ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

A Triple Key 3-d Chaotic Image EncryptionMethod using Double Chaotic Neural Networks

Neethu Subash[1], Meera Vijayan[2], Dr. Varghese Paul[3]

MTech Student, CSE, AdiShankara Institute of Engineering and Technology, Kalady, India[1]

Asst.Professor, IT, AdiShankara Institute of Engineering and Technology, Kalady, India[2]

Dean, CS IT, Cochin University for Science and Technology, Cochin, India [3]

Abstract: The thesis highly aims on the security of images for secure communication. To achieve this, the need is to confuse any unauthorized who is trying to get the image. Here the image planes are taken into consideration. Three chaotic functions are studied and implemented into the system to create a secure system. The Red, Green and Blue components as on X,Y and Z axis are extracted. The scrambling of these pixels using Arnold cat maps does not create any change in the intensity or color of the image. A Chebyshev map is also induced which again creates a set of manipulations on the generated keys. A Triple key encryption is carried out on each of the plane using a 3-D chaotic neural network using three different keys on individual networks. This creates a more complex system where, if either of the key is wrong, a scrambled image will be the decrypted output. As s result a highly secure system will be in effective. Nine different keys will decide the predictability of the framework. Neural network performs XOR operation and XNOR operations works on two stages that is dependent only on the flow of the operation. Chaotic systems provide unpredictability of execution. The direction of manipulations cannot be predicted as a slight change in the value of the keys will make many deviations in calculations. Analysis of the method results in infinite value of PSNR. Higher quality of encryption nearly 96%. Hence the use of multi-dimensional chaotic functions creates much security due to the unpredictability's and randomness.

Keywords: PSNR ; CI; NPCR; UACI; QoI; CNN

I. INTRODUCTION

The utilization of chaotic systems for protected or private communications has been an active area of research. It is based on the facts that chaotic signals are generally noise-like and chaotic systems are very sensitive to initial condition. In addition the analogue secure communications that are relied on the management of chaotic systems. Baptista proposed a chaotic cryptographic method that encrypts the message as the number of iterations applied in the chaotic map in order to reach the region corresponds to that text. He established his advancement using a simple one dimensional logistic map governed by the following equation:

$X_n+1= bX_n (1-X_n)$.......................eqn(1) [1]

Since the cipher messages are small integers, they are appropriate to be transmitted all the way through today's public digital networks. In order to avoid statistical and differential cryptanalysis, a random number is generated each time the chaotic trajectory has reached the desired region. There are two major drawbacks with Baptista's approach. First, the resultant cipher text is usually intense at the smaller number of iterations. The other drawback is that a sequence of random numbers may have to be generated for a single block of message text. The encryption takes much longer time and the random numbers generated may repeat at an early time. Further, the chaotism is exploited and additional security is attained by introduced 3 keys, triple keys for the encryptions and decryptions. A new methodology adding extra bit of security is, implementing chaotic encryption using triple keys, where three keys are used. First and second keys are calculated from the 80 bit session key entered by the user. Certain summations are implemented to induce these keys. Third key is users input. The encryption is completed using xor-ing the image pixels to the values obtained from the chaotic logistic mappings. It highly depends on the session key, initial key and control parameters knowing this triple key, no one can decrypt the cipher. The encryption results are very sensitive to the parameter fluctuation. Chaotic Equations can be used in 3-Dimensional using the color image properties of the three planes, Red, Green and Blue. These equations provide high degree of sensitivity which is always unpredictable. A double layered chaotic neural network using xor and xnor isapplied.Here triple keys are applied onto each plane differently and individually. This creates a high degree of security to images.

