A new image encryption method using chaotic map

Rezvaneh Babazade Gorji
Department of Computer Engineering,
Sari Branch, Islamic Azad University,
Sari, Iran
r.babazadeh1211@yahoo.com

Mirsaeid Hosseini Shirvani[1], Farhad Ramezani Mooziraji[2]
[1,2] Department of Computer Engineering,
Sari Branch, Islamic Azad University,
Sari,Iran
[1] mirsaeid_hosseini@yahoo.com
[2] ramezani.farhad@gmail.com

***Abstract*—Nowadays, using transfer information includes images has increased due to increasing use of computer demands. Chaos-based image encryption method is one of the most efficient methods which is used to hide visual information during transmission. This paper presents a new image encryption method based on Logistic and Tent chaotic maps and permutation-diffusion architecture, in which, chaotic maps will change the pixels of the plain-image to encrypt that. Finally, the encrypted image will be decrypted to remake the plain-image. To assess the efficiency of this method, it has been implemented with MATLAB software and also has been measured by doing some tests as analysis of the space key, histogram analysis, key sensitivity analysis, maximum signal-to-noise ratio, adding salt & pepper noise and also data loss. Simulation results shows that the proposed image encryption method has high accuracy while it is resistant against salt & pepper noise, data loss and universal Search attack. The test results, such as histogram analysis and key sensitivity tests are also confirmation on the suitability of proposed method.**

Keywords— image encryption; chaotic map; Logistic chaotic map; Tent chaotic map; permutation; diffusion.

I. INTRODUCTION

With the development and progress of science and technology, hiding the information has evolved as well and found its position as a powerful tool in order to maintain the information. Nowadays, communication through telecommunication equipment has increased dramatically at different levels, so there is always the risk of eavesdropping and tampering by enemy or profiteering that threatens this information. The security of image as one of the most common exchangeable data is taken into consideration with the progress of technology in the past decade to prevent unauthorized access at network level. So researchers are looking for a way to slow down the rate of correlation between the pixels in the images. So, high correlation between the pixels of the images will ease guessing the original one [14].

Encryption systems from key point of view are divided into to two categories as symmetric systems or safe key and asymmetric systems or public key. In symmetric encryption systems, encryption and decryption operations is dependent on a secret key agreement called private key and the safety and validation of the message is dependent on a safety of this key. Symmetric systems are divided into Block Cipher and Stream Cipher or the sequence systems. In Block Cipher (cryptographic) systems, the sequence of information is divided to the templates with specified length and each Block is encrypted under a certain algorithm that is dependent on a key. But in Stream Cipher, encryption will happen for the entire data. The ideal mode in a Stream encryption, is applying a completely random sequence as a key. In Block Cipher systems to regenerate a key sequence by decoder, we should necessarily use definite and specific methods for the production of sequences. In fact we can use Pseudo Random Sequences rather than Random Sequences. One way to generate a Pseudo Random Sequence is using chaos systems. Chaos in many physical, chemistry and atmospheric phenomenon and so on is visible and attract the attention of several researchers in recent years. Encryption methods based on chaos has two stages: Turbulence and influence (distribution). In turbulence method, the pixels of image will find permutation by some chaos mapping and in influence stage the pixels value will change in a way that a small change in an initial image will cause a great change in a relevant Cipher image. In techniques based on chaos, the designing of change function is challenging, so designing an effective and easy change function can lead us to cryptography. In this paper we try to reach a new method in image encryption using Tenet and Logistic chaos functions. These functions using generation of random numbers will produce Cipher image.

II. REVIEW OF LITERATURE

Chaos is a phenomenon that occurs in deterministic non-linear systems that has high sensitivity to the initial condition and shows a pseudo random behavior at the same of being deterministic. It means that by having initial values and mapping function, we can regenerate the exact initial values. Small change in initial condition will cause a great change in the future. This phenomenon in chaos theory is called Butterfly effect. Such systems will stay in chaos mode so that can have the condition of Lyapunov exponential equation. An important feature that makes this phenomenon being highly regarded for encryption is the definability of the system and at same time having the pseudo random behavior that causes the output of the system seems randomly at attacker's point of view, while it is definable at a decoder of Cipher system point of view so it can be decrypted easily.

