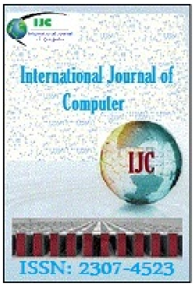
International Journal of Computer (IJC)

ISSN 2307-4531

http://gssrr.org/index.php?journal=InternationalJournalOfComputer&page=index



A New Image Encryption And Decryption Approach Based On Chaotic Analog Signal Generator

Mritunjay Singh[a*], Dr.Yogendra Kumar Jain[b], Ramratan Ahirwal[c]

[a,b, c] *Department of Computer Science and Engineering*
Samarat Ashok Techonological Institute, Vidisha (M.P.)

mri10cs@gmail.com[a]

ykjain_p@yahoo.co.in[b]

ram2004_ahirwal2004@rediffmail.com[c]

Abstract

In the last one and half decade, chaos has occurred as a new favorable candidate for network security because many chaos important features such as very much sensitivity to initial conditions and ergodicity, are directly related with two basic properties of cipher texts: confusion and diffusion. In this paper a new image encryption and decryption method is proposed which is based on the chaotic signal generator and 2D baker maps. A 144 bit external secrete key acts as the input of the chaotic signal generator. Baker maps used for the confusion of the main input image after that XOR operation used in diffusion process. The proposed method is simulated using Matlab and the results are secure with all type of cryptanalytic tests and statistical analysis tests.

Keywords: Analog signal generator, Baker maps, Differential attack, Chaotic maps, Statistical analysis, Key sensitivity test;

1. Introduction

In the last few years, the transfer of data by the use of communication media is drastically increases, data contains information in the form of text, image, and video. So the need of the security of data is also increases, but this need becomes necessary when the transmission media transfers high confidential data like military data, medical data and video conferencing etc. Traditional data encryption algorithms like Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES), linear feedback shift register (LFSR), etc.

----

* Corresponding author. Tel.:07869557989.
E-mail address: mri10cs@gmail.com.

These algorithms are suitable for the data which contains more text information but if the data contains more color image and video then this indicate that the message contains huge amount of data, in case of image there is a problem like high correlation between pixels, in such situation all these conventional algorithms not work properly[1,2]. So here is the necessity of some nontraditional algorithms, which are different from these conventional algorithms, it is the conditions where chaos based cryptosystem came in to the picture. Chaos systems have some basic properties like sensitive dependence on initial condition, ergodicity and mixing, all these properties are very useful in image encryption.

Many researchers study that there is a strong relationship between chaos and cryptography. It is appear that chaos system just like noisy system but in reality it is not, both are two different things chaotic systems are deterministic, so the precise knowledge of initial condition recovers the original message, by the use of this concept decryption process done. In recent years there are many chaos based cryptosystem has been proposed. Some papers are related to one dimensional chaotic map, these are used for data security in form of text or documents [3- 5] and many of them based on 2D or higher dimensional chaotic map, used for image encryption and decryption, we can think image as 2D array of pixels[6-13].

In [6], Fridrich proposed that image encryption method is basically divided in two parts confusion and pixel diffusion, confusion displays the permutation of the pixels and diffusion modify the values of the pixels. On basis of these concept, many chaotic maps used by the researchers for confusion process, For example, Chen and his research group working on three-dimensional 3D cat map [11] and a 3D baker map [12] in the permutation phase.Guan uses 2Dcat map for pixel location permutation [8]. The inclusion of chaos in data encryption is not new initially it was used by Shannon in 1949[14], but he not mention the term chaos he propose mixing and sensitive type words. The first paper on chaos is proposed in 1989, Matthews [15] proposed the idea of stream cipher based on one dimensional chaotic map. After one year Pecora and Caroll [16] give the concept of synchronization of chaotic system. After that chaotic cryptography divided in two completely different paths digital chaotic ciphers and chaos synchronization. In this paper, 2D baker map is used, so the basics of baker map given as follow:

