NEURAL NETWORK FOR CRYPTOGRAPHY

Shweta B. Suryawanshi[1], Snehlata V. Bhokare[2]

[1,2]Department of E &TC, Asst. Prof. DYPIEMR, Akurdi, Pune, SPPU, (India)

ABSTRACT

Cryptography is the exchange of information among the users without leakage of information to others. Many public key cryptography are available which are related to number theory but it suffer from the drawback of requirement of large computational power, complexity and time consumption during generation of key. To recover these drawbacks, a neural network can be used to generate secret key. Here in this paper cryptography is performed using different methods and analysis is done for more security.

Keywords: Chaos, Cryptography, Decryption, Encryption, Neural Network

I. INTRODUCTION

Artificial Neural Networks are massively parallel adaptive network which consist of non-linear computing elements called Neurons [3]. ANN has no. of applications in various fields like communication, control, instrumentation etc. The ANN is capable of performing on nonlinear input and output systems in the workspace due to its large parallel interconnections between different layers and its nonlinear processing characteristics. The working of artificial neural network is weighted sum of input signal and the connecting weight. The sum is added with bias or threshold and resultant signal is then considered or proposed for sigmoid nonlinear function.

Cryptography is a word that has been derived from the Greek words for ‘Secret Writing’. Here sensitive information which is intelligible called plaintext is converted in to unintelligible form called cipher text and process is called Encryption. The reverse process is called Decryption. Many cryptographic algorithms use the secret value called key which is useful for encryption and decryption. [1,5]. Cryptography is exchanging the information between the related persons without leakage of information by unauthorized one. For this secure transmission or communication, data is encrypted at transmitter and decrypted at receiver. The encryption is obtained by scrambling the phase spectrum of original one, reverse process is used for decryption. [1,7]. the types of cryptography are Public, Secret and hash cryptography. If the same key is used at both for encryption and decryption then it is called as secret or symmetric cryptography and if different key is used then called public cryptography.

Ordinary data can be kept secured using number of encryption methods like DES (Data encryption standard), TDES(triple), IDEA (international data encryption algorithm), but problems occurred for real time application like audio or video has to be encrypted. Due to large data size, computational complexity and real time constraints, encryption of multimedia data becomes difficult. so chaotic scrambling of an image is more desirable than conventional methods.[2]

In this paper, we proposed to create a secret cryptography using triple key chaotic neural network. At both the sides same or symmetric key is used for encryption and decryption. The secret key provides the network parameter such as coupling strengths. The cryptography is obtained using chaotic neural network. Chaotic sequence which is a binary random but deterministic sequence used to mask or to scramble the original information. It results in to the data like noise signal so hackers or cryptanalyst can’t attract towards it

II. CHAOTIC NEURAL NETWORK

The meaning of chaos is not generally accepted but from a practical point of view chaos can be defined as bounded steady stat behavior that is not equilibrium point not periodic and not quasi periodic. It is a random and look like a noise but deterministic. Chaotic systems are non periodical sensitive to initial conditions, system parameters and topological transitivity. These properties are also remarkable for cryptanalysts. Noise like behavior of chaotic system is main reason of using this system in cryptology. Chaotic spectrum does not have discreet frequencies but has a continuous, broad band nature.

A network is called chaotic neural network if its weights and biases are determined by chaotic sequence. It is a stochastic behavior occurring in deterministic system.

In this, we consider the Hopfield neural networks which exhibit chaotic phenomenon.

$$x'(t) = -Cx(t) + Af(x(t)) + Bf(x(t-\tau(t)) + I \qquad (1)$$

$$x'_i(t) = -c_i x_i(t) + \sum a_j f_i(x_i(t)) + \sum b_j f_j(x_j(t-\tau_j(t))) + I_i,$$

$$i = 1,2,3\ldots\ldots n$$

Where, n denotes the number of units in a neural network.