In recent years, many encryption algorithms base on chaos are proposed. Pareek and Patidar (2006) have proposed a new way of image encryption scheme which utilizes two chaotic logistic maps and an external key of 80-bit. The initial conditions for both the logistic maps were derived using the external secret key by providing weightage to its bits corresponding to their position in the key. Gao and Chen (2006) presented an image encryption scheme which employs a new image total shuffling matrix to shuffle the positions of image pixels and then uses the states combination of two chaotic systems to confuse the relationship between the plain-image and the cipher-image.

III. BACKGROUND

In the group of chaotic maps, the 1D chaotic maps have lots of applications because of their simple structure. In this section, we briefly review one of the named Logistic map. Then we review a 2D chaotic map name Tent map. They will be used for our new chaotic system.

A. *Logistic map*

The Logistic map is one of the famous 1D chaotic maps. it is a simple dynamical equation with complex chaotic behavior. the mathematical definition of this map can be expressed in the following equation:

$$x_{n+1} = \alpha x_n(1 - x_n) \quad (1)$$

Where α is as parameter with range of (0,4] and $x_n$is the output chaotic sequence. α in this map is a control parameter which sometimes displayed with *r* or λ. This map is irreversible, means that by knowing x_n, we can not determine x_{n+1} uniquely. By following the trajectory of this map over the time, completely different behavior is observed. This behaviors are depend into control parameter α and initial conditions x_n. Logistic map is a member of large family of maps, named single-humped maps. Public property of these maps is that their corresponding function as presented in Fig.1 has one maximum point.

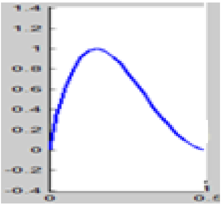


Fig. 1. Logistic map

B. Tent map

The Tent map is known as its tent-like shape in the graph of its bifurcation diagram. It can be defined bye equation (2).

$$(2) \qquad X_{n+1} = \tau(\mathrm{u}, X_n) = \begin{cases} uX_n/2\,, & X_i < 0.5 \\ u(1 - X_n/2), & X_i \geq 0.5 \end{cases}$$

Where parameter $\in (0,4]$. The chaotic property of this map appears when $u \in [2,4]$.

IV. Proposed Image Encryption Method

In image encryption process, first, the plain image encrypted with key image and finally the cipher image decrypted with the key image. The encryption phase composed of two major steps: confusion and diffusion. In the proposed method, the main key encrypted during the plain-image encryption. Encryption steps of the proposed algorithm defined as below:

A. Confusion step

a) The plain-image received and based on the first pixel value of it andapply the Tent map, the initial values for the next level chaotic function will be generate.

b) With the help of the numbers generated in the previous step and using logistic chaotic function, two arrays are created according to the number of the total root square of the image pixels and random values between 1 and the number of drives.

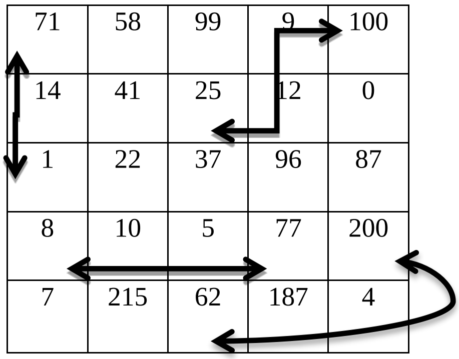
c) Using the chaotic Logistic map, an array contained of 8 pseudorandoic numbers corresponding to pixel levels will be generated.

d) Using the numbers generated in previous steps, the main key will be created.