The standard equation of baker map was presented in [6] and the equation is defined as

$$m_{i+1} = (m_i + n_i) mod 2\pi$$

$$n_{i+1} = n_i + k\,sin(m_i + n_i)\ mod 2\pi \qquad (1)$$

Where k>0 and k is the control parameter, m_i and n_i is the i^{th} value of input in between [0, 2 π)∀ i. The equation (1)

is continuous equation, this equation can be discretized by the use of given parameters x = m_iN/2π, y = n_iN/2π and K= kN/2π. Then the discrete equation is given as follow:

$$x_{i+1} = (x_i + y_i) mod\ N$$

$$y_{i+1} = \left(y_i + K\,sin\frac{x_{i+1}\,N}{2\pi}\right) mod\ N. \qquad (2)$$

Where K is a positive integer constant. The outcome of 2D baker map on the image of size 1×1 is given in figure 1.

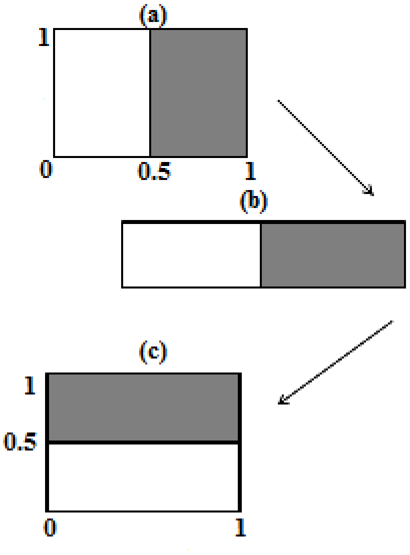
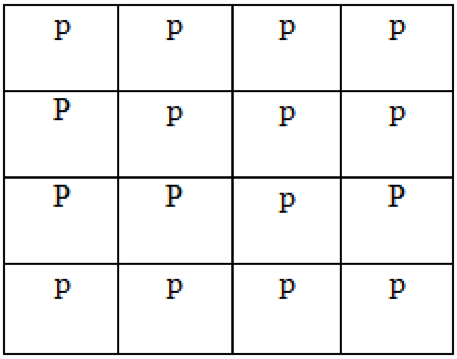


Fig. 1. Baker map concept.

This figure indicate that the initial above image (a) becomes lower image (c) if equation (2) apply on 1× 1 image, like this entire pixels of the image plane changes its location, this is the reason baker map is used in the confusion process of the proposed method.

A p added p value matrix is also used in the proposed method, Figure 2 shows the example of 5× 5 padded matrixes with value p, the matrix used in the proposed method is of size y × z, and all the elements of matrixes are p. where p is the output of the chaotic key generator, the decision of taking variable p is that p is a chaotic variable and it also change in the next new experiment.



p	p	p	p
P	p	p	p
P	P	p	P
p	p	p	p

Fig. 2. p value matrix.

2. Architecture of proposed chaos-based cryptosystem

The proposed chaos-based cryptosystem basically contains two stages first stage is confusion stage and second one is diffusion stage. The external secret key acts as the input of chaotic key generator, when key generator circuit runs the three independent loops in the proposed circuit flows current i_1, i_2andi_3, the magnitude of the currents are p,q and r which acts as the input of the confusion process. The output of the circuit shows, chaotic property so it is known as chaotic key generator.

The first stage is confusion process, in this process by the use of baker map the location of the pixel is scrambled over the entire image, but the value of the pixels becomes unchanged. In this stage the image becomes unrecognized, but it is not completely secure, it can be crack by cracker with some efforts.

In the second stage which is diffusion process, the value of the permuted pixel is scattered over the whole image, it is fundamentally pixel value modification stage. After pixel value modification stages the secrecy of the system becomes more and more strong. The whole process is repeated, in which confusion process repeats r-times and diffusion process repeats for x-times. After that final output cipher image is obtained, by the addition of all the output, final cipher image is obtained. The architecture of proposed chaos based cryptosystem given in figure 3.

