ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/307034011

Public key Cryptography Based on Chaotic Neural Network

Conference Paper · August 2014

CITATION
1

READS
360

2 authors, including:

Hany Hamdy
Higher Institute of Management Science and Advanced Computing, El-Beheira, Egypt
8 PUBLICATIONS **21** CITATIONS

SEE PROFILE

Some of the authors of this publication are also working on these related projects:

using neural networks to detect Network intrusions View project

All content following this page was uploaded by Hany Hamdy on 27 August 2016.

The user has requested enhancement of the downloaded file.

Public key Cryptography Based on Chaotic Neural Network

Adel A. El-Zoghabi[#1], Amr H. Yassin[#2], Hany H. Hamdy[#3]

#1 Head, Department of Information technology, Institute of Graduate Studies and Research, Alexandria University.
#2 Lecturer, Electronics & Communication, Engineering Department, Alexandria Higher Institute of Engineering and Technology.
#3 PHD student, Department of Information technology, Institute of Graduate Studies and Research, Alexandria University.

ABSTRACT

In this work, a public key cryptography system based on chaotic neural network (CNN) is used to encrypt and decrypt a digital image. The most traditional public key cryptography is based on number theory which has some drawbacks such as large computational power, complexity, and time consumption. To overcome these drawbacks, a new chaotic neural network is introduced used multidimensional chaotic maps as a chaotic sequence for determined the neural network weight and basis through five layers of networks and additional layer for public key using Chebyshev chaotic map as a chaotic sequence for basis neural network. Simulation results were given to show the achievability and efficiency of the proposed public key model. As a result, CNN becomes more practical in the cryptography transmission field.

Key words: Chaos-based cryptography, Chaos System, Chaotic Maps, Decryption, Encryption, Public key cryptography, Chaotic neural network.

I. INTRODUCTION

The most mounting area in today's world is communication. Everyone wants to secure the information of work that sent over the public network. They use many insecure pathways for transferring and sharing information, but at a certain level it's not secure. Cryptography is method used for sharing information in a concealed way. Cryptography is the detection of 'scrambling' messages so that even if detected, they are very difficult to decode. Cryptography is exchanging the information between the related persons without leakage of information by unauthorized one, trough encrypted the data at transmitter and decrypted at receiver. The encryption is obtained by scrambling the phase spectrum of original one, reverse process is used for decryption [1] [2].

Cryptography has two main techniques for encrypting data [3]:

- Symmetric encryptions, or algorithms, which use one key for encryption as they do for decryption process. Other names for this type of encryption are secret-key, shared-key, and private-key.
- Asymmetric cryptography, which uses different encryption keys for encryption and decryption. In this case an end user on a network, public or private, has a pair of keys; one for encryption and one for decryption. These keys are labeled or known as a public and a private key.

Generalized encryption schemes are symmetric encryption and asymmetric encryption but there are some other cryptographic techniques are also the part of literature like chaotic image encryption, quantum cryptography, bio-cryptosystems, visual cryptography, and elliptic cryptography which lie under symmetric or asymmetric schemes [4].

The rapid growth of computer networks allowed large files, such as digital images, to be easily transmitted over the internet. Data encryption is widely used to ensure security however, most of the available encryption algorithms are used for text data. Due to large data size and real time constrains, algorithms that are good for textual data may not be suitable for multimedia data. Attributable to several substantial features of images, such as bulk data capacity and high correlation among pixels, traditional encryption algorithms are not appropriate for functional image encryption [5]. Neural network can be used to design a real time data protection schemes for its complicated and time-varying structures. Due to the attractive properties of combination neural and the sensitively to initial value conditions and parameters of chaotic maps, a chaos-based neural network created a combination model called a chaotic neural network (CNN) which given a novel and efficient way for data encryption [6].

This work presents a public key algorithm coupled with a chaotic neural network model to encrypt with key, and then decrypt with another key. This algorithm supports speed, efficiency, and robustness that are not existed in many traditional encryptions. The rest of the paper network is organized as follows, in section 2 discusses background and related work in the field of ANN based cryptography. In section 3, the model diagram is proposed. In section 4, the Multidimensional chaotic function is produced. In section 5, the proposed public key algorithm is described in detail. In section 6, the performance and security analyses are described in depth. Finally section 7, concludes the whole work.

II. BACKGROUND AND RELATED WORK

A number of research works have sought a link between chaotic neural networks (CNN) and increased security in cryptosystems. Wenwu Yu proposed an encryption techniques based on the chaotic Hopfield neural networks with time varying delay. The chaotic neural network is used for generating binary sequences for masking the plaintext based on randomly chaotic logistic map. Simulation results show that the proposed model is more functional in the secure transmission of large multi-media files [7] [8].

Rajender S. presented a triple key chaotic neural network for cryptography. The triple key chaotic neural networks are contained of 20 hexadecimal characters, initial value, and control parameters. Experimental results show that the model is highly secure, with a little concern about time consumption [8] [9].

Shweta B. presented a triple key chaotic neural network for image cryptography. The triple key contains a hexadecimal key which combined with initial and control parameters to generate

chaotic sequence. Experimental results shows that algorithm successfully perform the cryptography and can be applied on different colour image size [8] [10].

Tarip A. proposed adapted system model containing MPEG-2 for compression and a chaotic neural network for cryptography. The logistics map is used with neural network to produce a combination of CNN. It has been shown from analysis results that the proposed algorithm has high security with low cost, and also supports quality and bit rate control [8] [11].

Navita A. proposed two artificial neural networks for cryptography, The First network is neural network based n-state sequential machine and other one is chaotic neural network. The weights and biases of the neural network act as a key for encryption and decryption process. Experimental results show that the two networks are secure, without any results about efficiency [8] [12].

Geethavani proposed a new combined model for cryptography and steganography. The model used the Hopfield Chaotic Neural Network (HCNN) for the encryption process, and the Double Density Discrete Wavelet Transform (DD DWT) to embed the cipher-text into the audio cover. Experimental results show that the model is efficiency and secure against the most knows attacks [8] [13].

Neethv Subash proposed a triple key 3-D chaotic neural network model using 4 types of chaotic maps, which are Arnold cat map for scrambling pixels of image, Chebyshev map for generate keys, Double layer neural network for encryption and decryption based on Logistic map. Experimental results show that the quality of encryption is improved [14].

III. THE PUBLIC KEY MODEL DIAGRAM

The pubic key model is described in Fig 1. The chaotic sequence is generated and the image is converted into binary pixels, the image signal is firstly magic by the henon map chaotic sequence through dividing the image pixels into 16 blocks and rearranges the pixels position as existed security step before encryption. The image is being ready for applying the chaotic neural network algorithm for encryption process, and then the cipher image is being sent through the open communication channel. The receiver side follows the same procedures with a little change for extract and encrypts the image.