II. BACKGROUND

A triple-key method of image data encryption as in [1], a session key of 80 bit is entered in the form of 20 hexadecimal characters. Portions of this key are extracted and some calculations are done on it to form an intermediate key. Intermediate key is combined with the initial parameter key and the control parameter key which are then used to produce a chaotic sequence. The chaotic sequence is produced using the one-dimensional chaotic logistic map. The technique is called Triple-key because it provides a three-fold shield to the original image and three keys have to be entered in the accurate order for decrypting the image. The basic idea comes from Baptista's Cryptography using chaos as in[2].Baptista proposed that encryption of some character is the number of iterations applied in the eqn (1), to make its trajectory, departing from an initial condition X0, reach an e-interval associated with that characters.3D Chaotic Functions for Image Encryption[3] explains a method where the algorithm uses 3-D logistic equation, 3-D and 2-D Arnold cat map, and 3-D Chebyshev map for color image encryptions. These three chaotic functions provide high security and each of these mapping are used for specifically for different functions. 3-D Arnold cat map provide R, G and B component substitutions. The three keys for the encryptions are obtained from chebyshev mapping function and fed to 3-D logistic A composition of two logistic map can be seen in A Digital Image Encryption Algorithm Based on a Composition of Two Chaotic Logistic Maps[4]. This paper introduces a well-organized chaos-based stream secret message, composing two chaotic logistic maps and a bulky sufficient external secret input for image encryption. The external secret input is used to derive the primary conditions for the chaotic maps, and is working with the two chaotic maps to confuse the relationship between the cipher image and the plain image. In the encryption phase, the image pixels are encrypted using an iterative cipher module based feedback and data-dependent inputs method for mixing the current encryption parameters with previously encrypted information.

A new advancement recommended as in a symmetric image encryption scheme based on 3D chaotic Cat maps [6], for fast and secure image encryption. Since digital images are frequently represented as two-dimensional arrays, in order to fast de-correlate associations among pixels in an image, a superior-dimensional chaotic map is premeditated and then used to shuffle the positions and, if desired, grey values of pixels in the image to puzzle the relationship between secret message-image and plain-image, a transmission process among pixels is performed. It is found that Arnold's cat map is a good quality candidate for permutation, thus it is comprehensive to a three dimensional extension, called 3D cat map, and then used for this principle. Taking enhancement of the outstandingly good properties of incorporating and sensitivity to initial circumstances and parameters of the chaotic 3D cat map, the proposed scheme incorporates Chen's chaotic coordination in key scheming and then yet again uses combination and diffusion to render the image completely unrecognizable.

III. PROPOSED WORK

Proposed method uses multidimensional chaotic functions and a double layered chaotic neural networks. The use of the chaotic functions create a high rate of security and high key space.2-D Arnold Cat map, 3-D chebyshev map and 3-D logistic mapping are used in this method. The XOR and XNOR operation is carried out on a double layer concept as in[9] using neural network.Huge numbers of chaotic methods are being proposed for the image encryption now a days. Chaotic functions are blessed with properties like sensitivity to the primary condition, and ergodicity which make them very attractive for encryption. There are many image encryption algorithms based on low dimension chaotic function. Security provided by these algorithms is limited since these functions provide the limited key space and possesses some weaknesses. Three dimension functions are far more secure from cryptanalytic hits. We propose the improved 3D logistic map that is functional in encrypting the Red, Green, Blue component of the image separately. Two Dimensional Arnold image scrambling, 3D Chebyshev map for key generation, 3D logistic map for image encryption are used here. The encryption method make use of both diffusion and confusion mechanism which make it very secure. Encryption is done onto the red green and blue planes individually by feeding into the neural network.

A. 2-D Arnold Cat Map

A 2-dimensional Arnold Cat Map is used to provide scrambling of pixels of a color image.The use of Arnolds Cat Map provides additional security in the development of image encryption. Arnolds Cat Map does not change the intensity or color composition of the pixels in the image, it only shuffles the image data.

B. 3-D Chebyshev Map

In this method Chebyshev equation is used to generate the keys from triple key generation after a set of 80 random roundups. Chebyshev polynomial $S_n(x)$ of the first kind is a polynomial in x degree of n, defined by the relation,

$S_n(x) = \cos n$ where $x = \cos\theta$.