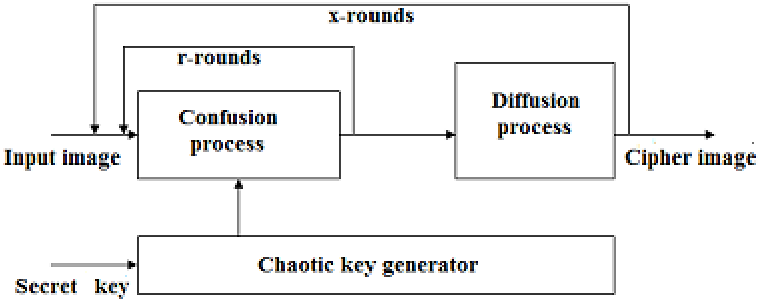


Fig.3 Architecture of proposed chaos based cryptosystem

3. Proposed method

In this part the proposed image encryption and decryption method will be discussed. The input image first processed by the confusion process then diffusion process occurs. The input values of the baker maps obtained by the use of nonlinear chaotic signal generator and external 144 bit secret key acts as the input of the circuit. The step by step discussion of proposed method is given as follow.

Step 1: Encryption Method: The external secret key used in this method is 144 bit long. First of all the secret key is divided in to three equal parts, so each part is 6 character or 48 bit long. All three keys act as the input constant of the circuit oscillator. After processing the chaotic signal generator produces three outputs, and all three outputs exhibits chaotic property, the output variables are p, q and r.

Step 2: Anothervariablek has been founded by the addition of variable p and q. The inputted image is converted in to 3D image. This 3D image is taken by the 2D baker map, one by one from top to bottom just like as pop operation in stack. By the use of variables p, q and k, the 2D baker map permutes the input image; this permutation process is repeated r-times. It is complete permutation stage.

Step 3: After that the diffusion process is started, in this process the XOR operation is performed, one operand in this operation is output of the confusion process(step 2) and another is same size constant p value matrix. This diffusion process repeated x-times.

Step 4: All 2D cipher image is layered one by one x-time, and after that it becomes output 3D cipher image and finally this 3D cipher image is converted in to 2D cipher image. This is the complete encryption process.

Step 5: Decryption Method: This is similar to encryption process but some steps are reverse. First step is same as the encryption method. The second step of decryption is same as the third step of the encryption method, only difference is that here the input image is the cipher image in place of plain image. The XOR operation is performed by the use of p value matrix and same size cipher image. In third step the 2D baker map is used, the output of the second step acts as the input of the baker map. Fourth step is similar as the encryption method. The output of the decryption method is the same plain image.

4. Experimental Results

The proposed cryptosystem uses 256×256 colored images for the result analysis, any proposed method is good if it resist all kind of attacks like cipher-text only attack, known/chosen plain-text attacks, differential attack, statistical attack, and various brute-force attack. The security analysis performed in this paper is key space analysis, key sensitivity test, histogram analysis, correlation coefficient and entropy analysis, all these experiments proves that proposed method fulfill all the results nicely.

4.1. Key space analysis

The key space analysis mainly gives the security knowledge of bruite-force attacks of the proposed method, large key space makes bruite-force attack infeasible. In proposed method the size of key is 18 characters so the external key is 144 bit long it will take total 2144 or 2.33×1043 attempts to crack the system security. This proves that it will take very much time to break the security of the proposed method. So the proposed method is secure against bruit-force attacks.

4.2. Key sensitivity test

In this test the waterfall image of size 256× 256 is used for experiment. In this key sensitivity test we use keys for encryption and decryption, if the least significant bit of key has changed for decrypted image two times and then experiments are performed two times, after finding two decrypted image, we take the difference between two images. In the proposed method the difference between two cipher images is 99.34% means both the images are very much different, if we change only one bit. It indicates that the attackers cannot find the real image if they have cipher image. And subsequently if the same key is used in experiment which is used for encryption process then the result is same waterfall image. The result of this test shown in figure 4.

4.3. Histogram analysis

Histogram analysis gives the idea to statistical analysis attackers, but in this proposed method by the use of histogram the attackers cannot find the any clue about the original image. The proposed method gives the original image and cipher image histogram, which is shown in figure 5; it shows that the cipher image histogram is completely horizontal so if any statistical attackers attack, then opponent cannot break the proposed security. In this method the cipher image red, green and blue histograms are flat because of diffusion method, which altered the original values of pixels. Nearly horizontal histogram proves that this proposed method is secure from external users.