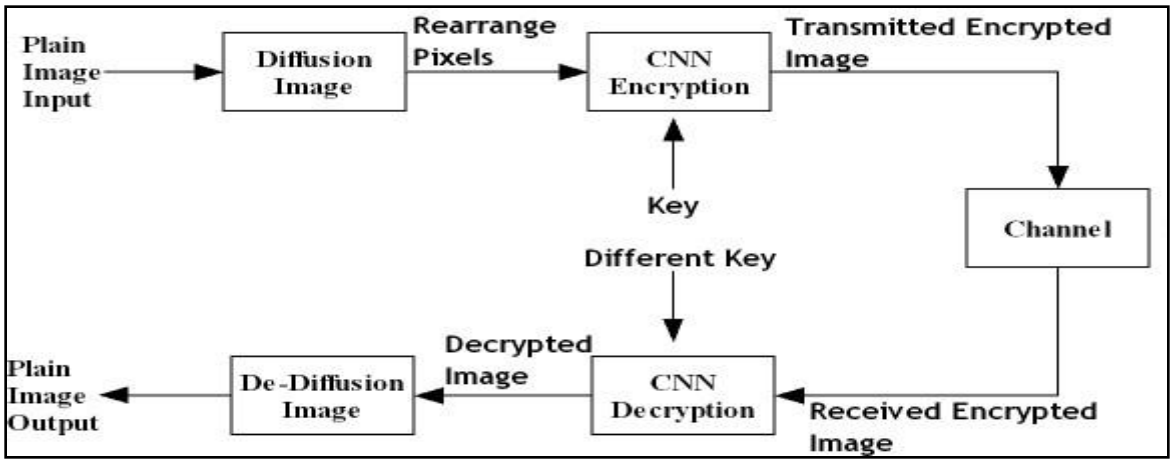

Fig 1: The General Architecture of the proposed public key model

IV. MULTIDIMENSIONAL CHAOTIC FUNCTIONS

The chaotic system is rich in importance for it characterizes such as sensitivity to change initial conditions and parameters, ergodicity, random behaviour, and unstable periodic orbits with long periods. The properties of diffusion, dispersion, disorder, and confusion are required in classical cryptography algorithms through iterative processing.

1D Henon Map: The proposed model used the Henon chaotic map for the diffusion process by magic the pixels of a colour image. The use of Henon chaotic map provides additional security in the development of image public key model. Henon chaotic map does not change the intensity or colour composition of the pixels in the image, it only rearranges the image data pixels, which defined in Equation 1 [15] [16]:

$$X_{n+1} = 1 - aX_n^2 \qquad (1)$$
$$Y_{n+1} = bX_n$$

Where a, and b, are the control parameters of the system, the system will show the chaotic behaviour when a=0.3 and b=1.4.

The proposed model used the selected modified chaotic maps with neural network to produce a combination of CNN, based on a binary sequence generated from the chaotic maps, which the biases and weights of neurons are set in each iteration for encryption and decryption process for selected image through five layer of neural network to gain more security. Cryptography scheme was done by a chaotic neural network, the network is called chaotic neural network if its weights and biases are determined by chaotic sequence. Specially encryption of digital signal we used chaotic neural network.

2D Cross Chaotic Map: The proposed model used the modified cross chaotic map with neural network to produce a combination of CNN, based on a binary sequence generated from the cross chaotic map. The modified cross chaotic map is defined in Equation 2 [16] [17]:

$$X_{n+1} = 1 - \mu Y_n^2 ; \quad X, Y \in [-1,1] \text{ Mod P} \qquad (2)$$
$$Y_{n+1} = \text{Cos}(K \, \text{Cos}^{-1} Y_n) \text{Mod P}$$

Where μ, and K, are the control parameters of the system, where p is a prime number parameter changing the top of the map. The system will show the chaotic behaviour when μ=2 and k=6.

2D Logistic Chaotic Map: The proposed model used the modified logistic chaotic map with neural network to produce a combination of CNN, based on a binary sequence generated from the logistic chaotic map. The modified logistic chaotic map is defined in Equation 3 [18] [19]:

$$X_{i+1} = \mu_1 X_i (1 - X_i) + \beta_1 Y_i^2 \text{ Mod P} \qquad (3)$$
$$Y_{i+1} = \mu_2 Y_i (1 - Y_i) + \beta_2 Y_i^2 + X_i Y_i \text{Mod P}$$

The above formulas increase the quadratic coupling of the items Yi2 , Xi, Yi provide more security to the system. Where the parameters of the system $2.75 < \mu 1 < 3.4$, $2.7 < \mu 2 < 3.45$, $0.15 < \beta 1 < 0.22$, and $0.13 < \beta 2 < 0.15$, the system comes into chaotic state and can generate a chaotic sequence in the region (0, 1).

1D Ikeda Chaotic Map: The proposed model used the modified ikeda chaotic map with neural network to produce a combination of CNN, based on a binary sequence generated from the ikeda chaotic map. The modified logistic chaotic map is defined in Equation 4[20]:

$$X_{s+1} = a + bx_s \cos(s) - Y_s \sin(s) \text{Mod } P \quad (4)$$

Where a, and b, are the control parameters of the system, where p is a prime number parameter changing the top of the map. The system will show the chaotic behaviour when a=1.0 and b=0.9.

1D Chebyshev Chaotic Map: The proposed model used the Chebyshev chaotic maps with neural network to produce a combination of CNN, based on a binary sequence generated from the Chebyshev chaotic maps, which the biases of neurons are set in every iteration for generation the public key. The Chebyshev map possesses the semi group property which lead to TsTr= TrTs. Here the Chebyshev polynomial map Tn: R→R of degree p is defined using the following recurrent relation: The Chebyshev map is defined in Equation 5 [21]:

$$T_n(x) = \cos(n.\cos^{-1}(x))$$
$$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x) \quad (5)$$

Where, n > 2, T0(x) = 1, T1(x) = x.

V. THE PROPOSED PUBLIC KEY ALGORITHM

The public key algorithm model is composed of the following five parts, which are Key generation, Diffusion process, encryption process, and decryption process, De-diffusion process.

A. **Key Generation:** Alice (receiver), in order to generate the keys, does the following:

Step 1: Generates a large integer S.

Step 2: Selects a random number $X \in [-1,1]$ and computes Ts(X).

Step 3: Alice sets her public key to (X,Ts(X)) and her private key to S.

B. **Diffusion Process:** Bob, in order to diffuse the image, does the following:

Step 1: Read the image.

Step 2: Determine the size and the length of image.

Step 3: Determine control parameters a, and b.

Step 4: Generate the chaotic sequences X(1), X(2), X(3), ….. X(m) using the Henon chaotic map as follow in equation 1.

Step5: Perform the Henon chaotic map as row key for rearrange the image pixels based on 16 blocks through change the image pixel place from direction to another direction as a step for diffusion process before encryption process.

C. **Encryption Process:** Bob, in order to encrypt the image, does the following:

Step1: Convert the magic image matrix into binary matrix as a perpetration process for the chaotic neural network public key encryption process.

Step 2: Determine the control parameters μand k.

Step 3: Generate the chaotic sequences X(1), X(2), X(3), ….. X(m) and Y(1), Y(2), Y(3), ….. Y(m) using the 2D modified cross chaotic map as follow in equation 2.