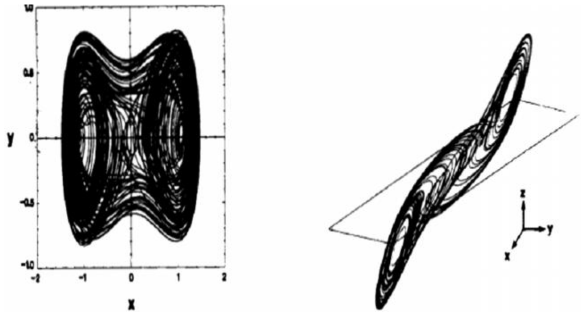

Figure 1: Chaotic Trajectories

$X(t) = (x_1(t), x_2(t)\ldots\ldots\ldots x_n(t))^T$ € R^n is the state vector associated with neurons.

$I = (I_1, I_2\ldots\ldots I_n)^T$ € R^n is the external input vector.

$F(x(t)) = (f_1(x1(t)), f_2(x2(t))\ldots\ldots f_n(xn(t)))^T$ € R^n is the activation function of neurons.

$\tau(t) = \tau_{ij}(t)$ $i,j=1,2,3\ldots.n$ are time delays.

Equation (1) exhibit chaotic phenomenon,

$$\begin{bmatrix} \frac{d_{x1}(t)}{dt} \\ \frac{d_{x2}(t)}{dt} \end{bmatrix} = -c \begin{bmatrix} x_1(t) \\ x_2(t) \end{bmatrix} + A \begin{bmatrix} \tanh(x1(t)) \\ \tanh(x2(t)) \end{bmatrix}$$

$$+ B \begin{bmatrix} \tanh(x_1(t-\tau(t))) \\ \tanh(x_2(t-\tau(t))) \end{bmatrix}$$

C= diagonal matrix

$A = (a_{ij})_{n \times n}$ and $B = (b_{ij})_{n \times n}$ are the connection weight matrix and delayed connection weight matrix. Pseudorandom number sequences with good properties are frequently used in secure communications and cryptosystem. Iterative equations are used to generate the chaotic dynamics.[6] Computation time for encryption and decryption depends on complexity of equations and value of state variables. If complexity of equation is low, computation time for encryption and decryption will be less otherwise it will take long time for computation. If the equation is with lower complexity then discrete map have to preferred, it involves basic arithmetic operation like addition, subtraction, multiplication and division. On the other hand, if the behaviour of chaotic equation is continuous in nature, it involves differential or integral operations to calculate value of the next state variable. From complexity point of view, integral value of the state variable is preferred because it takes shorter time for computing next state variable, if it is floating point then takes longer time for computation.

III. CRYPTOGRAPHY USING CHAOTIC NEURAL NETWORK

3.1 Cryptography using Simple Chaotic Neural Network

Image has some features like bulk data capacity, high data redundancy so encryption of image is different than that of the text, so conventional methods of cryptography are giving poor response for image cryptography. Ordinary data can be kept secured using number of encryption methods like DES, IDEA, but problems occurred for real time application like audio or video has to be encrypted. Due to large data size, computational complexity and real time constraints, encryption of multimedia data becomes difficult. so chaotic scrambling of an image is more desirable than conventional methods. For generating chaotic sequence 1D logistic map is used.

The one-dimensional Logistic map is proposed by R. M. May. It is one of the simplest nonlinear chaotic discrete systems that exhibit chaotic behaviour, defined by the equation:

$$z_{n+1} = \lambda z_n(1 - z_n)$$

where z_o is initial condition, λ is the system parameter and n is the number of iterations. The research shows that the map is chaotic for $3.57 < \lambda < 4$ and z_{n+1} belong to the interval (0, 1) for all n. The sequence generated from eq^n has random-like behaviour. The sequence doesn't require any type of pre-processing. The sequence generated by Logistic map of eq^n is used to encrypt. The logistic equation involves two multiplications and one subtraction per iteration.

