A COMPARATIVE STUDY OF IMAGE ENCRYPTION TECHNIQUES USING CHAOTIC MAPS

Bhagyashri R. Pandurangi[1],Dr.MeenakshiR.Patil[2] ,Vinay Sangolli[3]

[1]AssistantProfessor, Department of Electronics and Communication,

KLS Gogte Institute of Technology, Belgaum (India)

[2]Principal, Jain A.G.M Institute of Technology, Jamkhandi, (India)

[3]Department of Electronics and Communication, Jain College of Engineering, Belgaum (India)

ABSTRACT

For secure image encryption techniques Chaos Based cryptographic algorithms have suggested some new and efficient ways. Image encryption based on chaos became very popular for cryptography since properties of chaos are related to confusion and diffusion, two basic properties of good cipher. In this paper the encryption algorithms using chaotic maps are proposed. The two algorithms proposed are encryption algorithms using compound sine and cosine chaotic map and encryption algorithm based on logistic map. Experiments are performed in Matlab. In order to evaluate performance, the proposed algorithms are tested to measure the security and effectiveness. These tests includes visual test through histogram analysis, correlation coefficient analysis, information entropy test, measurement of encryption quality and time taken analysis.

Keywords*: *Cryptography, Chaotic maps, Decryption, Image processing, Symmetric Encryption

I. INTRODUCTION

Cryptography is the science of information security. It deals with hiding the private information. Cryptography is a method where in the data with useful information referred to as plain image is converted into random image referred to as cipher image with the help of cipher i.e., algorithm and key. Visual images play a vital role in information sharing. Due to extensive use of computers data integrity is of major concern. Chaotic systems are defined on real numbers. Any encryption algorithm which uses chaotic maps when implemented on a computer finite-state machine becomes a transformation from a finite set onto itself. Because of its wide dynamic range, the floating-point implementation seems to be the most appropriate for software implementation of chaotic maps. Conventional image encryption algorithms like DES, AES etc take more computational time and power especially when the image is large. Whereas most of the multimedia applications like image transmission, video etc require less computational time and power. Chaos based encryption algorithms offer good computational efficiency along with the combination of secure image encryption, speed for all the practical purposes. Chaotic systems are defined as dynamical systems with the following three properties: sensitivity to initial conditions, topological mixing, and density of periodic orbits.

Chaos-based encryption algorithms are performed in two stages, confusion and diffusion. Usually a single chaotic map or a set of maps are used for the generation of security keys. Mintu Philip[1] proposed encryption algorithm based on coupled chaotic map. The most important components of image are selected and encrypted.

In [2] the two-dimensional chaotic cat map is generalized to three dimensional for designing a real-time secure symmetric encryption scheme. The most commonly used chaotic maps used for chaotic image encryption are the baker map, tent map, the standard map [3-9]. Paper [9] employs the properties of chaotic systems to design a random bit generator, called CCCBG (Cross coupled Chaotic Based Bit Generator). In [10], image is partially encrypted using phase manipulation and sign encryption. Sign encryption finally provides the partially encrypted image by extracting the sign bits of modified image. In [11], invertible two-dimensional chaotic maps are employed on a torus or on a square for encryption using asymmetric block encryption schemes. Paper [12] describes a symmetric key block cipher algorithm which uses multiple one-dimensional chaotic maps instead of a one-dimensional chaotic map. For gray scale image there is no need of color transformation. Paper [13] describes a data hiding and extraction procedure for AVI videos by inserting the secret message bits in the DCT higher order co efficients. This method is tested for 28 frames by embedding 128 ×128 image.In [15] the Henon chaotic map is used for generation of keys and layered encryption technique for enhanced security along with color transformation technique for separation of color components in RGB images.

II PROPOSED WORK

2.1 Encryption Algorithm Based On Sine and Cosinechaotic Map

The proposed method is simple but highly secured image encryption and decryption algorithm which uses compound sine and cosine maps. The process starts by reading the size of the read image. The image is then prepared for diffusing. The original image is subdivided into three sub images based on the color component that is R, G and B planes. Each sub image is then converted into matrix with the pixel values in them and each pixel is converted into eight bit binary value, thereby resulting in binary matrix. Each pixel will be separated into eight planes corresponding to binary bits, there by resulting in 24 sets of bit plane images represented in matrix forms with single binary number in each pixel, these pixels are further ready for E-XOR with the keys.