Step 4: Create a chaotic bit sequences bx(0), bx(1), bx(2) from the chaotic sequences X(1), X(2), X(3), ….. X(m) and by(0), by(1), by(2) from the chaotic sequences Y(1), Y(2), Y(3), ….. Y(m) through the generation scheme b(m), b(m), …… b(m-1), which is the binary representation of x(m) and y(m), for m=1,2,….M.

Step 5: Calculated the weight for bx, and by as follows:

For i=0 to M, and J=0 to M

$$W_{ji} = \begin{Bmatrix} 1\ if\ j = i\ and\ b(m,i) = 0 \\ -1\ if\ \ b(m,i) = 1 \\ 0\ if\ j \neq i \end{Bmatrix}$$

Step 6: Calculated the biases for b_x, and b_y as follows:

For i=0 to M

$$\theta_i = \begin{Bmatrix} -\frac{1}{2}\ if\ b(m,i) = 0 \\ \frac{1}{2}\ if\ b(m,i) = 1 \end{Bmatrix}$$

End

Step 7: Calculated the layer one and layer two of the cipher image as follows:

$$d_1^{'}(n) = Sign(\sum_{j=i}^{m} W_{ji}\, d_i) + \theta_i$$

$$d_2^{'}(n) = hardlim(\sum_{j=i}^{m} W_{ji}\, d_1^{'}) + \theta_i$$

Step 8: Do the same steps from step 2 to step 6 based on the 1D modified ikeda chaotic map as follow in equation 4.

Step 9: Calculated the layer three of the cipher image as follows:

$$d_3^{'}(n) = Sign(\sum_{j=i}^{m} W_{ji}\, d_2{'}) + \theta_i$$

Step 10: Do the same steps from step 2 to step 6 based on the 2D modified logistic chaotic map as follow in equation 3.

Step 11: Calculated the layer four and layer five of the cipher image as follows:

$$d_4^{'}(n) = hardlim(\sum_{j=i}^{m} W_{ji}\, d'_3) + \theta_i$$

$$d_5^{'}(n) = Sign(\sum_{j=i}^{m} W_{ji}\, d_4^{'}) + \theta_i$$

Step 12: Bob (Sender), Obtain Alice's authentic public key (x,Ts(x)).
Step 13: Generates a large integer r.
Step 14: Computes Tr(x),Tr·s(x) = Tr(Ts(x))
Step 15: Reshape the keyTr(Ts(x)).
Step 16: Create a chaotic bit sequences $bT_{rs}(0)$, bT_{rs} (1), bT_{rs} (2) from the chaotic sequences Tr(1), Tr(2), Tr(3), ….. Tr(m) through the generation scheme b(m), b(m), …… b(m-1), which is the binary representation of Tr(m) for m=1,2,….M.

Step 17: Calculated the biases for bT_{rs}as follows:

For i=0 to M

$$\theta Tr_i = \begin{Bmatrix} -\frac{1}{2}\ if\ b(m,i) = 0 \\ \frac{1}{2}\ if\ b(m,i) = 1 \end{Bmatrix}$$

End

Step 18: Computes the cipher image as follows:

$C\_img = d_5^{'} + \theta Tr_i$

Step 19: Sends the cipher image C = (Tr(x),C_img) to Alice.

D. **Decryption Process:** Alice, to recover the image M from the cipher image C, does the following:

Step 1: Uses her private key S to compute Ts·r = Ts(Tr(x)).

Step 2: Reshape the keyTs(Tr(x)).

Step 3: Create a chaotic bit sequences $bT_{sr}(0)$, bT_{sr} (1), bT_{sr} (2) from the chaotic sequences Ts(1), Ts(2), Ts(3), ….. Ts(m) through the generation scheme b(m), b(m), …… b(m-1), which is the binary representation of Ts(m) for m=1,2,….M.

Step 4: Calculated the biases for bT_{sr} as follows:

For i=0 to M

$$\theta Ts_i = \begin{Bmatrix} -\frac{1}{2}\ if\ b(m,i) = 0 \\ \frac{1}{2}\ if\ b(m,i) = 1 \end{Bmatrix}$$

End

Step 5: Recovers M by computing the follows:

$M = \text{C\_img} - \theta Ts_i$

E. **De-Diffusion Process:** Alice, in order to recover the original image, does the following:

Step 1: Do the same steps of the diffusion process from step 1 to step 5

Step 2: Determine the key for the de-diffusion operation by subtracting the modified chaotic sequences form the size of the image.

Step 3: Perform the determined key as row key for reorganize the image pixels based on 16 blocks through change the image pixel place from direction to original direction.

VI. EXPERIMENT AND TEST RESULTS

In this work two standard cases of the grey image of Lena has been used, 128 *128, and 512 * 512 size as the original image, used the Matlab environment to simulate experiment, the initial value of X, and Y are Set as X= 0.883896, Y=0.883896.

We demonstrate the performance of the public key model in encryption and decryption techniques and compare it with AES, RSA, and RC5 models using some statistical and other measures:

A. Processing time

Chaos based encryption enables secure and fast mode of communication. We tested the above algorithm on a system running on Core i7-2.8 GHz processor with 4 GB RAM. The encryption and decryption time of the proposal model are listed in Table 1 and Fig 2.

Table 1: Comparison of The encryption & Decryption time for various Encryption Algorithms

Image Size	Public key model		AES		RSA		RC5	
	Enc. Time (in Sec)	Dec. Time (in Sec)	Enc. Time (in Sec)	Dec. Time (in Sec)	Enc. Time (in Sec)	Dec. Time (in Sec)	Enc. Time (in Sec)	Dec. Time (in Sec)
128 *128	5.7968	6.3351	65.0652	502.6936	429.0887	803.9719	62.0393	56.5870
256 *256	35.5076	6.1970	130.1304	1041.3873	1698.5132	3162.5472	246.8768	226.5874

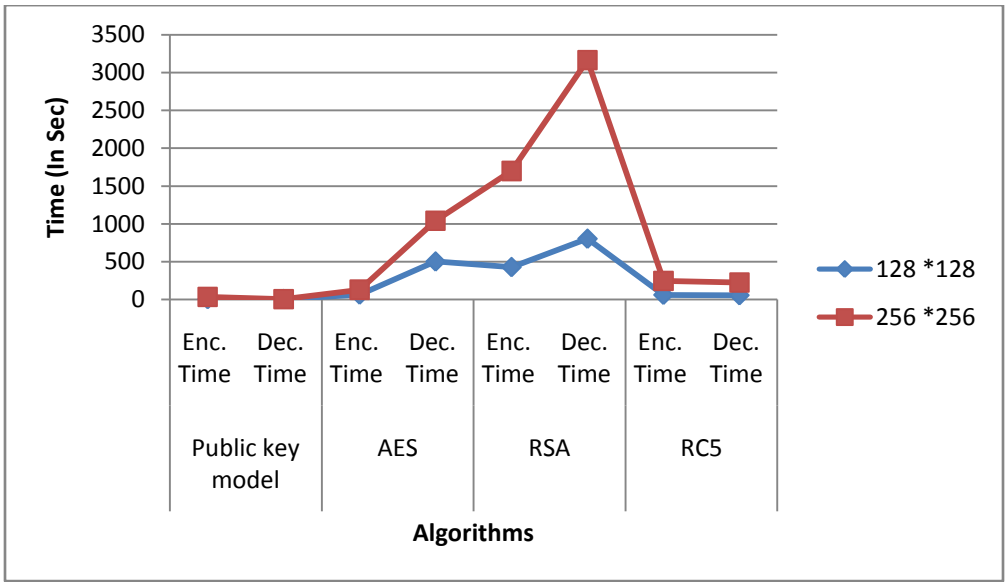

Fig 2: Comparison of The encryption & Decryption time for various Encryption Algorithms

As shown for previous table, the most perfect time for encryption and decryption is our public key model, while the RSA is the long time processing, which illustration that the public key model is less complexity than the RSA algorithm.