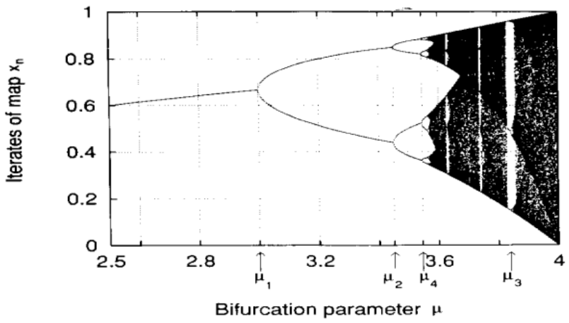

Figure 2: Bifurcation Diagram of Logistic Map

3.2 Cryptography Using Shuffled Image Concept with Chaotic Neural Network

In this, image is shuffled using cat map. Shuffling means to change the position co-ordinates of the original image. So it look like scrambled image but its histogram doesn't change. Cat map is periodic so it is combined with logistic map which is non periodic and cryptography is performed. A 2D Cat map is first presented by V.I. Arnold in the research of ergodic theory. Let the coordinates of positions of pixels in an image are P = {(x, y) | x, y = 1, 2, 3, . . ., N}, a 2D Cat map with two control parameters is as follows:

$$x' = (x + ay)\mathrm{mod}(N)$$

$$y' = (bx + (ab+1)y)\mathrm{mod}(N)$$

Where, a, b are control parameters which are positive integers and (x', y') is the new position of the original pixel position (x, y) of N x N plain-image when Cat map is applied once to the original. Cat map permutes/shuffles the organization of pixels of plain-image by replacing the position of the image pixel points with new coordinate. After several iterations, the correlation among the adjacent pixels is disturbed completely and the image appears distorted and meaningless. But after iterating many times it will return the original image i.e. the Cat map is periodic . To deal with the periodicity of Cat map, a block based image shuffling is performed using 2D Cat map in which the control parameters of the Cat map are randomly generated.

3.3 Triple Key Chaotic Neural Network

In triple key chaotic encryption method, 20 hexadecimal characters are entered as a session key. The binarisation of this hexadecimal key gives 80 bits. Some bits are extracted and some manipulations are performed on it to obtain the intermediate key. This intermediate key is combined with initial and control parameters to generate chaotic sequence. This is the concept of 'Triple key'. In this, there is three step protection to the original image user has to enter three keys to decrypt the image.

3.3.1 Algorithm

1. Read the image.
2. Determine the size and length of image.
3. Converting two dimensional image vector in one dimensional image vector.
4. Computing initial parameter from hexadecimal session key, A=$a_1a_2a_3\ldots a_{20}$. It consists of 80 bits i.e. binary representation of hexadecimal key.
5. X(1) = (s_1+s_2+s_3) mod 1.

   Where, $s_1=(a_{71}*2\wedge^{0}+\ldots.a_{84}*2\wedge^{7}+a1_{24}*2\wedge^{23})/2\wedge^{24}$

   $s_2=(a_{13}+a_{14}+\ldots.a_{18})/(16*6)$

   s_3= entered
6. Determine parameter μ.
7. Generate the chaotic sequence $x(1)$, $x(2)$,X(3)…..

   $x(M)$ by the formula

   $x(n + 1) = \text{m}x(n)\,(1 – x(n))$

   Create $b(0)$, $b(l)$, ..., $b(8M – 1)$ from $x(l)$, $x(2)$,.... $x(M)$ by the generating scheme that 0.$b(8m – 8)b(8m –7)$…............$b(8m – 2)$ $b(8m – l)$ … is the binary Representation of $x(m)$ for m = 1, 2,….M.
8. Weights and theta are decided

   for n = 0 to M – 1

$$g(n) = \sum_{i=0}^{l} d_i 2^i$$

For i = 0 to 7

$$w_{ij} = \begin{cases} 1 & j = i, b(8n+i) = 0 \\ -1 & j = 1, b(8n+i) = 1 \\ 0 & j \neq i \end{cases}$$

j={0, 1, 2, 3, 4, 5, 6, 7}

$$\theta_i = \begin{cases} \frac{-1}{2} & b(8n+i) = 0 \\ \frac{1}{2} & b(8n+i) = 1 \end{cases}$$

End

For i = 0 to 7

$$d_i' = f\left(\sum_{j=0}^{7} w_{ij} d_i + \theta_i\right)$$

```
    where $f(x)$ is 1 if $x$ >=0`
    End
    $g'(n) = \sum_{i=0}^{7} d'_i 2^i$
  End
```