C. 3-D Chaotic Logistic Equation

The encryption decryption methods implemented are based on Chaotic Logistic Maps. With the properties of sensitivity to primary conditions and control parameters, randomness and ergodicity, chaotic maps have been widely used in data and image encryptions. Compared with conventional cryptosystems, the ones based on chaos are easier to be realized, which makes it more appropriate for great-scale data encryption such as images,audio or video data. Chaotic cryptography hit upon its application mainly when it comes to real time applications. Bulk size data, computational density and real time constraints make encryption complicated. This makes chaotic scrambling of an image more advantageous when compared to Conventional encryption algorithms. The message to be transmitted is a text composed by some alphabet. A typical property of chaotic systems is ergodicity. The one dimensional equation is depending on eqn(1). The same idea is been extended over the three planes of the image, x-axis,y-axis and z-axis. Like b, we use three control parameters a, b, c.The 1-dimensional eqn(1) is extended to 3-dimensional as,

$$X_{i+1} = c\, x_i(1- x_i) + b\, y_i^2\, x_i + a\, z_i^3 \ldots\ldots\ldots\ldots\ldots(1)$$

$$Y_{i+1} = c\, y_i(1- y_i) + b\, z_i^2 y_i + a\, x_i^3 \ldots\ldots\ldots\ldots\ldots..(2)$$

$$Z_{i+1} = c\, z_i\, (1- z_i) + b\, x_i^2 z_i + a\, y_i^3 \ldots\ldots\ldots\ldots\ldots...(3)$$

Chaotic behavior exhibited for $3.53<c<3.81$, $0<b<0.022$, $0<a<0.015$ and can take any value between [0, 1].

D. Double-Layer Neural Network

Neural Network is configured using the chaotic sequences generated from the 3-dimensional logistic equations. The pixel values are placed as, 8 and 8 forming 16 pixels in one row. The method is applied onto each planes differently. First we are taking a plane and its pixels to have N/2 pixels. Chaotic sequence is divided into two sections. These decides the weights and biases to the neural network. First layer of chaotic sequence, that is elements 1 to N performs XOR operation in the neural network. Second layer does XNOR operation, that is elements from N+1 to 2N. Thus the encrypted image will consist of first half with pixels of XOR neural encryption and second half with pixels of XNOR operation.

E. Algorithm

A Triple key 3-d chaotic image encryption method using double chaotic neural networks:

Step 1: Input an image of size N

Step 2: Perform an Arnold 2-D map to every pixel in the image

p = (x' , y') = [1 1; 1 2] x [x ; y]

(x' , y') = mod(p(2), m)+1, mod(p(1),m)+1

Step 3: The session key K consisting of 20 hexadecimal characters 0 to 9 and A to F is entered.

$K=k_1k_2\ k_3....k_{20}$

Step 4: Each hexadecimal character in the session key is converted into its binary equivalent of four bits so that the session key consists of 80 bits.

Let $k_1=k_{11}\ k_{12}\ k_{13}\ k_{14}$

$k_2=k_{21}\ k_{22}\ k_{23}\ k_{24}$............... $k_{20} = k_{201}\ k_{202}\ k_{203}\ k_{204}$

Step 5. A block k of 24 bits $k_7\ k_8\ k_9\ k_{10}\ k_{11}\ k_{12}$ is extracted from the session key .

Step 6. X01 and X02 are computed

$$X01 = (k_{71} * 2^0 + ... +k_{74}*2^3 + k_{81}* 2^4 +....+ k_{84}*2^7 +....+ k_{121}*2^{20} +....+k_{124}*2^{23})/2^{24}$$

$$X02 = (k_{13} + k_{14}+....+k_{18})/16 \times 6$$

Step 7. The initial parameter X(1) is computed when the user enters key X03

$$X(1) = (X01 + X02 + X03) \bmod 1 \ldots\ldots\ldots\ldots\ldots\ldots(4)$$

Step 8.X(2) & X(3) is calculated for each plane.

Step 9: Perform chebyshev mapping on the sequence generated:

Sum= X(1) of x-plane + X(2) of y-plane + X(3) of z-plane

Generate random numbers for x,y z planes

```
fori = 1,……,80 do
for j = 1,…..,number of elements (pr,pg,pb) do
    u=mod(X(1)+pr(j),1)
    v=mod(X(2)+pg(j),1)
    w=mod(X(3)+pb(j),1)
    T2u=2 x (u2)-1
    T3v=4 x (v3)-3 x v
    T4w=8 x (w4)-8 x (w2)+1
```