The size of the input key is 16 alphanumeric characters which are used to form two set of ASCII codes, X_m and Y_m for setting initial conditions and parameters. The values of m range from 1 to 8. These values are converted into 48 bit binary values which are used in the equations below for the generating initial conditions and the control parameters.

$$R_{Xm} = \frac{(B_{X1} \times 2^0 + B_{X2} \times 2^1 + \ldots + B_{X48} \times 2^{\cdot}}{2^{48}} \quad (1)$$

$$R_{Ym} = \frac{(B_{Y1} \times 2^0 + B_{Y2} \times 2^1 + \ldots + B_{Y48} \times 2^{\cdot}}{2^{48}} \quad (2)$$

Therefore, the values of initial conditions and parameters are genereated using the R_j and R_1 values

$$a_m = (R_{Xm} \times R_{Ym}) mod \quad (3)$$

$$b_m = (R_{Ym} \times R_{Ym+1}) mod \quad (4)$$

The value generated by equations are too small to generate the required chaos, therefore they are enhanced by iterating 100 times. These iterated values will be used in the compound sine and cosine chaotic map equations to

generate the key

$$x_{n+1}=\cos a x_n+\sin b \quad (5)$$

The initial value of x_n will be 0.5.

These generated chaotic bits from (5) are XORed with the 24 sets of bit planes. The XOR operation gives the result as "0" if two input bits are similar and "1" if the two input bits are different. The result obtained by this XOR operation is 24 matrices with single binary number in each pixel. As a result, the encrypted image is obtained.

The decryption process is exactly the reverse process of encryption with the input image as the encrypted image, and the security keys being shared with the decryption algorithm.

2.2Encryption Algorithm Based On Logistic Map

The proposed encryption algorithm makes use of the logistic map for the generation of initial conditions and parameters.

Step 1: The read color image is divided into three sub images based on R, G & B components.

Step 2: Then value from each sub image is converted into binary value. These values are converted into column matrix and resized by combining with the size of the image.

Step 3: This is repeated for all the sub images, these sub images are concatenated to form one single binary image which is used to do bit XOR with the key.

Step 4: The initial value of the parameter 'a' is chosen as 4 in equation (9). As the signal generated by these values (3.57 to 4) is completely chaotic.

$$\mathbf{Y_{n+1} = a\, X_n\, (1 - X_n)} \qquad (9)$$

Step 5: The input key will be seven bit alphanumeric which will be stored as an ASCII number, this input key will be converted into binary number which is of length 40 bits. Finally by using equation (10) the initial value for starting the execution of the chaotic function logistic map is obtained.

$$U = P_{1,1} \times 2^{39} + \cdots \ldots + P_{5,8} \times 2^0 / 2 \quad (10)$$

Step 6: The image is read part by part, for encrypting the pixels in each part of the image, the initial value of that part and equation (10) are used as follows.

$$\textbf{New value} = \textbf{Round (U)} \oplus \textbf{Old value} \quad (11)$$

The bits generated by the chaotic series are bit XOR ed with the binary images there by resulting in an encrypted binary values.

Step 7: These values are used to reconstruct the image. The first step will be to separate the R, G and components.

Step 8: These components are converted into column vectors and are stored as binary values. These values are stored in their respective planes. This procedure is repeated for green and blue components also. The stored binary values from the respective planes are fetched and are converted into the decimal values.

Step 9: Finally these decimal values of all the planes are concatenated to form the encrypted image.

The decryption algorithm is similar to the encryption algorithm but receiving encryption key and operating with the encrypted image.

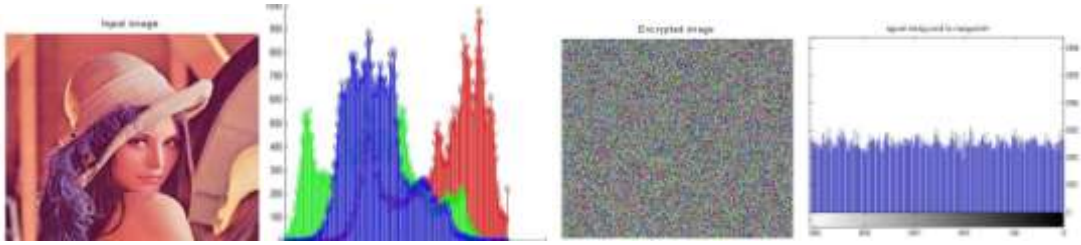
III. SECURITY TEST AND COMPARATIVE STUDY

3.1Statistical Analysis

To prove the robustness of the proposed image encryption procedure, Statistical analysis is supported by the histograms, the correlation between two adjacent pixels in the encrypted images and the correlation coefficient for several plain images and their corresponding encrypted images.