*e) With respect to the number of pixels of plain-image, the main key break into two images with the size of plain-image and a 3*6 image.*

f) The first and second obtained from the main key will be confused with help of pseudorandom arrays of step "b".

g) Confussion of plain-image pixels: the values corresponding to each row and column will be exchanged with the values corresponding to the adjacent row and column which can be completely different from its real corresponding value.



71	58	99	9	100
14	41	25	12	0
1	22	37	96	87
8	10	5	77	200
7	215	62	187	4

Fig. 2. Exchange operation among pixels

B. Diffusion step

At this point the values of the pixels of the scrambled image are changed by reusing logistic function in a way that cannot be identified.

This step contains bellow sublevels:

a) Since the numbers corresponding to image pixels are between 0 and 255, and the corresponding numbers to these numbers are 8-bit digits, the eight bits of each pixel will be saved in one matrix.

b) 8 binary matrices generated so that the i'th matrix elements contains the corresponding i'th bit of all pixels.

c) Using the numbers generated in step "A.c", an 8-cell array of matrices will be generate and i'th level matrix will be inserted in the cell that correspond to random number generated in the previous step.

d) The drives of the array created in previous step are XOR two by two and are placed in a first drive.

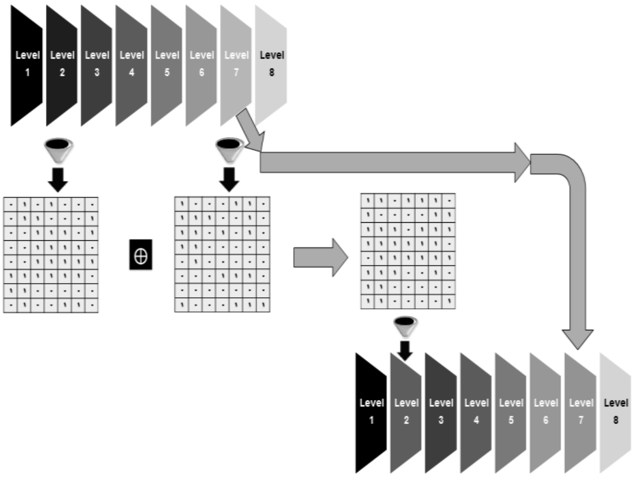


Fig. 3. XOR operation among binary levels of pixels

e) By replacing each 8 bit of the created matrix in step (e), the new image is created in a new matrix.

f) this is the final encrypted image.

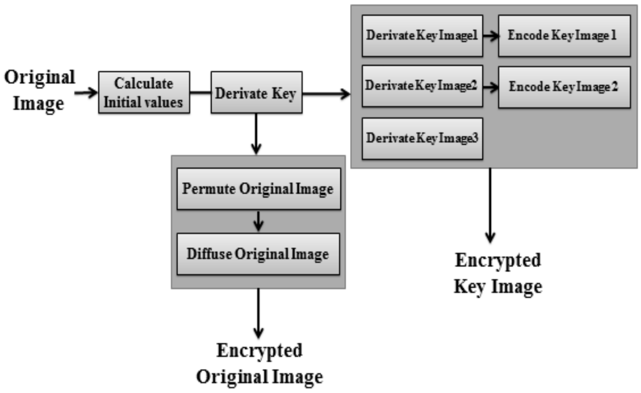


Fig. 4. Steps of image encryption

V. Proposed Image Decryption Method

Decryption steps in the proposed method defined as bellow:

The decryption phase begins reversely and is ended by pixels map and returning them to the previous place. This level contains below steps:

a) In this step,the three key-images are available. So the first and second one must be repermuted to be decrypted.

b) The two decrypted kei-images of previous ste, within the third key-image must reconstruct the main key.

c) This step is like diffusion step in encryption and it apply on the final encrypted image.Since we want the pixels of the encrypted image return to their initial value using retrieval first key, each of binary pages should return to their initial value according to the order of the image of the change phase in encryption mood.

d) At this phase using main key, the map of pixels are created for returning pixels to their initial place in the form of picture.