Step 10:Define control parameters to be

a=0.015,b=0.022,c= 3.5

Step 11: for i=1....2 x number of elements in each plane

$$X_n = c \times X_1 \times (1-X_1)+ b \times (Y_1^2) \times X_1+ a \times (Z_1^3)$$

$$Y_n = c \times Y_1 \times (1-Y_1)+ b \times (Z_1^2) \times Y_1+ a \times (X_1^3)$$

$$Z_n = c \times Z_1 \times (1- Z_1)+ b \times (X_1^2) \times Z_1+ a \times (Y_1^3)$$

Step 12: Generate chaotic sequence for each plane represented by

$$B = \begin{pmatrix} b_{11}\ b_{12}\ \ldots b_{1N} \\ b_{21}\ b_{22} \ldots . b_{2N} \\ .. \qquad\qquad \ldots \\ .. \qquad \ldots \\ b_{N1}\ b_{N2} \ldots . b_{NN} \end{pmatrix}$$

Step 13: Divide the sequence into two equal groups C & D.

$$C = \begin{pmatrix} c_{11}c_{12}c_{13}...c_{12k} \\ c_{21}c_{22}c_{23}\ldots c_{22k} \\ ..\ ..\quad \ldots. \\ c_{81}c_{82}c_{83}\ldots c_{82k} \end{pmatrix}$$

$$D = \begin{pmatrix} d_{11}\ d_{12}\ d_{13}\ldots.d_{12k} \\ d_{21}\ d_{22}\ d_{23}\ldots.d_{22k} \\ ..\ ..\quad ..\ \ ..\quad ... \\ d_{81}\ d_{82}\ d_{83}\ldots.d_{82k} \end{pmatrix}$$

Step 14 :Configuring the neural network, first layer, each row of C is mapped onto a weight matrix Wc_{ij} of size 2k×2k.

$$Wc_{ij} = \begin{cases} 0, i\neq j \\ 1-2cnj, i=j \end{cases}$$

i& j vary from 1 to 2k & n varies from 1 to 8

Step 15 : When i=j,

$$Wc_{ij} = \begin{cases} 1, i= j \& cnj=0 \\ -1,\ i=j \& cnj=1 \end{cases}$$

Step 16:Each row of C is mapped into bias matrix $\odot$ of size

1 x 2k

$$\odot_c = \begin{cases} 1/2,\ cnj=1 \\ -1/2,\ cnj=0 \end{cases}$$

Step 17: Configuring the second layer neural network, each row of D is mapped onto a weight matrix $Wd_{ij}$of size 2k x 2k.

$$Wd_{ij}= \begin{cases} 0\ , i\neq j \\ 2dnj-1, i=j \end{cases}$$

wherei& j vary from 1 to 2k & n varies from 1 to 8

Step 18: Each row of D is mapped into bias matrix $\odot$ of size

1 x 2k

$$\odot_d = \begin{cases} 1/2,\ dnj=1 \\ -1/2,\ dnj=0 \end{cases}$$

Step 19: Encryption process of the first layer can be summarized as

$$f_{nj}= \text{sign}\ (\Sigma\ Wc_{ij} \text{ x } b_{nj} + \odot_c)$$

where i varies between 1 to 2k

$$\text{sign}(x) = \begin{cases} 1,\ x \geq 0 \\ 0,\ x \leq 0 \end{cases}$$

In simple step,

$$f_{nj}= b_{nj}\text{xor}c_{nj}$$

Step 20: Second layer of encryption can be seen as,

$$g_{nj}= \text{comp}\ (\Sigma\ Wd_{ij} \text{ x } f_{nj} + \odot_d\ )$$

wherei varies between 1 to 2k

$$\text{comp}(x) = \begin{cases} \text{comp(floor}(x)),\ x \geq 0 \\ \text{floor(abs}(x)),\ x< 0 \end{cases}$$

Generalized as,

$$g_{nj}= b_{nj}\text{xnor}f_{nj}$$

Step 21: Decryption is the reverse process of encryption. A successful decryption requires correct hexadecimal keys and control keys to be entered. The only difference being, the layers in the neural network are reversed. The XNOR operation is performed first and secondly XOR.