3.1.1 Histogram analysis

An image-histogram indicates the image pixel distribution by indicating the number of pixels at each color intensity level. In Fig. 1, the histogram of the original image of Lena of size 256 × 256 and the histogram of corresponding cipher Image has been presented which depicts that the histogram of plain image has certain pattern of R, G, and B components. But in the Cipher image all the pixels are uniformly distributed, thus making the cryptanalysis difficult.



(a) (b) (c) (d)

Fig 1: (a) Plain original image, (b) histogram of original image (c) Encrypted Image, (d) Histogram of encrypted image

This test is conducted for all the three algorithms and satisfactory results were obtained.

3.1.2 Correlation coefficient analysis

In most of the plain images, there exists high degree of correlation among adjacent pixels whereas poor correlation between the neighboring pixels of corresponding cipher image is The correlation coefficient of the the R, G and B componentsfor the encryption algorithm using sine and cosine map, logistic map are shown in the Fig. 2. The correlation between various horizontally, vertically and diagonally adjacent pixels of both the plain and cipher image obtained using Encryption Algorithm based on logistic map are shown in Fig.3.

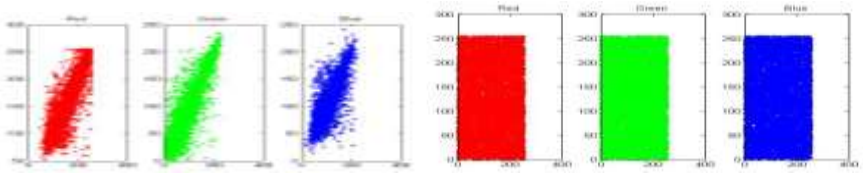


Fig 2: (a) Correlation of adjacent pixels of R, G and B components in plain image, (b) encrypted image

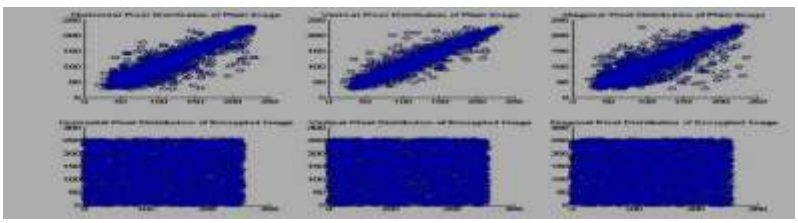


Fig 3: Horizontal, vertical diagonal pixel distribution of plain image and encrypted image.

Table 1.coefficientof horizontal, vertical, diagonal adjacentpixels of original and encrypted images

Image Name	Horizontal Correlation		Vertical Correlation		Diagonal Correlation	
	Plain Image	Cipher Image	Plain Image	Cipher Image	Plain Image	Cipher Image
Lena	0.9453	-0.0012	0.9716	-0.0095	0.9194	0.0078
Jellyfish	0.9669	0.0170	0.9694	0.0150	0.9531	-0.0106

Table1 shows the correlation coefficients between horizontal, vertical, diagonal adjacent pixels of original and encrypted images. Table 2 shows the comparison of correlation coefficient of different encrypted images obtained by encryption algorithms using sine and cosine map (Algorithm1) and logisticmap (Algorithm2).

Table 2.Comparasion of correlation co efficient of Different encrypted images

Image Name	Correlation parameter	Algorithm1	Algorithm2
Lena	Crr	-0.017499	-0.000331
	Crg	-0.015323	0.001827
	Crb	-0.009225	-0.001558
Mandril	Crr	-0.020522	-0.000400
	Crg	-0.008145	-0.004129
	Crb	-0.005235	0.000327
Jelly fish	Crr	-0.029583	0.004773
	Crg	-0.010927	-0.000769
	Crb	0.022440	0.003085

3.2Information Entropy Analysis

Entropy measures the randomness that indicates the texture of an image. The entropy H(s) of a message source s can be calculated as

$$\mathbf{H(s)} = \sum_{i=0}^{2^N-1} p(I_i) log_2 \frac{}{p} \qquad (12)$$

where $p($ represents the probability of message .When an image is encrypted, the ideal value of entropy should be 8. If it is less than this value, there exists a certain degree of predictability which threatens its security. Table 3 compares the entropy values for plain and encrypted images.