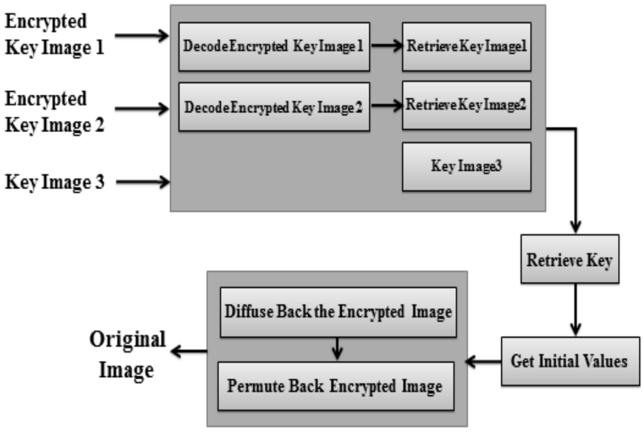


Fig. 5. Steps of image decryption

VI. EXPERIMENTAL RESULT

Resistance against any kind of attacks including statistic and brute-force attacks could be make a fine method from an encryption process. In this section we analyze the proposed method with some tests including key space analysis, histogram analysis, key sensitivity analysis, Peak to Noise Signal Ratio, adding salt & Pepper noise and Data Loss attack.

A. Key sensitivity analysis

A proper image encryption process should be sensitive toward small changes of key. This means that a one-bit-change in main key causes a very different result. In this paper one bit of the main key changed and the encrypted image decrypted with the new key. But this new decrypted image is absolutely different from the plain-image.

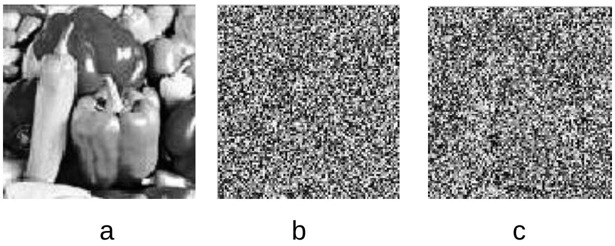


Fig 6. (a) plain-image, (b) encrypted image, (c) decrypted image after one-bit-change in main key. (key sensitivity change in decrypted image)

B. Histogram analysis

An image histogram is a graph by which the number of pixels in each gray level of the input image is determined. For each grayscale input image with 256 gray levels, each pixel of image has a [0.. 255] value range. Difference between plain-image histogram and encrypted image histogram shows the scale of encryption algorithm success. Uniformity of the histogram will reduce the possibility of statistic attacks. This fact displayed in fig. 7.

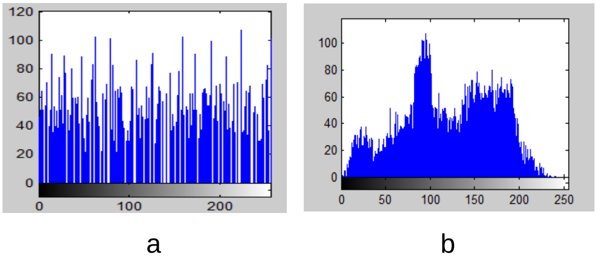


Fig 7. (a) histogram of plain-image, (b) histogram of encrypted image. (histogram)

C. Key space analysis

Key space, in a proper image encryption algorithm, should be large enough to resist against brute-force attack. In the proposed method, for a n*n plain-image, the key must have (n^2 + 18) digits. This key has a proper size and is proper for encryption. We used three arrays to display this large key and create three images from this arrays. (این بخش لازم نیست دقیقا مثل متن باشد)

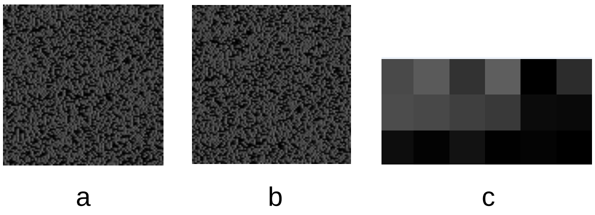


Fig 8. (a) key-image 1 , (b) key-image 2, (c) key-image 3. (key images)

D. Adding Salt & Pepper noise

In this section, first we transmuted the plain-image to encrypted form and then added Salt & Pepper noise with different noise rate. At least we decrypted the images. Results of simulation are shown in Fig. 9.