7. Various image properties takes place on original and decrypted image.

IV. RESULTS

Image is encrypted and decrypted using session key = ‘A6C3D7F6D21E96B85B33S’,s_3=.9 and µ=3.8, result is shown in following figure. If the session key, initial and control parameter are unknown then result does not get proper so cryptanalyst unable to hack the information. The correlation co-efficient of original and encrypted image are **0.7747** and **-0.0749** respectively. This difference between them indicates that original image is perfectly encrypted. Fig. 2 shows original image, encrypted image and decrypted image with known parameters and unknown parameters

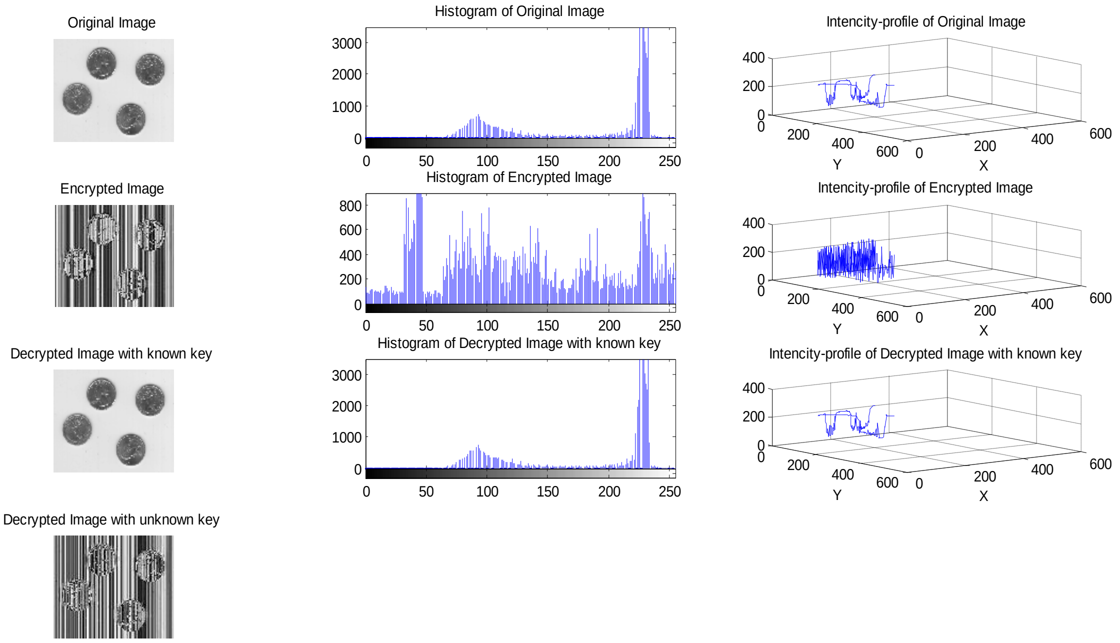

Figure 3: Original Image, Encrypted Image and Decrypted Image with Known Parameters and Unknown Parameters Using Simple Chaotic Neural Network

