International Journal of Engineering Sciences & Emerging Technologies, April 2012.
ISSN: 2231 – 6604 Volume 2, Issue 1, pp: 46-50 ©IJESET

A TRIPLE-KEY CHAOTIC NEURAL NETWORK FOR CRYPTOGRAPHY IN IMAGE PROCESSING

Shweta B. Suryawanshi[1], Devesh D. Nawgaje[2]
[1]Department of E&TC, SSGMCE, Shegaon, Amaravati University,
suryawanshi.shweta@gmail.com
[2]Department of E&TC, Sr. Faculty, SSGMCE, Shegaon, Amaravati University,
dnawgaje@gmail.com

ABSTRACT
Cryptography is the exchange of information among the users without leakage of information to others. Many public key cryptography are available which are based on number theory but it has the drawback of requirement of large computational power, complexity and time consumption during generation of key. To overcome these drawbacks, a neural network can be used to generate secret key. Many methods using chaotic neural network for cryptography here in this paper 'Triple key' is using in the network to encrypt and decrypt the data. Three different parameters which are decided by user are used to scramble the image data and so hackers get many difficulties to hack the data hence providing more security. For simulation MATLAB software is used. The experimental results shows that algorithm successfully perform the cryptography and highly sensitive to the small changes in key parameters.

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.

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 (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. Triple key means three parameters that are initial and control parameters and hexadecimal sequence. 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 behaviour 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 behaviour 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.

Chaos signals are considering better for practical because of its characteristics above mentioned. Field of information security is nothing but the combination of two concepts that are cryptography and chaos theory. A network is called chaotic neural network if its weights and biases are determined by chaotic sequence. It is a stochastic behaviour 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.

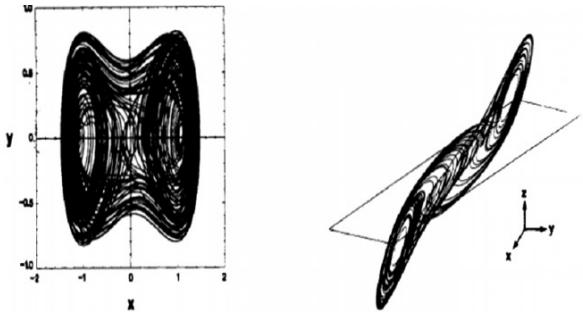

Figure1: Chaotic Trajectories

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

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

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

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

Equation (1) exhibit chaotic phenomenon,

$$\begin{bmatrix} \frac{dx_1(t)}{dt} \\ \frac{dx_2(t)}{dt} \end{bmatrix} = -C \begin{bmatrix} x_1(t) \\ x_2(t) \end{bmatrix} + A \begin{bmatrix} \tanh(x1(t)) \\ \tanh(x2(t)) \end{bmatrix} + B \begin{bmatrix} \tanh(x_1(t-\tau(t))) \\ \tanh(x_2(t-\tau(t))) \end{bmatrix}$$

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 behavior 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. 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 entered three keys to decrypt the image.

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. $X(1) = (s_1+s_2+s_3) \bmod 1$.

   Where, $s_1=(a_{71}*2\text{^}0+\ldots.a_{84}*2\text{^}7+a1_{24}*2\text{^}23)/2\text{^}24$
   $s_2=(a_{13}+a_{14}+\ldots.a_{18})/(16*6)$
   s_3= entered
6. Determine parameter μ.
7. Generate the chaotic sequence $x(1)$, $x(2)$,X(3)…..
   $x(M)$ by the formula
   $x(n + 1) = mx(n)\,(1 - x(n))$
   Create $b(0)$, $b(1)$, ..., $b(8M - 1)$ from $x(1)$, $x(2)$,.... $x(M)$ by the generating scheme that $0.b(8m - 8)b(8m - 7)\ldots..\ b(8m - 2)\ b(8m - 1)$ … is the binary Representation of $x(m)$ for m = 1, 2,….M.
8. Weights and theta are decided
   for $n = 0$ to $M - 1$