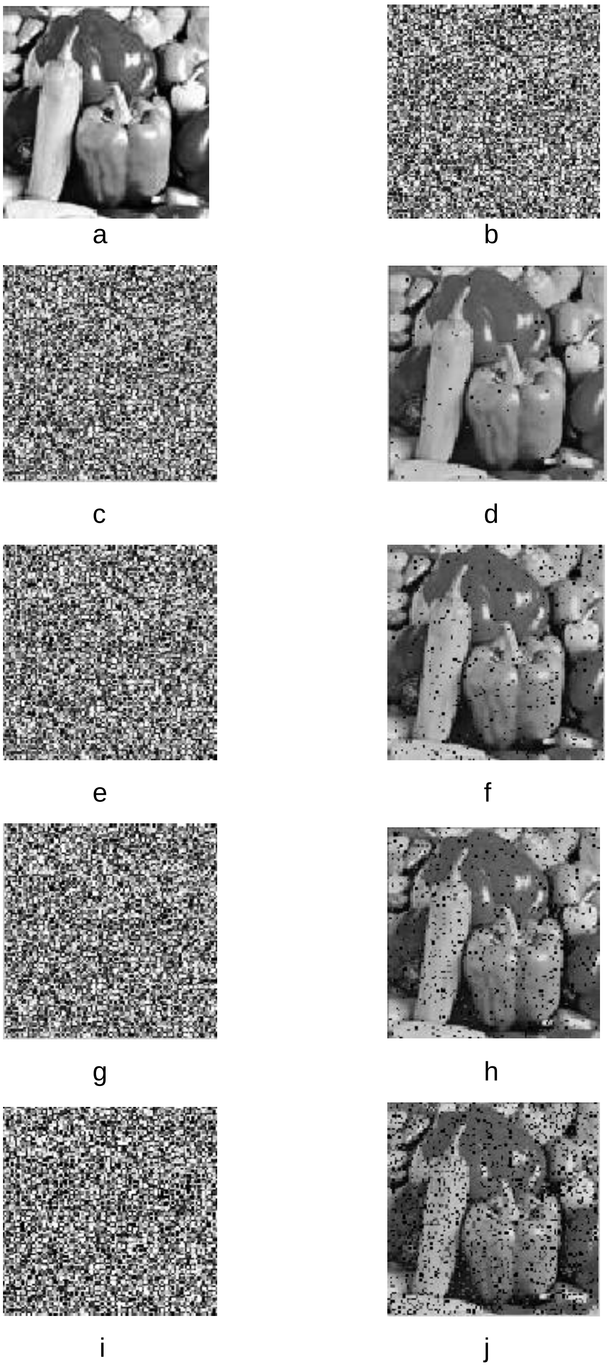


Fig 9. (a) plain-image, (b) encrypted image before applying Salt & Pepper noise, (c) the encrypted image added with 1% Salt & Pepper noise, (d) the decrypted image of (c), (e) the encrypted image added with 5% Salt & Pepper noise, (f) the decrypted image of (e), (g) the encrypted image added with 10% Salt & Pepper noise, (h) the decrypted image of (g), (i) the encrypted image added with 20% Salt & Pepper noise, (j) the decrypted image of (i). (Applying Salt & Pepper noise)

E. Data Loss attack

When this noise applies to the image, some parts of the image lose their real value. In this section, first we encrypt the plain-image and then add Data Loss attack with various loss rates. And finally the encrypted image will be decrypted. Simulation results are shown in Fig. 10.

