, Chaotic encryption scheme for real time digital video, Proceedings of the SPIE on electronic imaging, San Jose, CA, USA, 2002.
[13] M. S. Baptista, "Cryptography with chaos". Phys. Lett. A, vol.240, pp.50-54,1998.
[14] G. Jakimoski and L. Kocarev, "Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps," IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications, vol. 48, no. 2, February 2001.
[15] St even Henry Strogatz, "Nonlinear dynamics and chaos: With applications to physics, biologym chemistry, and engineering," first ed., Addison-Wesley Publishing Company, Reading, Massachusetts, 1994.
[16] Shujun Li, Guanrong Chen and Xuan Zheng, "Chaos-based encryption for digital images and videos," chapter 4 in Multimedia Security Handbook, February 2004.
[17] Yaobin Mao, Guanrong Chen, and Shiguo Lian, "A symmetric image encryption scheme based on 3D chaotic Cat maps," Chaos, Solitons and Fractals 21, pages 749-761, 2004.