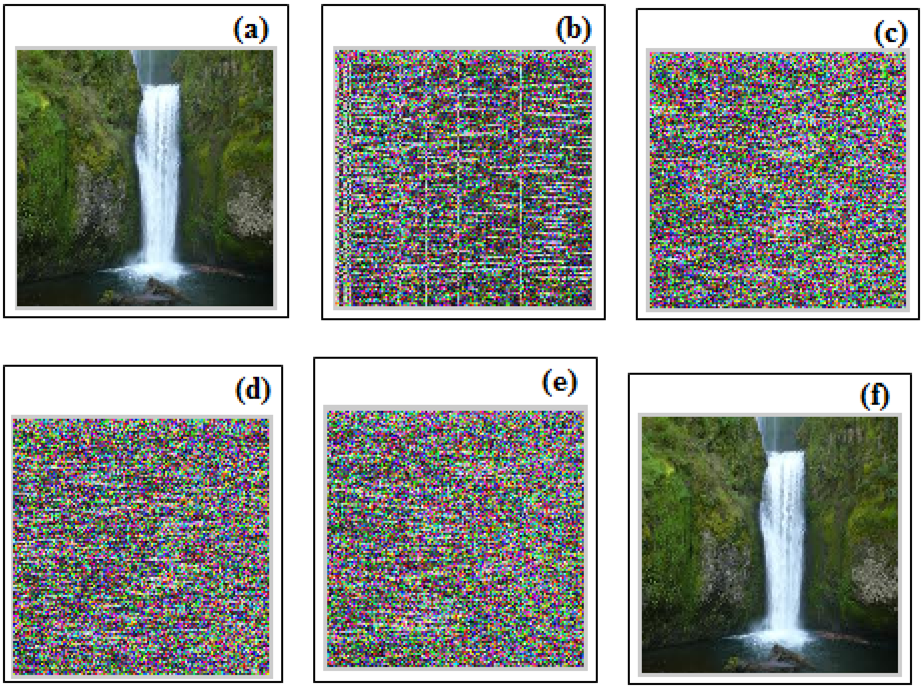


Fig.4. Key sensitivity test: figure (a) shows the original image figure (b) encrypted image by the use of key 02w3e4r5t6y7A8i9D7 figure (c) decrypted image by the use of key02w3e4r5t6y7A8i9D6 figure (d) decrypted image by the use of key12w3e4r5t6y7A8i9D7 figure. (e) difference image offigure (c) and (d). (f) decrypted image by the use of key 02w3e4r5t6y7A8i9D7.