B. Histogram analysis

To avoid the infiltration of information, it is necessary for the encrypted image to bear a little or no statistical similarity to the plain image. An image histogram describes how the image-pixels are distributed by plotting the number of pixels at each intensity level. Histograms of the random sequence generated from chaotic neural network are uniformly distributed and significantly different from that of the original images and therefore bear no statistical resemblance to the plain-images. Fig 3 show the original and encrypted histogram image which does not provide any clue to employ any statistical attack of the encrypted images [22].The histogram is fairly uniform and does not reveal any statistical information of the plain-image.

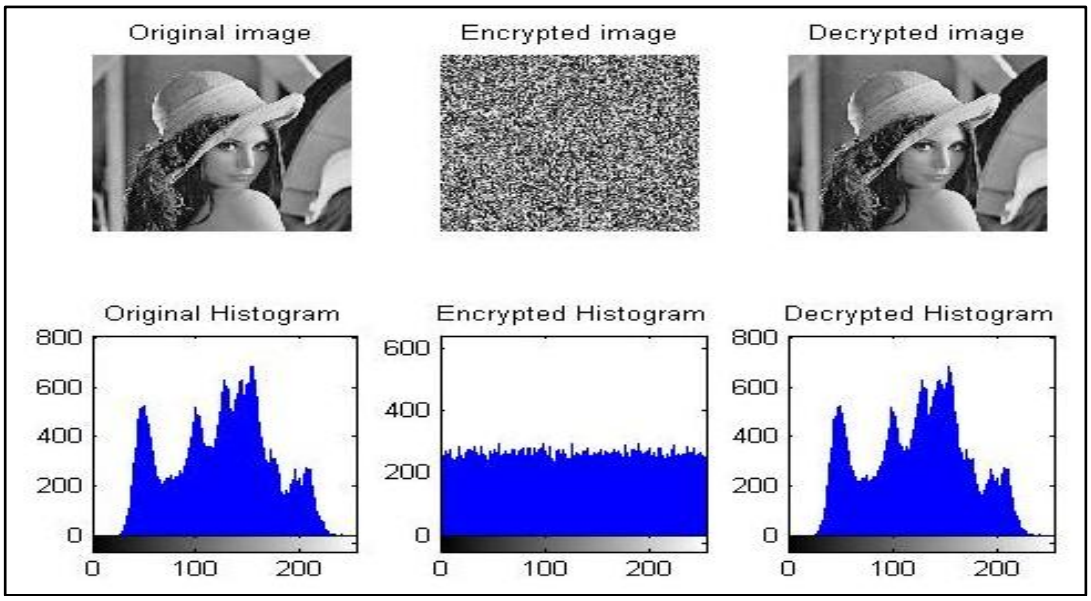

Fig 3: The histogram of the proposal model

C. Information Entropy Analysis

Is a scalar value representing the entropy of a grayscale image. It is a statistical measure of randomness that can be used to characterize the texture of the input image. Entropy is defined as per Equation 6 [23]:

$$\mathbf{E} = \sum_{\mathbf{i=0}}^{\mathbf{n}} \mathbf{P(X_i)\ log_2\ P(X_i)} \quad (6)$$

Where, p_i is the probability that the difference between two neighbor pixels equals i. The ideal value of entropy of the image should be 8. If it is less than this value, there will be some certain predictability that threatens the security**.** The calculated entropies for the original and cipher image are presented in Table 2 and Fig 4.

Table 2: Comparison of Entropy of the cipher image for various Encryption Algorithms

Image Case	**Public key model**	**AES**	**RSA**	**RC5**
128*128	7.9994	7.9992	7.9511	7.9548
256*256	7.9998	7.9972	7.9498	7.9471

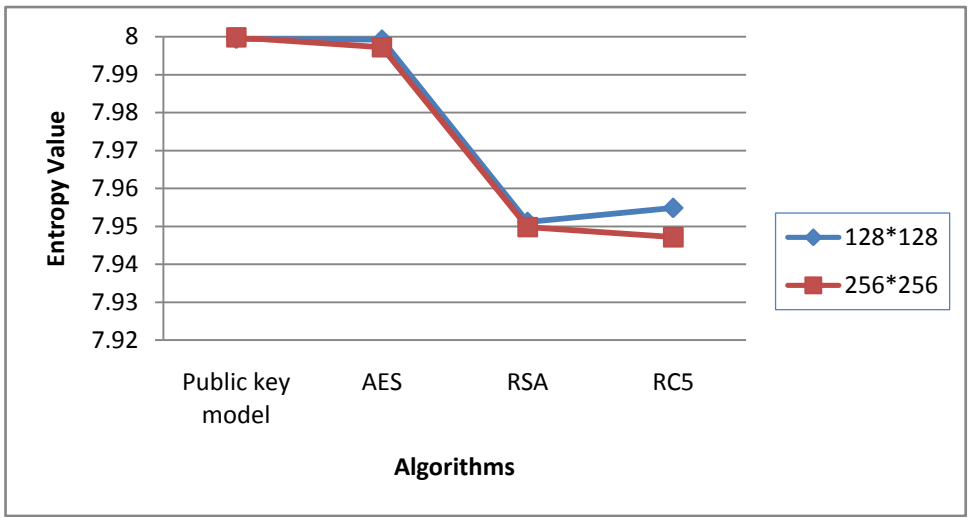

Fig 4: Comparison of Entropy of the cipher image for various Encryption Algorithms

As shown in Table 2 and Fig 4 for Our public key model, AES, and RSA the value of entropy is very close to the theoretical value of 8 bits, which implies that information leakage is negligible and secure against entropy attack. But RC5 has less entropy value as compare to other algorithms.

D. Correlation Analysis

Correlation is a measure that computes degree of similarity between two variables. Correlation coefficient is a useful measure to judge encryption quality of any cryptosystem. Any image cryptosystem is said to be good, if encryption algorithm hides all attributes of a plaintext image, and encrypted image is totally random and highly uncorrelated. If encrypted image and plaintext image are completely different then their corresponding correlation coefficient must be very low, or very close to zero. If correlation coefficient is equal to one, then two images are identical and they are in perfect correlation. In case of perfect correlation (correlation coefficient is equal to 1), encryption process completely fails because the encrypted image is same as the plaintext image. When correlation coefficient is -1 then encrypted image is negative of original (plaintext) image [24].The calculated correlation for the original and cipher image are presented in Table 3 and Fig 5.

