ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 3, Issue 4, April 2016

A Study on Comparison of Various Image Encryption schemes based on Chaotic Maps

[1]Rachit Jain, [2] J.B.Sharma
[1] MTech, Digital Communication, Scholar, [2] Associate Professor, Electronics Department
U.C.E, R.T.U, KOTA
[1] racjain11@gmail.com,[2] jbsharma@rtu.ac.in

***Abstract*- This paper shows the study on image encryption scheme using different Chaotic Maps. The main purpose is security management in transmission and storage. There are various image encryption techniques which have been continuously studied to fulfill the demand of real-time secure image transmission through wireless networks and over the Internet. Conventional image encryption methods like data encryption standard (DES), has the weakness of low-level efficiency and high redundancy when the image is large. The chaos-based image encryption technique provides an efficient way to deal with the difficult problems of high security, pseudorandom property, topological transivity and fast image encryption. The objective of this paper is to compare Logistic map, Baker map and Arnold cat map image encryption techniques by visually, statistically and noise analysis to get an efficient approach of image encryption.**

***Keywords* – Chaotic Maps, Logistic map, Baker map, Arnold cat map, Image Encryption.**

I. INTRODUCTION

Security of image data nowadays becomes an important over the internet communication, medical imaging, military Communication, and Tele-medicine etc [1]. Image encryption techniques are very efficient in protection of secret information i.e. conversion of plain-image into a cipher-image which is unreadable to anyone without decrypting the encrypted data. Decryption means converting the encrypted data into its original data to make it readable [2]. Image encryption transports the image securely over the network such that no unauthorized user can able to decrypt it. The progression of encryption is moving towards a future where the image data have special properties such as, high redundancy, bulk capability and high correlation among the pixels.

In this process the special mathematical algorithms and keys are used to transform digital data into cipher code before they are transmitted and decrypt it. Image encryption algorithms are classified on value transformation[3-4], position permutation and visual transformation based algorithm [5]. Many schemes are proposed [6] using permutation and substitution methods to provide high security and enhance the pseudorandom characteristics of chaotic systems. Similarly, another method by Huang-Pei Xiao et.al [7] made combination of two chaotic systems. First system generates a chaotic sequence, which was changed into a binary stream function and the second chaotic system constructs the permutation matrix. In this the binary stream act as a key stream, randomize the pixel values of image then encrypts the image again by permutation matrix.

This paper contains V sections those include an introduction in section I which gives the brief knowledge of need of security required during image communication. Then section II discussed about the various chaotic maps used for image encryptions. Section III shows the simulation results on different type of images which are performed by the techniques discussed in the above section. Then in section IV the performance parameter evaluation is done using different analysis. In the end of the paper section V concludes the above comparison and the efficient method which is to be used by image encryption algorithm for security of an image.

II. DIFFERENT TYPES OF ENCRYPTION TECHNIQUES

Chaos-based cryptography [8-10] is depends on the complex dynamics of nonlinear systems or maps which are deterministic but simple. Hence, it provides a secure and fast means for data protection. It seems to be a good due to its complex dynamics and periodicity. Chaotic systems are assumed to work in the real number domain, and hence there speed is limited for actual implementation [11-13]. They also have various features like secure communications,

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 3, Issue 4, April 2016

such as sensitivity to initial conditions, periodicity, control parameters and random like behavior.

A: Logistic Map:

The nonlinearity based property makes the logistic map famous for its encryption process, in which random behaviors are predictable from simple applied equations. The chaotic map such as logistic map [14], a bounded random iterative sequences can be generated having the non-correlation, ergodicity and pseudo-randomness properties. The one-dimensional nonlinear logistic map function is:

$$f(y) = qy(1-y) \quad (1)$$

the system parameter is bounded for $0 \leq q \leq 4$, which is known as bifurcation parameter. The iterative form is given by

$$y_{n+1} = qy_n(1-y_n) \quad (2)$$

where $y_n \in (0, 1)$ is the iterative value and y_0 is the initial value. The dynamical systems are in chaotic state under the condition $q \in [3.5699456, 4]$.