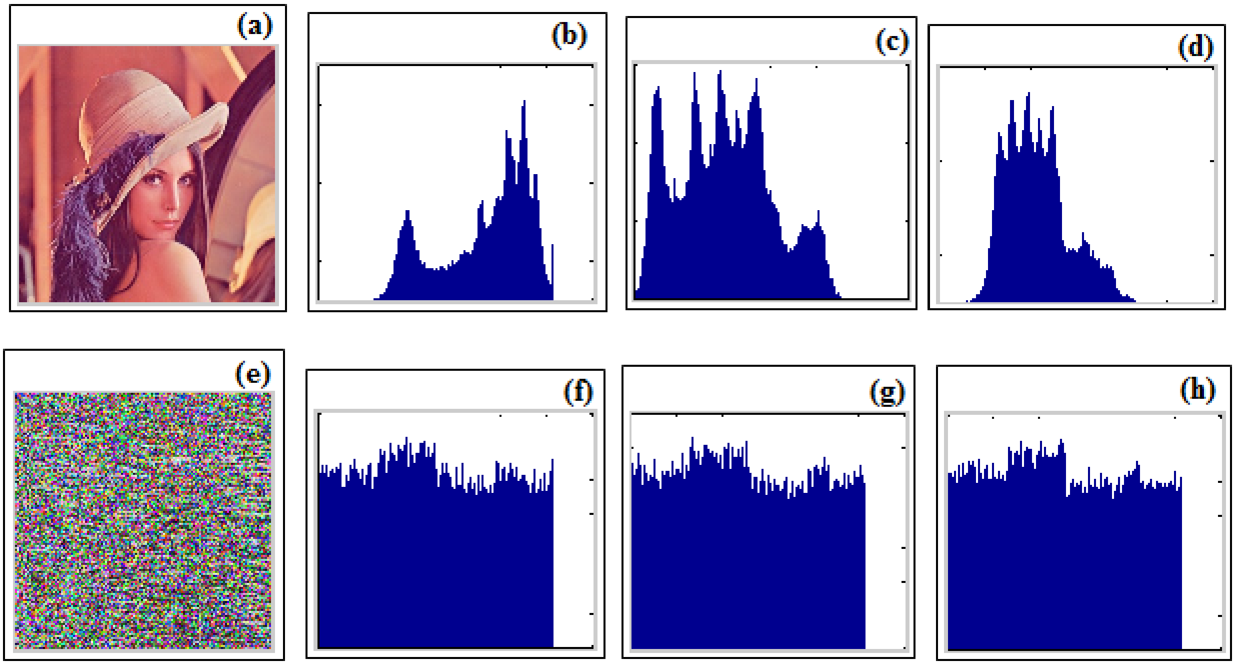


Fig.5. Histogram analysis (a) shows original image histogram. (b), (c) and (d) shows histogram of the red, green and blue color of the original image. (e) show the encrypted image of the plain image key 12w3e4r5t6y7u8i9o0. (f) (g) and (h) shows histogram of the red, green and blue color of the cipher image.

4.4. Correlation coefficient analysis

The correlation coefficient give the relationship between two neighboring pixels, if correlation between two pixels is nearly 1 then the image is highly correlated but if it is nearly 0 the image pixels are highly uncorrelated. In the proposed method the experiments on the images proves that the original image correlation nearly one, and cipher image correlation is nearly zero. So this saves the system from statistical attacks. Table 1. (a) and Table 1. (b) show the results of experiments. The formula of correlation coefficient of two adjacent pixels gives as follow:

$$cov(x,y) = E\big(x - E(x)\big)\big(y - E(y)\big),$$

$$r_{xy} = \frac{cov(x,y)}{\sqrt{var(x)}\ \ \sqrt{var(y)}}$$

Where x and y are the values of two adjacent pixels in the image. We can calculate cov(x,y) , var(x) and var(y) by the use of following equation.

$$E(x) = \tfrac{1}{N}\textstyle\sum_{i=1}^{N} x_i, \qquad var(x) = \tfrac{1}{N}\textstyle\sum_{i=1}^{N}(x_i\ - E(x))^2 \text{and}$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}\big(x_i - E(x)\big)\,(y_i - E(y))$$

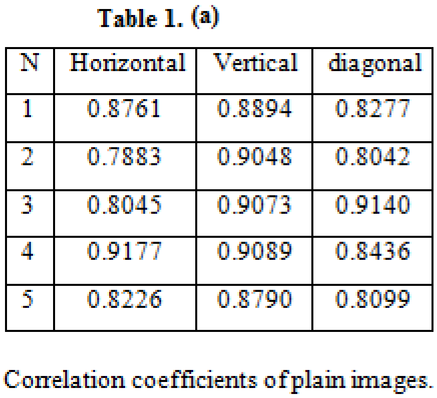


Table 1. (a)

N	Horizontal	Vertical	diagonal
1	0.8761	0.8894	0.8277
2	0.7883	0.9048	0.8042
3	0.8045	0.9073	0.9140
4	0.9177	0.9089	0.8436
5	0.8226	0.8790	0.8099

Correlation coefficients of plain images.