Table 3: Comparison of Correlation between the original image and cipher image for various Encryption Algorithms

Image Size	Public key model	AES	RSA	RC5
128*128	-0.0056	0.0011	0.0022	0.0177
256*256	-0.0029	0.0019	0.0089	0.0275

Issue 4, Volume 4 (July-August 2014)
ISSN: 2250-1797

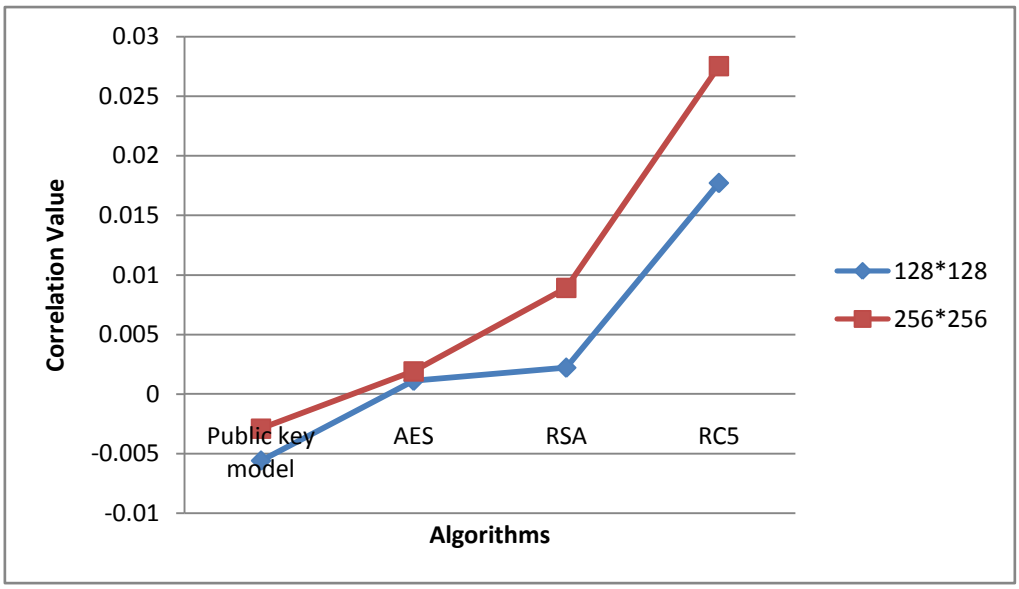

Fig 5: Comparison of Correlation between the original image and cipher image for various Encryption Algorithms

As shown in Table 3, and Fig 7 for the public key model, the value of correlation is very low, which implies that no match between the original image and encrypted images. While RC5 has medium correlation value as compare to other algorithms.

E. Distribution of two adjacent pixels

Correlation is a statistical technique that can show whether and how strongly pairs of variables are related, through comparing between two images before and after encryption. Given an image f(x, y), the correlation problem is to find all places in the image that match a given encrypted image f(x, y). The larger correlation value implies the best match between the two images. This means that if the correlation co-efficient of the initial image and the decrypted image is large, there is maximum similarity between two images [25]. The correlation co-efficient between the plain image and the transformed image is calculated by defined Equation 7[24] [26]:

$$E(X) = \frac{1}{N}\sum_{i=1}^{N} X_i$$
$$D(X) = \frac{1}{N}\sum_{i=1}^{N}\big(X_i - E(X)\big)\big(Y_i - E(Y)\big)$$
$$Cov(X,Y) = \frac{1}{N}\sum_{i=1}^{N}\big(X_i - E(X)\big)(Y_i - E(Y)) \quad (7)$$
$$R_{X,Y} = \frac{Cov(X,Y)}{\sqrt{D(X)}X\sqrt{D(Y)}}$$

Where x and yare grey value of two adjacent pixels in the image, cov(x, y) is covariance, D(x) is variance, E(x) is mean. For calculating the correlation co-efficient, 2,500 random points have been chosen from the original image, and encrypted image and the calculated correlation

co-efficient values in vertical, horizontal and diagonal pixel directions are as shown in the Table 4 and Fig 6.

Table 4: Comparison of The correlation co-efficient value of the adjacent pixels for various Encryption Algorithms

Direction of adjacent pixels		Original Image	Encrypted image			
			Public Key Model	AES	RSA	RC5
Vertical	128*128	0.9546	-0.0371	-0.0075	0.0306	-0.0011
	256*256	0.9602	-0.0158	-0.0101	0.0706	-0.0021
Horizontal	128*128	0.8924	-0.0320	-0.0024	0.0075	-0.0020
	256*256	0.9155	0.0042	-0.0046	0.0016	-0.0019
Diagonal	128*128	0.8397	0.0223	-0.0012	-0.0093	-0.0017
	256*256	0.9117	-0.0368	-0.0015	-0.0331	-0.0027

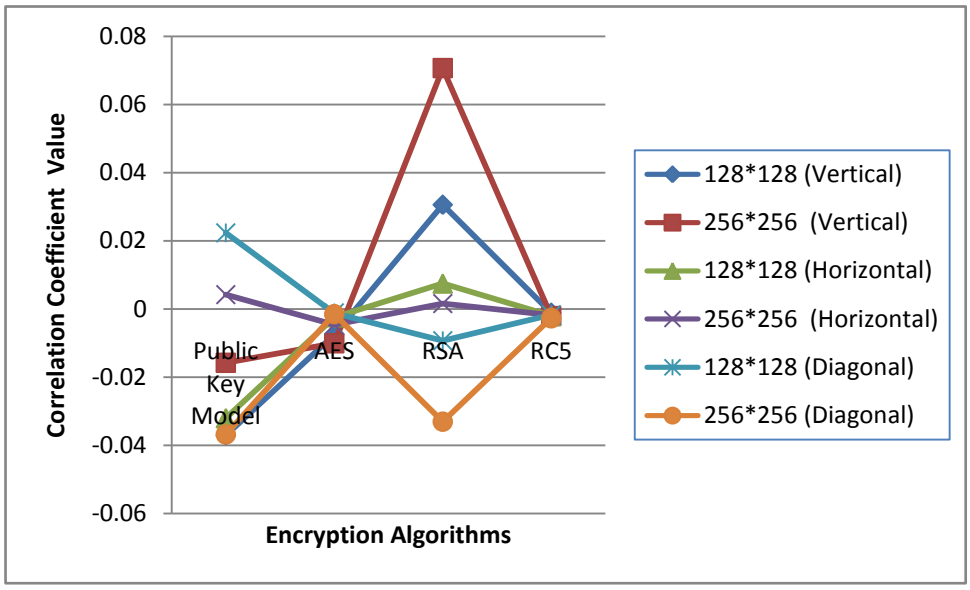

Fig 6: Comparison of The correlation co-efficient value of the adjacent pixels for various Encryption Algorithms

It is easy to see from the existed Table 4, and Fig 6 that the result of our algorithm is much closer to 0. This indicates that our algorithm has effectively removed the correlation of adjacent pixels in the plain-image, thus it is better for image confusion and diffusion.