B: Baker Map:

To remove the strong correlations between the adjacent pixels of an image, the random permutations based chaotic Baker map is applied to shuffle the pixel positions of the plain image. The discretized form of Baker map [12] provide us best results for its performance and key space. In this method, chaotic bijection of the unit square $N \times N$ on the square itself. As described in Fig.1, a $M \times M$ image is firstly divided into k vertical rectangles of height M and width m_i (i=0, 1, …, k-1), such that all m_i divide the side length M and $m_0+m_1+ \ldots +m_{k-1}= M$. Then, these columns in form of rectangles are extended in the horizontal rows and compressed in the vertical columns to obtain a horizontal rectangle rows. Then these horizontal rows are piled on each other to give the shuffled image. The discretized Baker map transform is given by:

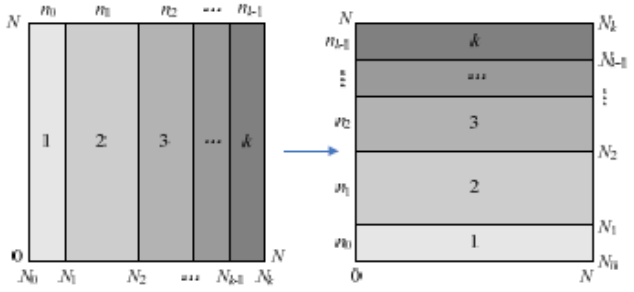


Fig.1Discretized Baker Map

$$B_{(n1,n2,n3,\ldots,nk)}(z,s) = \left[\frac{M}{m_i}(z-M_i) + s \bmod \frac{M}{m_i}, \frac{m_i}{M}(s - s \bmod \frac{M}{m_i}) + M_i\right]$$

where the pixel at the position (z,s), with $M_i \leq z < M_i + m_i$ and $0 \leq s < M$.

C: Arnold Cat Map:

The Arnold cat map is a 2-D chaotic map used to encrypt the image by shuffling the pixels of the plain image in diagonal manner [15-16]. Without loss of generality,

we assume the dimension of the original image to be $S \times S$. The coordinates of the pixels are N = {(a, b) | a, b= 0, 1, 2,3..... S-1}. The 2-D Arnold cat map can be described as follows:

$$\begin{bmatrix} a' \\ b' \end{bmatrix} = A \begin{bmatrix} a \\ b \end{bmatrix} (\bmod S) \quad (4)$$

$$= \begin{bmatrix} 1 & x \\ y & xy+1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} (\bmod S)$$

here $\begin{bmatrix} a \\ b \end{bmatrix}$ and $\begin{bmatrix} a' \\ b' \end{bmatrix}$ shows the pixel positions before and after applying the Arnold cat map transformation respectively and x and y are positive integers, det(A) = 1. The application of Arnold transformation is based on iterations 'I' which shuffles the pixels of original image in order to give encrypted image. The number of iterations I works as a secret key for the encryption and decryption process and depends on the parameters x, y and the size S of the plain-image. After several iterations, the correlation among the adjacent pixels is reduced completely to provide highly secured image.

III. SIMULATION RESULTS

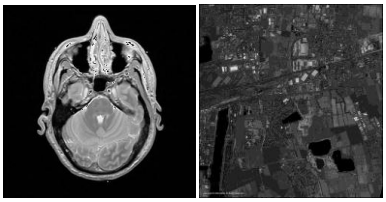
Simulations are performed using matlab on four different standard gray scale test images of dimension 472 x 472 as shown in fig.2(a-d) using three types of chaotic maps. Security analysis such as statistical, noise immunity [19] are done on the Barbara, Pepper, medical image [17] and satellite image [18] and the results for each analysis are tabulated. In fig.3 the following encrypted and decrypted

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 3, Issue 4, April 2016

images of the given images using logistic map, Baker map and Arnold map are shown.

(a.) (b.)



(c.) (d.)

Fig.2 Test images (a.)Barbara (b.)Pepper (c.) Medical image (d.) Satellite image.

(3

IV. PERFORMANCE ANALYSIS

An efficient encryption scheme should be robust against different kinds of attacks such as statistical, cryptanalytic and brute-force. In this section, the various security analysis is performed on various chaotic maps such as statistical analysis, peak signal noise ratio (PSNR), mean square error (MSE) and computational time to compare and gives the best method which is secure against attacks.

A. Histogram Analysis:

Image histogram illustrates the distribution of image pixels with the number of pixels at each intensity level. It is visually clear from fig.4 that the histograms of the encrypted images for different chaotic maps are different from the histograms of original image respectively and the histograms of decrypted image is similar to histograms of plain-image. Hence does not provide any hint to employ any statistical attacks.