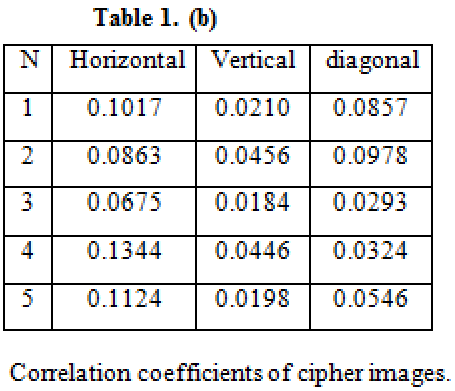


Table 1. (b)

N	Horizontal	Vertical	diagonal
1	0.1017	0.0210	0.0857
2	0.0863	0.0456	0.0978
3	0.0675	0.0184	0.0293
4	0.1344	0.0446	0.0324
5	0.1124	0.0198	0.0546

Correlation coefficients of cipher images.

The distribution of pixels of plane image and cipher image is shown in figure 6. In this figure horizontal, vertical and diagonal pixel distribution is presented for an image.

4.5. Information entropy *analysis*

Illegibility and indeterminateness are the chief objectives of image encryption. This indeterminateness can be displays by one of the most commonly used notional measure of entropy. Entropy states the degree of uncertainties in the system and the formula of entropy is given as follow:

$$H(s) = -\sum_{i=0}^{N-1} P(s_i)\log_2 p(s_i)$$

Where p(s_i) is the beginning probability of s_i. If each symbol has an equal probability, i.e.s=($s_0, s_1, s_2 \ldots \ldots . s_{256}$) where p($s_i$) is equal to $\frac{1}{2^8}$ then the entropy is $H(s)$=8. This resembles to an ideal case. Practically the entropy of the systems is less than the ideal case in the proposed image encryption method the entropy of the encrypted images close to 8, the information entropy of different encrypted images given in table 2. So the very less information outflow in the proposed cryptosystem, this proves that the proposed method is secure against entropy attacks.

Table 2 Entropy of Different encrypted images.