IV. OBSERVATIONS AND RESULTS

The simulation was done in MATLAB, evaluating the performance and the quality of encryption. The histogram is plotted for the three planes, since the three planes undergoes different encryption using different keys and parameters, the quality of encryption is far increased. Simulation diagrams as well as various factors like QoE, NPCR, UACI provide the performance factors of the system.

A. Encrypted Image Analysis

Encryption is carried out with the input of three different hexadecimal values, session key and user input which does encryption onto each of the three different planes. The use of chebyshev mapping and 2-D Arnold cat map provides much confusion and diffusion which makes this method more secure .Decryption will be unsuccessful if either of the keys are wrong or if one plane key is incorrect. This system becomes highly sensitive to a small change of data. As the chaos becomes three dimensional, more effective encryption is carried out.

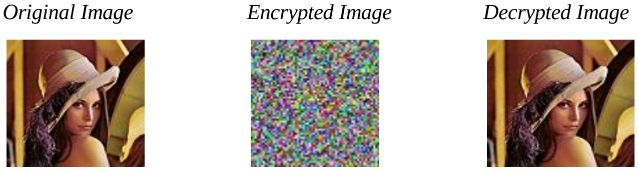
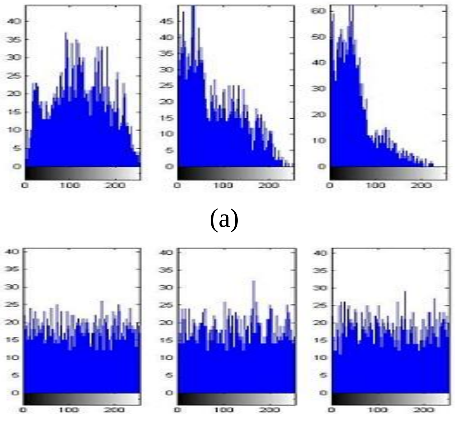


Fig 1: Encrypted Image Analysis

B. Histogram Analysis

Histogram represents the total number of pixels in an image, with the frequency of its occurrence. In this method, each plane is encrypted with its own keys and the histogram distribution shows uniformity of pixels in each plane.



(a)

(b)

Fig 2: 3-plane histogram of lena.png (a) histogram of the original image (b) histogram of the encrypted image

C. Quality of Encryption

Quality of Encryption is the deviation of encrypted image from the decrypted one. It is expressed in terms of correlation indexes. Calculated from the vertical and horizontal correlation indexes.

QoE = (1- CI) x 100

CI is the correlation Index which is defined as the average of correlation between horizontally adjacent pixels and vertically adjacent pixels. It takes values in the range [-1, 1]. Nearer the value of Correlation Index to zero, higher is the scrambling or mixing property of the encrypted image. Correlation can be defined as the similarity that exists between two images.

$CI = (C_h + C_v) / 2$

This method provides a considerably higher quality of encryption, in the range of 95.

Image	Lena.png	Football.jpg
Correlation value of original image	0.96226	0.31649
Correlation value of Encrypted image:	-0.10458	-0.011376
Quality of Encryption	92.73	95.69
NPCR	99.63	99.51
UACI	36.13	24.93

Table 1. Encryption results of png and jpg image type.

D. PSNR

Computes peak signal to noise ratio (Peak Signal to Noise Ratio) between images. Its the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. As many signals have a very wide range, PSNR is usually expressed in terms of the logarithmic decibel scale. It's a measurement that can be used to compute image similarity. PSNR is essentially a measurement of error between the two images. Higher PSNR is better. In this method we are able to retrieve the original image as such, resulting PSNR being infinity. PSNR is most easily defined via the mean squared error (MSE). PSNR defines how good the retrieved image is after decryption.

PSNR=10 log(MAX x MAX/MSE)

E. NPCR & UACI

NPCR & UACI is the number of changing pixel rate and Unified averaged changed intensity. To describe this property, Consider a pixel (i,j) at grid $C_1$and C_2,where original image pixel is C_1(i, j) and pixel after change is C_2(i,j).

$N(C_1,C_2) = \Sigma D(i, j) / T \times 100$

$U(C_1,C_2) =\Sigma (C_1(i, j) - C_2(i, j)) /F. T \times 100$

$$D(i, j) = \begin{cases} 0, C_1(i, j) = C_2(i, j) \\ 1, C_1(i, j) \neq C_2(i, j) \end{cases}$$

The range of NPCR is [0,1]. When its zero, it implies that all pixels in remain the same values as in the original image. When its one, it implies that all pixel values are changed compared to those in the original image.