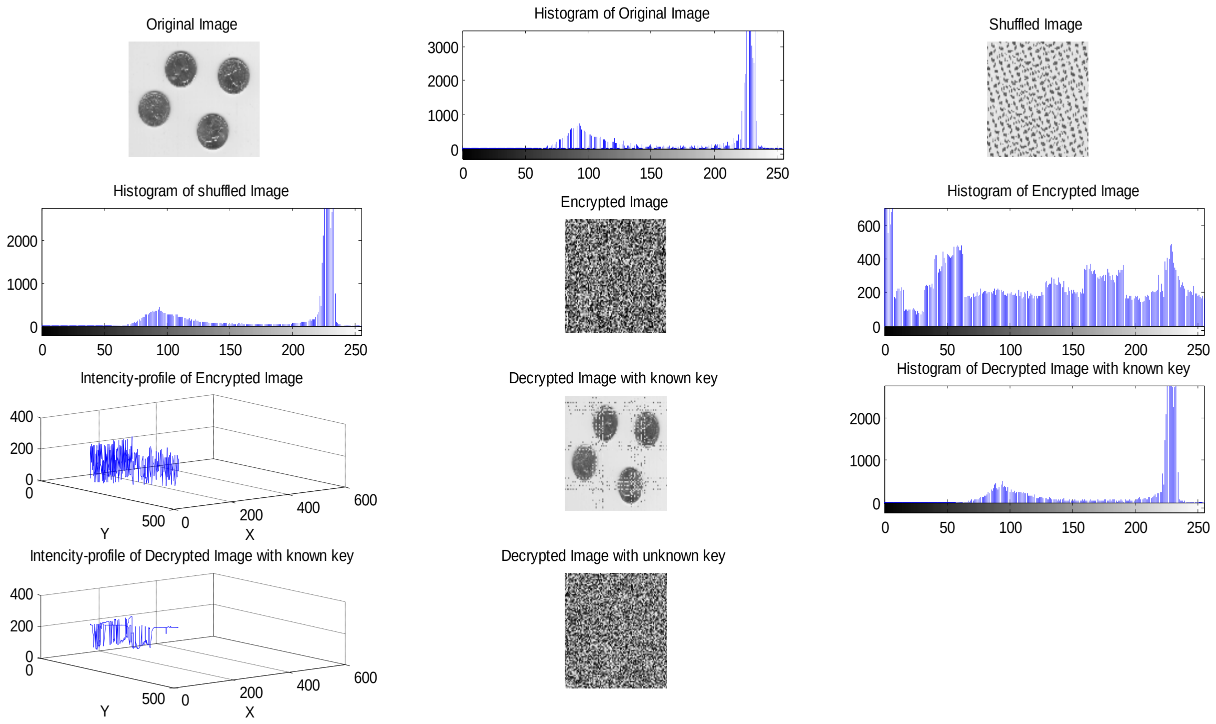

Figure 4: Original Image, Encrypted Image and Decrypted Image with Known Parameters and Unknown Parameters Using Shuffled Chaotic Neural Network