Test results for correlation of two co-efficient horizontally, vertically, and diagonally adjacent pixels are shown in Fig. 7:

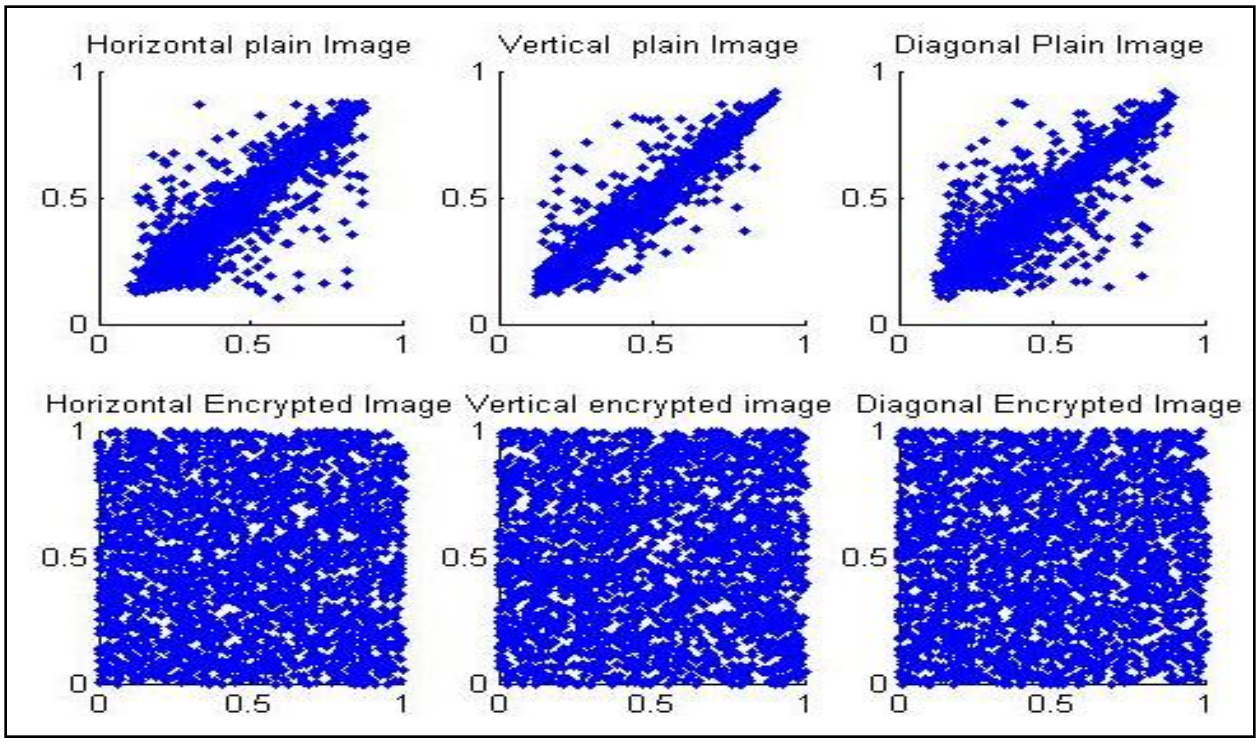

Fig 7: Correlation of the adjacent pixels

Results imply that it is very difficult to deduce secret key from cipher-image when it is attacked by know-plaintext attacks or chosen-plaintext attacks.

F. Peak Signal to Noise Ratio (PSNR)

Peak signal-to noise ratio can be used to evaluate an encryption scheme. PSNR reflects the encryption quality. It is a measurement which indicates the changes in pixel values between the plaintext image and the cipher text image, as shown in Equation 8 [27]:

$$PSNR = 10x\ Log_{10}\left[\frac{M\ x\ N\ x\ 255^2}{\sum_{i=0}^{M-1}\sum_{J=0}^{N-1}(P(i,j)-C(i,j))^2}\right] \quad (8)$$

Where M is the width and N is the height of digital image. P(i; j) is pixel value of the plaintext image at grid (i; j) and C(i; j) is pixel value of the cipher text image. The lower value of PSNR represents better encryption quality.

The PSNR value for proposal model and various encryption algorithms are presented in Table 5.

Table 5: Comparison of PSNR values for various Encryption Algorithms

Image Size	Public key model	AES	RSA	RC5
128*128	36.8810	59.3728	56.8258	43.4967
256*256	36.5118	59.5828	57.6638	43.5642

As shown in Table 5, the lower value of PSNR, which imply the best encryption algorithm is the value of our public key model comparing to other close algorithms RC5. While RSA has medium PSNR value as compare to AES algorithm.

G. Quality of Encryption

Quality of Encryption is the deviation of encrypted image from the decrypted one. It is expressed in terms of correlation indexes. The calculated of the quality is based on the average between the vertical and the horizontal correlation indexes, as shown in Equation 9[14]:

$$QoE = (1 - CI) * 100 \quad (9)$$

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.

The quality of encryption of the proposal model and various encryption algorithms are presented in Table 6.

Table 6: Comparison of quality of encryption for various Encryption Algorithms

Image Size	Public key model	AES	RSA	RC5
128*128	103.46	100.50	98.10	100.16
256*256	100.58	100.74	96.39	100.20

This method provides a considerably higher quality of encryption, in the range of 100, as shown for the AES encryption algorithm.

H. Differential attack

Attacker often make a slight change for the original image, and use the proposed scheme to encrypt for the original image before and after changing, through comparing the two encrypted images to find out the relationship between the original image and the encrypted image. It is called differential attack. To evaluate the influence of one-pixel change on the whole encrypted image, three common measures are used:

- **Avalanche Effect:**

A small change in key or plaintext image should cause significant change in the corresponding cipher text image. This property of cryptosystem is known as avalanche effect. Avalanche effect is desirable property for all cryptographic algorithms. Strict avalanche effect occurs when a single bit change in the plaintext image change 50% of the bits in the cipher text image. Mean Square Error (MSE) is the cumulative squared error between two digital images and can be used to check the avalanche effect. Let C1 and C2 be two cipher text images whose corresponding keys are differ by one bit, and then MSE can be calculated as shown in Equation 10 [28]:

(10)

$$MSE = \frac{1}{M\ x\ N}\sum_{i=0}^{N-1}\sum_{j=0}^{M-1}[C_1(i,j) - C_2(i,j)]^2$$

Where M, N is the width and height of digital images and C1(i; j) is gray scale value of pixel at grid (i; j) in cipher image C1 and C2(i; j) is gray scale value of pixel at grid (i; j) in cipher image C2. In the author discussed MSE and generally speaking, if the value obtained using Eq. 16 for MSE is ≥ 30 dB, quality difference between two images is evident [29].

The MSE value for proposal model and various encryption algorithms are presented in Table 6.