Keys			QoE
Lena.png	Red	X : 9EB243167FEA k1 : 0.1219	92.73
	Green	Y : 05B2415FE75A k2 : 0.5812	
	Blue	Z : E275BAE799F k3 : 0.2319	
Football.jpg	Red	X : 7F9AC40D2395 k1 : 0.291	95.69
	Green	Y : B9A10FA917EF k2 : 0.197	
	Blue	Z : C4E90AB00DE k3 : 0.102	

Table 2: Quality of Encryption for Lena and Football for different key values

V. CONCLUSION

A Triple Key 3-D chaotic method using Double Chaotic Neural Networks discusses about a encryption decryption method that uses multi dimensional chaotic equations and double layer neural network where the keen work is divided between the three planes, Red green and Blue. Since the encryption is induced with different keys on each plane, there is high security. If any of the nine keys goes wrong the resultant image will be scrambled one. So it takes hard effort for unknown users to break the image. The Quality of Encryption is improved theoretically as well as from the mathematical analysis. As the QoE is obtained is 92 and 95 from the analysis depicted. The Infinite value of PSNR and approximate zero coefficient value shows the effectiveness of the method. Also the readings of NPCR and UACI value from table 1 account this method to be a better scheme for secure encryptions, with saving time. A Better value of NPCR has been obtained with the new method.The proposed work evaluates is a better option for high scale secure communication. The greater chaos does not slow down the system. But it takes more time when it comes to large size data. This increases the computational complexity and overhead. Hence it is required to find a solution. My thesis works for an optimal speed comparing with the standards. Best correlation value of the encrypted image has to be zero.A Better value of NPCR has been obtained with the new method.

REFERENCES

[1] Srividya G, Nandakumar. P, “A Triple –Key Chaotic Image Encryption Method”, In. Cof. On Communications and Signal Processing, 2011, pages 266-270

[2] Cryptography with chaos M.S. BaptistaInstitute for Physical Science and Technology, University of Mm-yland, College Park, MD 20742. USA

[3] 3D Chaotic Functions for Image Encryption Pawan N. Khade and Prof. Manish Narnaware,IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1, May 2012

[4] A Digital Image Encryption Algorithm Based A Composition of Two Chaotic Logistic Maps Ismail Amr Ismail, Mohammed Amin, and HossamDiab,International Journal of Network Security, Vol.11, No.1, PP.1-10, July 2010

[5] N.K. Pareek, VinodPatidar, K.K. Sud, Image encryption using chaotic logistic map, Image and Vision Computing, Volume 24, Issue 9, 1 September 2006, Pages 926-934

[6] A symmetric image encryption scheme based on 3D chaotic cat maps Guanrong Chen, YaobinMao , Charles K. Chui

[7] Arumugam, A.S.; Jothi, D.K., "Image encryption algorithm based on improved 3d chaotic cat map," Computational Intelligence and Computing Research (ICCIC), 2010 IEEE International Conference on , vol., no., pp.1,4, 28-29 Dec. 2010

[8] Data security based on neural networks khaled m. g. noaman and hamid Abdullah jalab faculty of science, computer science department, sana'a university, p.o. Box 13499,Sana'a, Republic of Yemen

[9] Jain, A.; Rajpal, N., "A two layer chaotic network based image encryption technique," Computing and Communication Systems (NCCCS), 2012 National Conference on , vol., no., pp.1,5, 21-22 Nov. 2012

[10] Weiming Zhang; Xinpeng Zhang; Shuozhong Wang, "A Double Layered “Plus-Minus One” Data Embedding Scheme," Signal Processing Letters, IEEE , vol.14, no.11, pp.848,851, Nov. 2007

[11] Yunpeng Zhang; FeiZuo; ZhengjunZhai; CaiXiaobin, "A New Image Encryption Algorithm Based on Multiple Chaos System," Electronic Commerce and Security, 2008 International Symposium on , vol., no., pp.347,350, 3-5 Aug. 2008