Table 3.Comparison of information entropy

Image Name	Plain Image entropy	Entropy with Algorithm1	Entropy with Algorithm2
Lena	7.44	7.991	7.9991
Jelly fish	6.35	7.998	7.9983
Mendrill	7.48	7.997	7.990

3.3Encryption Quality – NPCR, UACI And Time Taken Analysis

NPCR (number of pixel change rate) and UACI (unified average change in intensity) are generally considered to evaluate the strength of the image encryption algorithm with respect to differential attacks. Opponent can create a small change in the input image to observe changes in the result. By this method, the meaningful relationship between original image and encrypted image can be found. To test the effect of one-pixel change on the image encrypted by the proposed algorithm, two common measures were used – Number of Pixel Change Rate (NPCR) , Unified Average Change in Intensity (UACI) . Consider two cipher-images, Ca(i, j) andCc(i , j) where i = 0,1,2, … , M - 1 and j = 0,1,2, … , N - 1,whose corresponding plain-images have only one pixel difference. Then NPCR and UACI are defined as

$$\mathbf{NPCR} = \frac{\sum_{i,j} D(i,j)}{M \times N} \qquad \text{where } \mathbf{D} = \begin{cases} \mathbf{0, if\ Ca(i,j) = Cc(i,} \\ \mathbf{1, if\ Ca(i,j) \neq Cc(i,} \end{cases} \quad (13)$$

$$\mathbf{UACI} = \frac{1}{M \times N} \sum_{i,j} |Ca(i,j) - Cc(i, / \mathbf{255} \quad (14)$$

Table 4.Measurement of encryption quality and time taken

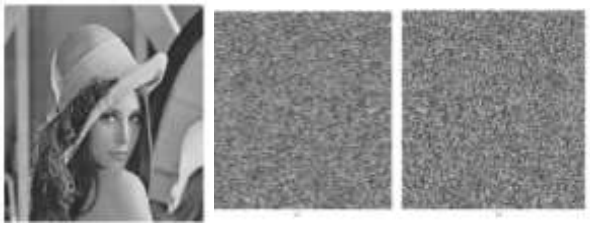
Apart from the security consideration, the speed of the algorithm is also an important parameter for a good encryption algorithm. In this paper the encryption/decryption rate of several images of different sizes by using the proposed image encryption algorithms are tested. The time analysis has been done on Intel i3 CPU with 4GB RAM computer. Table 4 depicts the related results.

Image Lena	NPCR	UACI	Time Taken	Image Mandril	NPCR	UACI	Time Taken
Algo1	99.8889	33.6119	2.4694	Algo1	99.9619	30.3741	5.4219
Algo2	99.8489	32.8281	0.3203	Algo2	99.8474	29.5381	0.3202

3.4Sensitivity Analysis

An ideal image encryption procedure should be sensitive with respect to the secret key i.e. the change of a single bit in the secret key should produce a different encrypted image.

For Algorithm1, the encryption and decryption realizes the 16 – character ASCII code “ABCDEFG012345678” as an input key. The resulting eight intial conditions and eight parameters, i.e a total of 16 keys, are represented by 8 – digit floating – point numbers results in 128 uncertain digits, which is greater than the minimum requirement of the 56 bit data encryption standard (DES) algorithm. For Algorithm2, plain image Lena of size 256 × 256 is considered as an example and is encrypted with x_0 = 0.45001, y_0 = 0.54001, μ1 = μ2 = 1.97. In Fig.4,different cipher images of Lena of size 256 × 256 with minor changes in secret keys have been presented.



(a) (b) (c)

Fig 4: Key sensitivity test (a)Plain Image Lena of size 256 × 256 (b) Cipher image with chosen key (c) Cipher image with change in x_0 =0.45002, y_0 = 0.54002

In this algorithm, a 40 bit long key is used which produces a key space equivalent to 2^{40} which is a very long key. In order to test the sensitivity of the key the image is once encrypted with the proposed algorithm, the same image is encrypted once again by changing the initial value of 'a' from to a value lesser than 4 (say 3.9). The encrypted images obtained are different from one another.