Table 6: Comparison of MSE values for various Encryption Algorithms

Image Size	Public key model	AES	RSA	RC5
128*128	45.39 dB	40.42 dB	40.37 dB	33.86 dB
256*256	44.89 dB	40.44 dB	40.39 dB	33.31 dB

Simulation results are shown in Table 6 for various Encryption Algorithms, the MSE is > 30 dB, and the cipher image is significantly different when plain image differs by one pixel. For the public key model, the quality differences are more than encryption algorithms.

- **Number of pixels change rate (NPCR)**

It is a common measure used to check the effect of one pixel change on the entire image. This will indicate the percentage of different pixels between two images, which defined as per Equation 11[30]:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{WXH} X100\% \quad (11)$$

- **Unified average changing intensity (UACI)**

A small change in plaintext image must cause some significant change in cipher-text image. UACI is helpful to identify the average intensity of difference in pixels between the two images which defined as per Equation 12[31]:

$$UACI = \frac{1}{W\ X\ H}\left[\sum_{i,j}\frac{E_1(i,j) - E_2(i,j)}{255}\right] X100\% \quad (12)$$

Where E1 and E2 denote the two encrypted images, respectively, W and H are the width and height of image, and the grayscale values of the pixels at grid (i,j) of E1 and E2 .

This measures the average intensity differences between two images. In the proposed model, NPCR and UACI are calculated after encrypting the plain images through multiply the pixels by 1.4. The results of NPCR & UACI are obtained by simulation for the proposal model in Table 7 and Fig. 8. The results show that the model has strong ability of resisting differential attack.

Higher NPCR values are desired for ideal encryption schemes. The UACI values must be in the range of 33% [30].

Table 7: Comparison of NPCR & UACI analysis values for various Encryption Algorithms

Image Size		Public key model	AES	RSA	RC5
NPCR	128*128	0.9960	0.9966	0.9969	0.8760
	256*256	0.9961	0.9961	0.9939	0.7839
UACI	128*128	0.3346	0.3373	0.3362	0.3246
	256*256	0.3346	0.3351	0.3369	0.3169

The NPCR for the proposed algorithm is very high, so one bit is changed then the encrypted image is totally different and also the average intensity differences between two images (UACI) (plain image and encrypted image) are also very high. Chosen plaintext attack is therefore impossible.

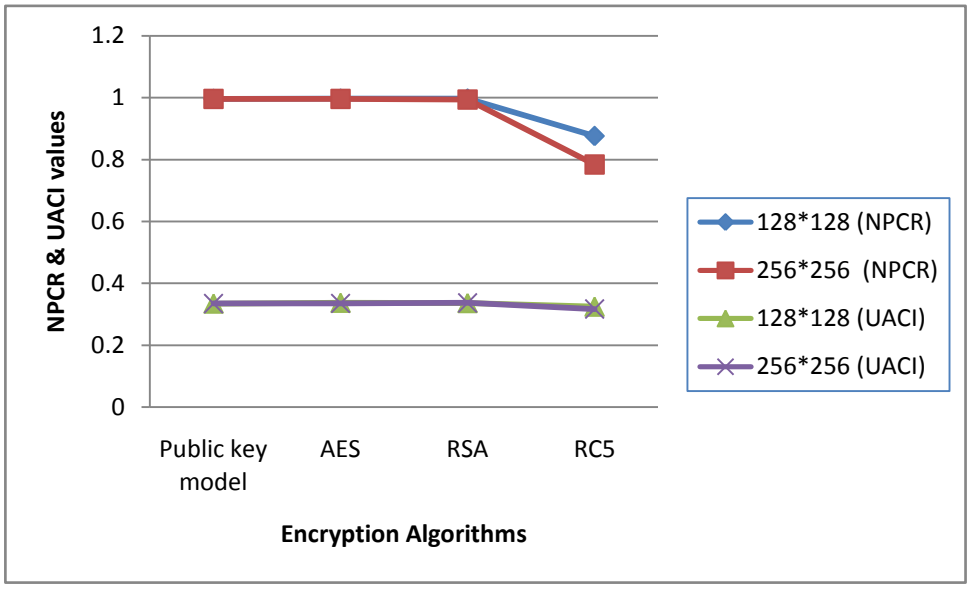

Fig 8: Comparison of NPCR & UACI analysis values for various Encryption Algorithms

As shown in Table 4, and Figure 8,the best encryption algorithms value for NPCR and UACI is the AES, and our public model which implies that the algorithms is secure against differential attack.

I. Key Sensitivity analysis

Chaotic neural network are highly sensitive to initial condition and system control parameters, and any algorithm for encrypting images should be robust enough to resist sensitivity-based attack. This means the cryptosystem should have high key sensitivity and plaintext sensitivity. Further, a tiny change, even a single pixel being modified by one bit, in the key or in the original image, causes a great difference in the cipher-image. These properties

make it difficult for diverse sensitivity-based (chosen plaintext, or differential) attacks to break the system. Chaotic map are highly sensitive to initial condition and system control parameters. Which mean, if there is a minute change, then decrypted image will no longer be similar to original image, which shown in Table 8 and Fig 9[32].

Table 8: Correlation coefficient of the key sensitivity analysis

	Key initial		**Correlation co-efficient**
	X	**Y**	
The public key model	0.883895	0.883895	0.00439953

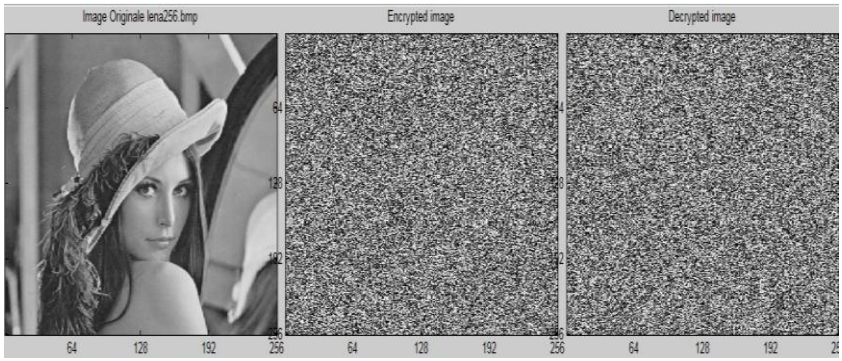

Fig 9: Sensitivity Analysis to secret key

VII. CONCLUSION

Chaos is statistically vague from randomness and yet it is deterministic and not random at all. Chaotic systems will produce the same results if given the same inputs it is unpredictable in the sense that you cannot predict in what way the system's behavior will change for any change in the input to that system. A binary sequence generated from a chaotic system, the biases and weights of neuron are set .So in the chaotic systems it is well known that it has sensitive dependence on initial conditions and it depends on the binary sequence which is unpredictable so it is very difficult to decrypt an encrypted data correctly by making an exhaustive search without knowing the parameters. In this work we have introduced a new public key model based on chaotic multi- layer neural network with multidimensional different chaotic maps. All the experimental analysis show that the proposed public key model has many advantages such as strongly sensitive to secrete key, effective histogram analysis, correlation coefficient analysis secure from statistical attacks, information entropy analysis give security of information leakage, and less computation time. These five experiments show that this proposed method is very robust and also saves the model from brute-force attacks and the obtained results are compared with some contemporary remarkable works in the same field. The detailed analysis of comparison deserves the superiority of the proposed algorithm.