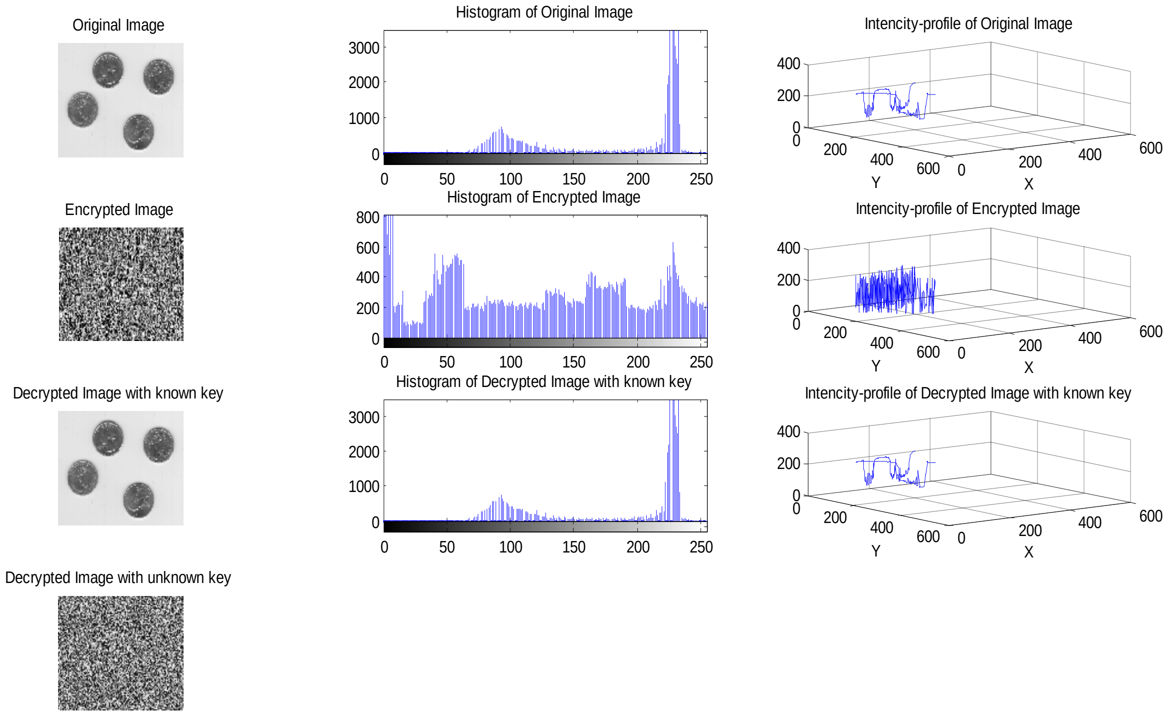

Figure 5: Original Image, Encrypted Image and Decrypted Image with Known Parameters and Unknown Parameters Using Triple Key Chaotic Neural Network

V. ANALYSIS

To analyze the original image and decrypted image, various image properties are taking on original image and decrypted image like entropy, histogram, mean, intensity profile. Results obtained from these properties are exactly same so this is 100% correct and guaranteed high secured method.

Table 1: Cryptography Using Simple Chaotic Neural Network

Eight.tif	Original image	Encrypted image	Decrypted image
Correlation co-efficient	0.7308	-0.0872	0.7308
Entropy	4.8796	7.6737	4.1796
Mean	198.2587	128.4423	198.2587

Table 2: Cryptography Using Shuffled Chaotic Neural Network

Eight.tif	Original image	Encrypted image	Decrypted image
Correlation co-efficient	0.7308	-0.0631	0.3664
Entropy	4.8796	7.8569	5.1982
Mean	198.2587	121.9045	198.0857

Table 3: Cryptography Using Triple Key Chaotic Neural Network

Eight.tif	Original image	Encrypted image	Decrypted image
Correlation co-efficient	0.7308	-0.1480	0.7308
Entropy	4.8796	7.8467	4.8796
Mean	198.2587	122.5045	198.2587

VI. CONCLUSION

Triple key chaotic neural network is secured way for cryptography. It is highly depends on the session key, initial and control parameters. Without knowing this triple key ,no one can decrypt the cipher text. A chaotic sequence i.e. binary sequence generated from chaotic system, biases and weights of neurons are set and are unpredictable. Among the various chaotic neural networks triple key chaotic neural network is having good security. Hence chaotic neural network is one of the guaranteed high secured. This method can be used for colour images of various sizes.

REFERENCES

[1] Shweta B Suryawanshi and Devesh D Nawgaje., 'Chaotic Neural Network for Cryptography in Image Processing'. IJCA Proceedings on 2nd National Conference on Information and Communication Technology NCICT(3):, November 2011. Published by Foundation of Computer Science, New York, USA.

[2] Srvidya, G. Nandakumar, P, 'A Triple-Key chaotic image encryption method', Communications and Signal Processing (ICCSP), 2011 International Conference on Feb. 2011 ,266 – 270

[3] T.Godhavari,'Cryptography using neural network', IEEE Indicon 2005 Conference, Chennai, India, 11-13 Dec. 2005,258-261.

[4] Harpreet Kaur and Tripatjot Singh Panag, ‘cryptography using chaotic neural network’ , International Journal of Information Technology and Knowledge Management July-December 2011, Volume 4, No. 2, pp. 417-422.

[5] Miles E. Smid and Dennis K. Branstad.‘The Data Encryption Standard: Past and Future’, proceedings of the ieee, vol. 76, no. 5, may 1988,550-559.

[6] C. Boyd, ‘Modem Data Encryption’, Electronics & Communication Journal, 1993.

[7] Chung J.Kuo and Maw S. Chen., ‘A new signal encryption tech. and its attack study’, ch3031-2/91/0000-0149 81.00' 1991 ieee,149-153.

[8] Ilker Dalkiran, Kenan Danisman. ‘Artificial neural network based chaotic generator for cryptography’, Turk J Elec Eng & Comp Sci, Vol.18, No.2, 2010.,225-240.

[9] An Introduction to Neural Network’ by Ben Krose Wenwu Yu, Jinde Cau, ‘Cryptography based on delayed chaotic neural network’, Physics Letters A 356 (2006) 333–338.