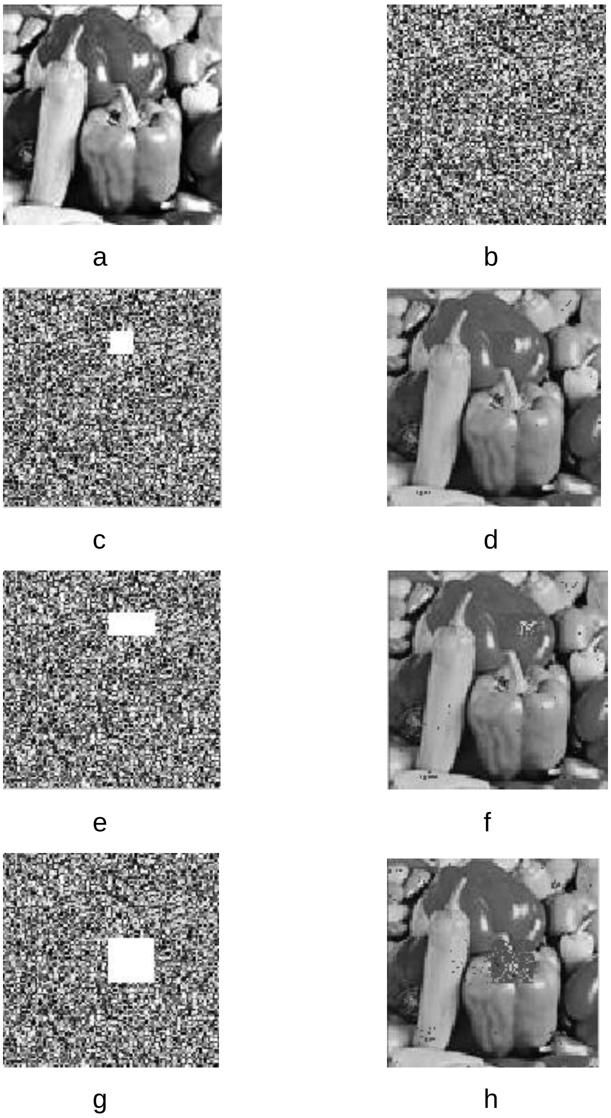


Fig 10. (a) plain-image, (b) encrypted image before applying Data Loss noise, (c) the encrypted image with a 10*10 Data Loss, (d) the decrypted image of (c), (e) the encrypted image with a 10*20 Data Loss, (f) the decrypted image of (e), (g) the encrypted image with a 20*20 Data Loss, (h) the decrypted image of (g). (Applying Data Loss noise)

F. Peak to Noise Signal Ratio

This metric computes the amount of equality of two images. Equation (3) represents this metric:

$$PSNR = 10 * \log\left(\frac{255^2}{\sum_{i=1}^{x}\sum_{j=1}^{y}\frac{(|A_{ij} - B_{ij}|)^2}{x * y}}\right) \tag{3}$$

The result of applying this test with Salt & Pepper noise and noise rate 1%, 5%, 10% and 20% are shown in table I.

TABLE I. AMOUNT OF PSNR WITH APPLYING SALT & PEPPER NOISE.

PSNR amount	***Salt & Pepper noise***

	rate
53.6654	1%
47.8638	5%
44.1972	10%
41.6635	20%

result of applying this test with a 10*10, 10*20 and 20*20 Data Loss noise and are shown in table II.

TABLE II. AMOUNT OF PSNR WITH APPLYING DATA LOSS NOISE.

PSNR amount	*Size of Data Loss noise*
56.6781	10*10
51.6348	10*20
48.4380	20*20

VII. CONCLUSION AND DISCUSSION

In this paper we used chaotic maps for image encryption. At first, using specifications of plain-image and chaotic maps help us to create the main key. Then with help of generated main key, the encrypted image has made. (Two major steps of image encryption operations including Confusion and Diffusion cause that The operation of encrypting pictures in permutations and change phase causes that the resulting encrypted image not only be similar to the main image from the appearance point of view, but also can not be identified easily and also breaking the password is too difficult.