REFERENCE

[1]. Miles E. Smid, Dennis K. Branstad. "The Data Encryption Standard: Past and Future", proceedings of the IEEE, Vol. 76, No. 5, 550-559, 1988.

[2].Menezes, A. J., Oorschot, P.C.V., Vanstone, S.A., "Handbook of Applied Cryptography", CRC Press, Boca Raton, 1997.
[3].William Stallings, "Cryptography and Network Security: Principles and Practice (6th Edition)", Prentice Hall, 2013.
[4].Ijaz Ali Shoukat, Kamalrulnizam Abu Bakar, MohsinIftikhar, "A Survey about the Latest Trends and Research Issues of Cryptographic Elements", IJCSI International Journal of Computer Science Issues, Vol.8, Issue 3, No.2, 140-149, 2011.
[5].Jianjiang CUI, Siyuan LI, Dingyu Xue, "A Novel Color Image Cryptosystem Using Chaotic Cat and Chebyshev Map", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 3, No 2, 63-69, 2013.
[6].Harpreet Kaur, Tripatjot Singh Panag, "Cryptography using Chaotic Neural Network", International Journal of Information Technology and Knowledge Management, Vol.4, No. 2, 417-422, 2011.
[7].Wenwu Yu, Jinde Cao, "Cryptography based on delayed chaotic neural networks", Physics Letters A, Vol. 356, (4) Elsevier, 333–338, 2006.
[8].Adel A. El-Zoghabi, Amr H. Yassin, Hany H. Hussien, "Survey report on cryptography based on neural network", International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 12, 456-462, 2013.
[9].Rajender Singh, Rahul Misra, Abhishek Chaudhary, "Power consumption using artificial neural network in the field of cryptography", Journal of information, Knowledge and research in computer Engineering, Vol.2, Issue.2, 443- 446, 2012.
[10]. Shweta B. Suryawanshi, Devesh D. Nawgaje, "A triple-key Chaotic neural network for cryptography in image processing", International Journal of Engineering Sciences & Emerging Technologies, Vol. 2, Issue. 1, 46-50, 2012.
[11]. Tariq A. fadil, Shahrul N. yaakob, Badlishahahmad, abidyahya, "Encryption of mpeg-2 video signal based on chaotic neural network", Journal of Engineering and Technology, Vol. 3, 35-42, 2012.
[12]. Navita Agarwal, Prachi Agarwal, "Use of Artificial Neural Network in the Field of Security", MIT International Journal of Computer Science & Information Technology, Vol. 3, No. 1, 42–44, 2013.
[13]. B. Geethavani, E. V. Prasad, "A Hybrid Model for Secure Data Transfer in Audio Signals using HCNN and DD DWT", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 4, No.7, 202-208, 2013.
[14]. Neethu Subash, MeeraVijayan, Varghese Paul, "A Triple Key 3-d Chaotic Image Encryption Method using Double Chaotic Neural Networks", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 1, 5015-5020, 2014.
[15]. M. Hénon, "A Two-Dimensional Mapping with a Strange Attractor", Commun. Math. Phys. 5D, 66-77, 1976.
[16]. Kuldeep Singh, Komalpreet Kaur, "Image Encryption using Chaotic Maps and DNA Addition Operation and Noise Effects on it", International Journal of Computer Applications (0975 – 8887), Volume 23, No.6, 17-24, 2011.
[17]. Chittaranjan Pradhan, Shibani Rath, Ajay Kumar Bisoi, "Non Blind Digital Watermarking Technique Using DWT and Cross Chaos",2 International Conference on Communication, Computing & Security , Elsevier, Vol. 6, 897–904, 2012.

[18]. X.Y. Wang, Q. J Shi, "New Type Crisis, Hysteresis and Fractal in Coupled Logistic Map." Chinese Journal of Applied Mechanics, 501-506, 2005.
[19]. Pawan N. Khade, Manish Narnaware, "3D Chaotic Functions for Image Encryption", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue. 3, No. 1, 323-328, 2012.
[20]. TaranjitKaur, Reecha Sharma, "TJ-ACA: An Advanced Cryptographic Algorithm for Color Images using Ikeda Mapping", International Journal of Computer Trends and Technology (IJCTT), Vol.4, Issue5, 1295-1300, 2013.
[21]. Ljupco Kocarav, Shingao Lian; "Chaos-based Cryptography theory algorithms and applications", Studies in Computational Intelligence, Volume 354, 2011.
[22]. Mintu Philip, "An Enhanced Chaotic image Encryption", International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol.1, No.5, 77-83, 2011.
[23]. RasulEnayatifar, "Image encryption via logistic map function and heap tree", International Journal of the Physical Sciences Vol. 6, No. 2, 221-228, 2011.
[24]. N. El-Fishawy, O. Zaid, "Quality of encryption measurement of bitmap images with rc6, mrc6, and rijndael block cipher algorithms", International Journal of Network Security, Vol. 5, no. 3, 241–251, 2007.
[25]. H. Elkamchouchi, M. Makar, "Measuring encryption quality for bitmap images encrypted with rijndael and kamkar block ciphers,"in Radio Science Conference, Proceedings of the Twenty-Second National. IEEE, 277–284, 2005.
[26]. S. Kamali, R. Shakerian, M. Hedayati, and M. Rahmani, "A newmodified version of advanced encryption standard based algorithm forimage encryption," in Electronics and Information Engineering (ICEIE),2010 International Conference On, Vol. 1. IEEE, V1–141, 2010.
[27]. M. El-lskandarani, S. Darwish, and S. Abuguba, "A robust and secure scheme for image transmission over wireless channels," in Security Technology, ICCST, 42nd Annual IEEE International Carnahan Conference on. IEEE, 51-55, 2008.
[28]. A. Mohamed, G. Zaibi, and A. Kachouri, "Implementation of rc5 and rc6 block ciphers on digital images," in Systems, Signals and Devices(SSD), 8th International Multi-Conference on. IEEE, 1-6, 2011.
[29]. Z. Liehuang, L. Wenzhuo, L. Lejian, and L. Hong, "A novel image scrambling algorithm for digital watermarking based on chaotic sequences," International Journal of Computer Science and Network Security, vol. 6, no. 8B, 125–130, 2006.
[30]. Lini Abraham, NeenuDaniel ," Secure Image Encryption Algorithms: A Review" , International Journal of Scientific & Technology Research, Vol. 2, Issue 4, 2013.
[31]. Jawad Ahmad, Fawad Ahmed, "Efficiency Analysis and Security Evaluation of Image Encryption Schemes", International Journal of Video & Image Processing and Network Security, IJVIPNS-IJENS, Vol.12, No. 4, 18-31, 2012.
[32]. R.Gnanajeyaraman, K.Prasadh , Vignesh, "Security Algorithm for Cryptosystems chaotic map", Global Journal of Computer Science and Technology, Vol. 9, Issue 5, (Ver 2.0), 50-54

View publication stats