B. Correlation Coefficient:

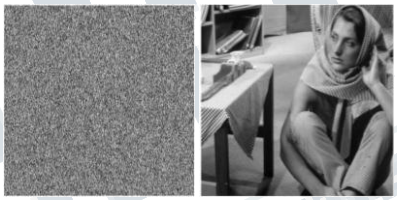
It computes the value of similarity between the pixels of the original and the encrypted image at same position. The correlation coefficient is calculated by:

$$r = \frac{\mathrm{cov}(f,\psi)}{\sqrt{D(f)\times D(\psi)}} \quad D(f) = \frac{1}{L}\sum_{l=1}^{L}(f_l - E(f))^2$$

$$\mathrm{cov}(f,\Psi) = \frac{1}{L}\sum_{l=1}^{L}(f_l - E(f))(\Psi_1 - E(\Psi)) \qquad (5)$$

where f and ψ are gray-scale pixel values of the original and encrypted images. Smaller the value of coefficient better the quality of encryption system. Table 1 shows the correlation coefficient values between the original image and the encrypted image for different chaotic maps using different types of images.

Encrypted Image ***Decrypted Image***



(a.) Logistic Map

(b.) Arnold Cat Map

(c.) Baker Map

Fig. 3 Encrypted and Decrypted images using different chaotic maps (a), (b) and (c)for above images.

Baker Map	Logistic Map	Arnold Cat Map

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 3, Issue 4, April 2016

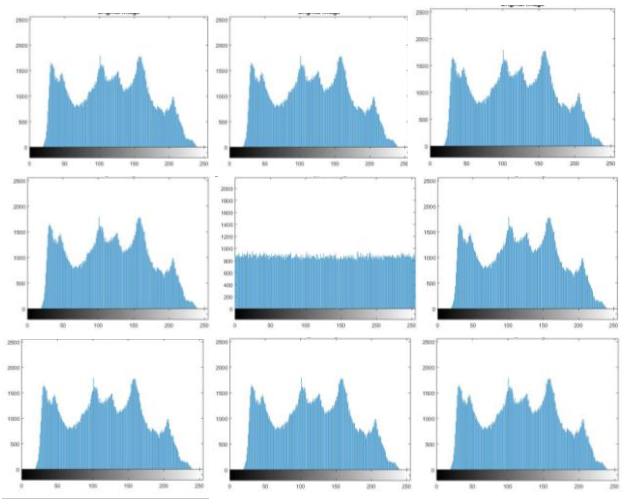


Fig. 4 Histogram outputs of original, encrypted and decrypted image for different chaotic maps for Barbara image.

C. Mean Square Error (MSE):

It is the squared error between recovered image and the original image. The lower MSE value means lower the error. The MSE is defined by

$$MSE = \frac{1}{XY}\sum_{x=1}^{X}\sum_{y=1}^{Y}| f(x,y) - \hat{f}(x,y) |^2 \qquad (6)$$

$f(x,y)$ and $\hat{f}(x,y)$ which represents the original and the decrypted images, respectively. The MSE values for the various chaotic systems are comes out low for the following images.

D. Peak Signal Noise Ratio (PSNR):

The reliability of different schemes is evaluated by PSNR value. More the PSNR value, the quality of image encryption is better but for encrypted image its value is low desired. PSNR is calculated by:

$$PSNR = 10\log_{10}\left(\frac{R^2}{MSE}\right) \qquad (7)$$

Table 2 shows the high value of PSNR for the decrypted image in presence of Gaussian noise with variance 0.1 after the encryption process. In compare to other two chaotic maps, Logistic map based encryption process gives high PSNR values.

TABLE 1. CORRELATION COEFFICIENT USING DIFFERENT CHAOTIC MAPS FOR DIFFERENT IMAGES.

S.No.	Images	Logistic Map	Baker Map	Arnold cat Map
1	Barbara	0.0222	0.0315	-0.0139
2	Pepper	0.0063	-0.0408	0.0232
3	Medical Image	-0.0238	0.2517	0.0089
4	Satellite Image	0.0084	0.0405	0.0064

TABLE 2. PSNR (dB) VALUES OF DECRYPTED IMAGE FOR DIFFERENT CHAOTIC MAPS.