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

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}

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

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 are 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. To analyse the encryption quality correlation coefficient is calculated. 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. The figure2 shows original image, encrypted image and decrypted image with known parameters and unknown parameters

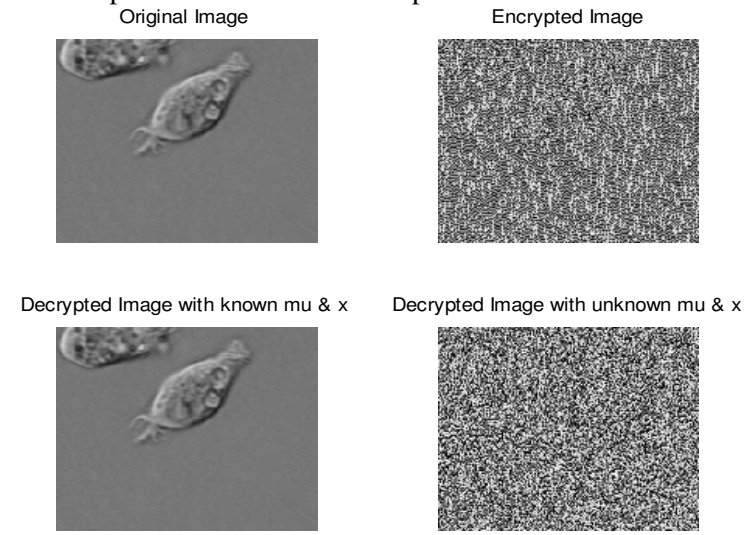

Figure2: original image, encrypted image and decrypted image with known parameters and unknown parameters.

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.

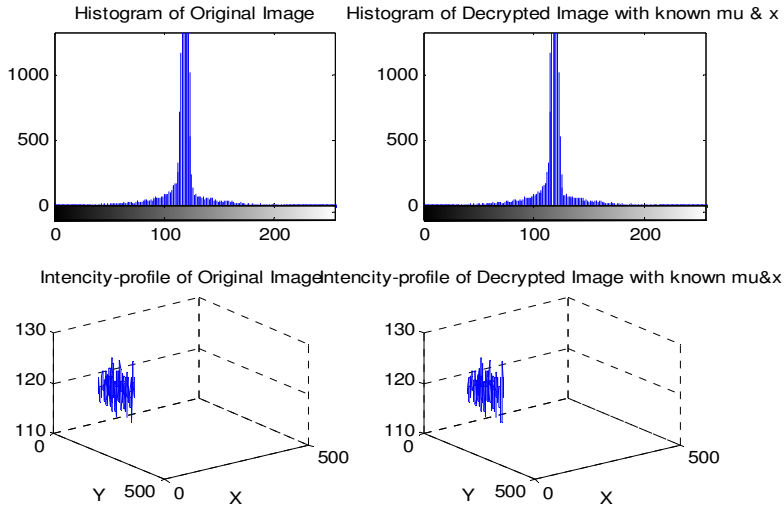

Figure3: Histogram and intensity profile of original image and decrypted image

V. CONCLUSION

In this paper presented the algorithm that performs encryption and decryption based on the concept of chaos. Triple parameters are used to perform the various operations on image so as to scramble the data in particular way which look like random but actually it is in particular sequence. At decryption image is decrypted in the same way of encryption. 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. 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]. Srividya, 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 .
[10]. Wenwu Yu, Jinde Cau, 'Cryptography based on delayed chaotic neural network', Physics Letters A 356 (2006) 333–338.

Authors

Shweta B. Suryawanshi. is a PG. student of SSGMCE, Shegaon, Maharashatra, India. She is doing project in neural network

Devesh Nawgaje is with Department of E&TC, Sr. Faculty, SSGMCE, Shegaon, Amaravati University, Maharashatra, India.