256×256(images) N	Entropy
1	7.9756
2	7.9728
3	7.9962
4	7.9726
5	7.9810

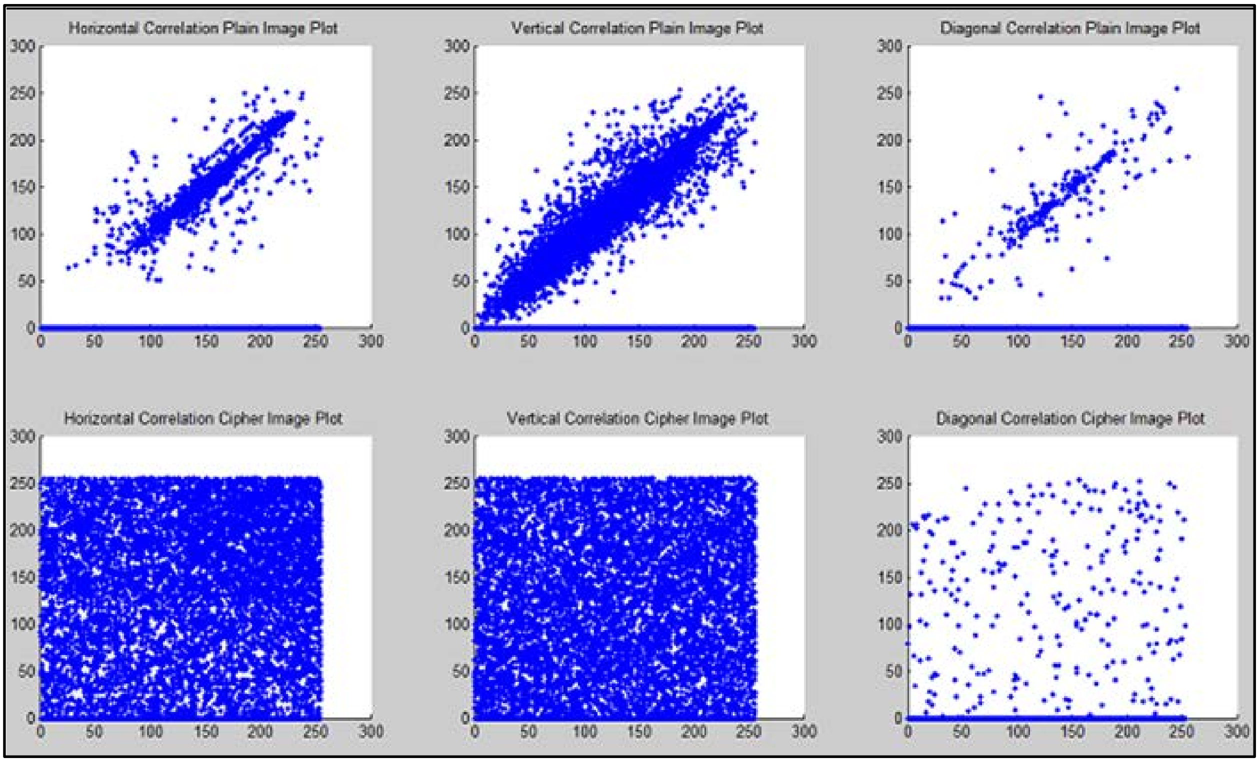


Figure 6. Correlation coefficient of pixels in the plain image and cipher image.

5. Conclusion

In this paper we present a new method of image encryption and decryption, proposed nonlinear oscillator produces chaotic keys, these keys are very much sensitive to initial condition, the 2D baker maps and XOR operation completes the confusion and diffusion process. All the experimental analysis show that the proposed image encryption system has (1) a very large key space (2) strongly sensitive to secrete key (3)effectivehistogram analysis (4)correlation coefficient analysis secure from statistical attacks (5)information entropy analysis give security of information leakage. These five experiments show that this proposed method is very robust and also saves the system from external attackers.

References

[1] Schneier, B.," Applied Cryptography - Protocols, Algorithms, and Source Code, second ed., C," John Wiley & Sons, Inc., New York, 1996.

[2] Daemen, J.; Sand, B.; Rijmen, V, " The Design of Rijndael: AES - The Advanced Encryption Standard,"Springer-Verlag, Berlin, 2002.

[3] Baptista MS., "Cryptography with chaos," Phys Lett A 1998;240(1-2):50-4.

[4] Wong KW, " A fast chaotic cryptography scheme with dynamic look-up table," Phys Lett A 2002;298:238-42.

[5] Pareek NK, Patidar V, Sud KK, "Discrete chaotic cryptography using external key," Phys Lett A 2003;309:75-82.

[6] Fridrich J, "Symmetric Ciphers Based on Two-dimensional Chaotic Map," Int. J. Bifurcat Chaos 1998;8(6):1259 84.

[7] Belkhouche F, Qidwai U, Gokcen I, Joachim D "Binary image transformation using two-dimensional chaotic maps," In: Proc ICPR 2004, Aug 2004, p.823-6.

[8] Guan ZH, Huang FJ, Guan WJ "Chaos-based image encryption algorithm," Phys LettA 2005;346:153-7.

[9] Lian SG, Sun J, Wang Z, "A block cipher based on a suitable use of chaotic standard map," Chaos, Solitons and Fractals 2005;26(1):117-29.

[10] Feng Y, Li LJ, Huang F, "A symmetric image encryption approach based on line maps," In: Proc ISSCAA 2006, Jan 2006, p. 1362-67.

[11] Chen G, Mao YB, Chui CK, " A symmetric image encryption scheme based on 3D chaotic cat maps," Chaos, Solitons & Fractals 2004;12:749-761.

[12] Mao YB, Chen G, Lian SG, "A novel fast image encryption scheme based on the 3D chaotic baker map," Int. J. Bifurcat Chaos 2004;14(10):3613-24.

[13] Lian SG, Sun J, "Wang Z. Security analysis of a chaos-based image encryption algorithm," Physica A 2005;351:645-61.

[14] Shannon CE, "Communication theory of secrecy system," Bell System Technical Journal 28:656 – 715, 1949.

[15] Matthews R.,"Cryptologia" 1989, XIII, 29–42.

[16] Pecora, L. M.; Carroll, T. L. Physical Review Letters, 1990, 64, 821–824.