S.No.	Images	Logistic Map	Baker Map	Arnold cat Map
1	Barbara	33.2150	27.9890	37.7086
2	Pepper	4102506	27.1105	34.1804
3	Medical Image	42.0275	26.4124	40.0670
4	Satellite Image	40.8024	27.8505	31.4188

V. CONCLUSION

This paper analyses the performance of various image encryption process such as Logistic map, Baker map and Arnold cat map. The chaotic maps are based on the concept of shuffling and changing the values of image pixels. To perform the shuffling Baker map and Arnold cat map are used and Logistic map to provide security. These encryption techniques are compared and analyzed to give the best performance. All the simulation and experimental analysis show that the Logistic map based encryption leads to low correlation value in compare to other methods. Hence, the analysis and comparison proves the security, effectiveness and robustness of the various chaotic maps.

REFERENCES

[1] Ephin M, Judy Ann Joy and N. A. Vasanthi, " Survey of Chaos based Image Encryption and Decryption Techniques " , *Amrita International Conference of Women in Computing (AICWIC'13) Proceedings published by International Journal of Computer Applications (IJCA).*

[2] John Justin M, Manimurugan S , "A Survey on Various Encryption Techniques ", *International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March 2012.*

[3] S.S.Maniccam, N.G. Bourbakis, "Lossless image compression and encryption using SCAN", *Pattern Recognition 34,1229- 1245,2001.*

[4] Aloha Sinha, Kehar Singh, "A technique for image encryption using digital signature", Optics Communications, Vol-2 I 8 (2203),229-234.

[5] Jiun-In Guo, Jui-Cheng Yen, "A new mirror-like image Encryption algorithm and its VLSI architecture", *Pattern Recognition and Image Analysis, vol.IO, no.2, pp.236-247, 2000.*

[6] Guosheng Gu ,Guoqiang Han, "An Enhanced Chaos Based Image Encryption Algorithm", *IEEE Proceedings of the First International Conference on Innovative Computing, Information and Control (ICICIC'06) in 2006.*

[7] Huang-Pei Xiao Guo-Ji Zhang, "An Image Encryption Scheme Based On Chaotic Systems", *IEEE Proceedings of the Fifth International Conference on Machine Learning and Cybernetics, Dalian, 13-16 August 2006.*

[8] Behnia S, Akhshani A, Mahmodi H, Akhavan A." A novel algorithm for image encryption based on mixture of chaotic maps." Chaos Soliton Fract 2008;35(2):408–19.

[9] F.Y. Sun, S.T. Liu, Z.Q. Li, Z.W. Lu, "A novel image encryption scheme based on spatial chaos map," Chaos Solitons & Fractals, vol. 38, no. 3, pp. 631-640, 2008.

[10] V. Patidar, N.K. Pareek, K.K. Sud, "A new substitution-diffusion based image cipher using chaotic standard and logistic maps*," Communications in Nonlinear Science and Numerical Simulation*, vol. 14, no. 7, pp. 3056-3075, 2009.

[11] K.W. Wong, B.S.H. Kwok, C.H. Yuen, "An efficient diffusion approach for chaos-based image encryption," *Chaos Solitons & Fractals*, vol. 41, no. 5, pp. 2652-2663, 2009.

[12]J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *International Journal of Bifurcation and Chaos*, vol. 8, no. 6, pp. 1259-1284, 1998.

[13]Y. Honglei, W. Guang-shou, W. Ting, L. Diantao, Y. Jun, M. Weitao, F. Y. Shaolei, andM. Yuankao, "An image encryption algorithm based on two dimensional Baker map," in *Proc. ICICTA*, 2009.

[14] Sui, L., Duan, K., Liang, J. Double-image encryption based on discrete multiple-parameter fractional angular transform and two-coupled logistic maps. *Opt. Commun.* 2015;343:140–149.

[15] Zhenwei Shang, Honge Ren, Jian Zhang. 2008.A Block Location Scrambling Algorithm of Digital Image Based on Arnold Transformation. The 9 th International Conference for Young Computer Scientists, 978-0-7695- 3398-8/08/$25.00 © IEEE.

[16] Zhu Liehuang, Li Wenzhuo, Liao Lejian, LiHong. 2006. A Novel Algorithm for Scrambling Digital Image Based on Cat Chaotic Mapping. Proceedings of the 2006 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP'06), 0-7695-2745-0/06© IEEE.

[17] [Online] Medical image source: https://www.nlm.nih.gov/research/visible/mri.html

[18] [Online] Satellite image source: http://www.satimagingcorp.com/

[19] Zhai, Y., Lin, S., Zhang, "Improving image encryption using multi-chaotic map," Proceedings of the Power Electronics and Intelligent Transportation System *(PEITS)*, pp. 143–148, 2008.