IV. CONCLUSION

The experimental results show that chaotic map based encryption algorithms are robust for image encryption. The encryption algorithm using sine and cosine chaotic map offers greater security as compared to the other two methods but takes more time to encrypt and decrypt. The algorithm using logistic map is faster and applicable to colour images but the algorithm with sine and cosine chaotic maps offers high level security hence is used for private data protection.

REFERENCES

[1] M. Philip, "An Enhanced Chaotic Image Encryption" InternationalJournal of Computer Science, Vol. 1, No. 5, 2011.

[2] G. Chen, Y. Mao, CK Chui, "A symmetric image encryption schemebased on 3D chaotic cat maps", Chaos, Solitons and Fractals, Vol.21,1992.

[3] H.K.L. Chang, J.L. Liu, "A linear quad tree compression scheme for imageencryption", Signal Process.vol 4, 279–290, 1997.

[4] J. Scharinger, "Fast encryption of image data using chaotic Kolmogrovflow", J. Electronic Engvol2, 318–325, 1998.

[5] Fridrich Jiri, "Symmetric ciphers based on two dimensional chaoticmaps", Int. Journal of . Bifurcation andChaos, vol 8, 1259–1284,1998.

[6] J.C. Yen, J.I. Guo, A new chaotic key based design for imageencryption and decryption, Proceedings of the IEEE InternationalSymposium Circuits and Systems, vol. 4,. 49–52, 2000.

[7] J.C. Yen, J.I. Guo, "An efficient hierarchical chaotic image encryptionalgorithm and its VLSI realization", IEE Proc. Vis. Image Processing, 167–175,2000.

[8]Fridrich J. "Symmetric ciphers based on two-dimensional chaotic Maps".International Journal of Bifurcation and Chaos,vol8,1259 – 1284, 1998.

[9] Feng Y, Li L J, Huang F. "A symmetric image encryption approachbased on line maps". In: Proceedings of the 1st InternationalSymposium on Systems and Control in Aerospace and Astronautics, 2001.

[10] Parameshachari B D, K M SunjivSoyjaudah, Sumitrha Devi K A,"Secure Transmission of an Image using Partial Encryption basedAlgorithm", International Journal of Computer Applications, vol. 63, no.16,0975 – 8887, February 2013.

[11] Jiri Fridrich, "Symmetric Ciphers Based on Two-Dimensional ChaoticMaps", International Journal of Bifurcation and Chaos, Vol. 8, No. 6, 1998.

[12] N.K. Pareek, VinodPatidar, K.K. Sud, "Cryptography using multipleone-dimensional chaotic maps", Communications in Nonlinear Scienceand Numerical Simulation,vol10 , 715–723,2005.

[13] Vandana Thakur, MonjulSaikia. "Hiding Secret Image in Video" ,International Conference on Intelligent Systems and Signal Processing(ISSP), 2013.

[14] K. Sakthidasan and B.V. Santhosh Krishna, "A New Chaotic Algorithmfor image encryption and Decryption of Digital Color Images",International Journal of Information and Education Technology, Vol. 1,No. 2, June 2011.

[15] Ramesh kumaryadava, Dr. B. K. singh, S. K. sinha, K. K. pandey, "ANew Approach of colour image encryption based on Henon like Chaoticmap", International Conference on Recent Trends in Applied Scienceswith Engineering Applications, Vol.3, No.6, 2013

[16] N.K. Pareek, VinodPatidar, K.K. Sud, Cryptography using Multiple one-dimensional chaotic maps, Communications in Nonlinear Science andNumerical Simulation, 2005.

[17] Kamlesh Gupta, Sanjay Silakari, "New Approach for Fast color imageencryption using chaotic Map", Journal of Information Security,vol 2,139-150, 2011.

[18] G.Chen, Y.Mao, and C.K. Chui,"ASymmetriEncryptionScheme Basedon 3D Chaotic Cat Map", Chao, Solitons& Fractals, 21,749-761,2004

[19] William Stalling, "Cryptography and Network Security", 3rd edition,Prentice Hall of India, 2003.

[20] Narendra K Pareek, VinodPatidar, Krishan K Sud, "A Random BitGenerator using Chaotic maps", International journal of network security Vol.10,No.1,PP.32,Jan2011