Results obtained from evaluation show that image encryption using the proposed method is resistant against various attacks, including salt and pepper noise, data loss and universal Search attack. To evaluate the proposed method, this paper applied Salt & Pepper and Data Loss noise to reach suitable success.

REFERENCES

[1] R. Enayati Far, M. Saberi Kamarposhti, and M. Meybodi, “Image encryption using chaotic map and binary search tree,” 5'th iranian conference of machine vision and image processing, pp. 4-6, November 2008.

[2] A. Hosseini, B. Shokoohi, "Image encryption using chaotic maps", 9'th iranian student conference on electrical eengineering.

[3] S. Z. Jafari, F. Baari, Hosseini, B. Shokoohi, "Chaos application in text cryptography", 2013.

[4] T. Gao, Z. Chen, "Image encryption based on a new total shuffling algorithm," Chaos, Solitons and Fractals 38, pp. 213–22,2006.

[5] N.K. Pareek, V. Patidar, K.K. Sud, "Image encryption using chaotic logistic map," Image and Vision Computing 24, pp.926-934, 2006.

[6] H. Gao, Y. Zhang, S. Liang, D. Li"A new chaotic algorithm for image encryption," Chaos, Solitons and Fractals 29, pp.393-399,2006.

[7]A. Bakhshandeh, Z. Eslami, "An authenticated image encryption scheme based on chaotic maps and memory cellular automata," Optics and Lasers in Engineering 51, pp. 665–673,2013.

[8] C. Dong, "Color image encryption using one-time keys and coupled chaotic systems," Signal Processing-Image Communication, 2013.

[9] H.S. Kwok, Wallace K.S. Tang, "A fast image encryption system based on chaotic maps with finite precision representation", Elsevies, chaos, solitons and Fractals, 2006.

[10] Chin- Chen Chang, Tai-Xing Yu, "Cryptanalysis of an encryption scheme for binary images", pattern Recognition letters, 2002, pp: 1847-1852.

[11] S. Behnia, A. akshani, S. Ahadpour, H. Mohmodi, A. Akbavan, "A fast chaotic encryption scheme based on piecewise non linear chaotic maps", physics letters A, 2007, pp:391-396.

[12] Hossan El-din, Hamdy M. Kalash, and Osama S.Farag Allah, "An efficient choos-based feedback stream cipher (ECBFSC) for image encryption and decryption", proccedings IEEE international conference on
Chaotic system, vol. 4,2005, pp:126-133.

[13] Shujun Li I and Xuan Zheng, "On the security of an image encryption method", proceedings of the 2002 IEEE international conference on image processing (ICIP 2002), vol.2, pp: 925-928,2002

[14] Narendra Singh, Aloka Sinha, "Optical image encryption using fractional fourier transform and chaos". Optics and lasers in engineering. Vol, 46. Issue 2, pages 117-123. February 2008

[15] A. Mitra, Y.V. Subba Rao, and S.R. M. Prasanna, "A new image encryption approach using combinational permutation techniques", in ternational journal of computer science vol, 2006, pp:1306-4428.

[16] Shiguo Lian, JinshengSun, Zhiquan Wang Zh., "security analysis of a chaos based image encryption algorithm", elsevier, physica A, vol.351, pp. 645-661, 2005.

[17] Yas Abbas Alsultanny, "random bit sequence generation from image data "image and vision computing", 2007, pp: 1178-1189.

[18] Eduardo Bayro-Corrochano, "Handbook of Computational Geometry for pattern recognition, computer vision, neural computing and robotics", springer, 2003.

[19] Steven H. Strogatz, "Nonlinear Dynamics and Chaos". Westview Press, 1994.

[20]Savvas A. Chatzichristofis, Dimitris A. Mitizias, Georgious Ch. Sirakoulis, and Yiannis S. Boutalis, "A novel cellular automata based technique for visual multimedia content encryption".