POWER CONSUMPTION USING ARTIFICAL NEURAL NETWORKS IN THE FIELD OF CRYPTOGRAPHY

[1] ER RAJENDER SINGH, [2] ER. RAHUL MISRA, [3] ABHISHEK CHAUDHARY

[1,2] M.Tech. Student, Department Of Computer Science, Bhagwant University, Ajmer, Rajasthan
[3] Asst.Professor, Department Of Computer Science, Bhagwant University, Ajmer, Rajasthan

rajendersinghk @gmail.com, misra.rrahul @gmail.com, abhishek02mar@rediffmail.com

***ABSTRACT*:** *Cryptography is the exchange of information among the users without leakage of information to others. Much 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. Today as we all know that energy and power are being scarce resources, their efficient utilization and over use remained a heated topic on international forums. The average energy consumption per person per annum is expected to cross the value of 2000 kg of energy /fuel resources .The Gauged estimations are limited .There is no mechanism for regular checks on idle losses which results in high financial losses [4]. So to overcome with all these drawbacks we analyzed neural networks in the field of cryptography. This can be achieved by "Chaotic Neural Network" which is an application of Artificial Neural Networks .Chaotic Neural Network uses "Triple key" in the network to encrypt and decrypt the data .Beside this certain parameters are decided by the user to scramble the image data and so cryptanalysis or hackers gets many difficulties to hack the data hence providing more security. For simulation and results we use "Chaotic Neural Network" and experimental results also shows that Chaotic Neural Network based algorithm successfully perform the cryptography and as well as highly sensitive to the generation of key, So we can say that it is a best approach for power consumption, time consumption and as well as for computing applications.*

***Keywords*— Chaos, Cryptography, Decryption, Encryption, Artificial Neural Network, Chaotic Neural Network, cryptanalysis or hackers.**

1. INTRODUCTION

The energy supply demand ratio has been a serious issue in most of the countries. Mismanagement, theft and artificial pricing are some of many reasons responsible for such situations .It is further compounded by the inability of users to measure their accurate needs of energy resources .A mechanism is directly needed for effective handling of these problems. As the growing numbered heating units in a distributed environment, data transfer applications and security aspects during data transfer is difficult to measure ,a mechanism has to be developed using these functional units so as to save time, budget and bringing in professional accuracy[4]. Furthermore, when we consider security aspects in data communication, Public Key Cryptography requires large computational power, complexity and time consumption during generation of key. In order to deliver novel ways for efficient control based mechanism and ANN is the required answer to this question[4];Artificial Neural Networks are parallel adaptive network and it is an information processing paradigm that is inspired by the biological nervous system such as the brain process and it has vast number of applications in fields like communication, control, instrumentation etc and as well as it is configured for specific applications such as pattern recognition or data classification through a learning process [2]. The ANN is capable of performing non-linear input and output systems in the workspace due to its large parallel interconnections between different layers and its non-linear processing characteristics.

This paper examines the comparison between conventional methods of cryptography, its power consumption techniques and recently techniques of cryptography by using "Chaotic Neural Network" which is application of Artificial Neural Network [1]. This paper examines this comparison because conventional methods of cryptography can secure ordinary data like text by using Triple DES, DES and IDEA (International Data Encryption Algorithm) but when we considering Audio Files, Video Files and Image data then problems are occurred because real time application such as video files ,audio files, image data has some features like bulk data capacity ,high data redundancy and due to all these features it consumes more power and more time while using conventional methods and on the contrary encryption of real application is difficult than that of simple text document and giving poor response for real time applications ,so using " Chaotic Neural Network "or Chaotic Scrambling is more desirable than conventional methods.[3]

2. RELATED WORK

Many Researches are carried on encryption and decryption technique of real media applications with the help of neural networks but it is difficult to understand and especially hard to predict how well a certain neural network will be able to predict the carrier signal. For this reason, much of the first portion of the research was simply trying different structures of neural networks, and what worked the best it all depends on the number of past inputs .If past inputs are less then it will not predicted the best chaotic carrier signal and vice versa. But this approach is not a practical approach and as well as during decryption the decrypted message was of medium quality or bad quality, so we are not using this approach [5].

Wenwn Yu Jinde Cao introduced cryptography based on delayed chaotic neural networks .he proposed a novel approach of encryption based on chaotic Hopfield neural networks with time varying delay is proposed .We use the Chaotic neural network to generate binary sequences which will be used for masking plaintext .The plaintext is masked by switching of chaotic neural network and permutation of generated binary sequences .Simulation results were given to show feasibility and effectiveness of the proposed scheme. As a result chaotic cryptography becomes more practical in the secure transmission of real media streaming applications over public data communication network. [6]

For Power consumption we will study the computation time for encryption and decryption which depends on the complexity of equations and the value of state variable because lower the complexity of the equations the shorter the computation time will be and vice versa. This reduced computation time will leads to less power consumption and vice versa.[7]

3. EXPERIMENTAL DESIGN

3.1 Cryptography achieved by using "Chaotic Neural Network"

3.1.1 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'. To prove the concept of chaotic neural network using triple key mechanism for encryption and decryption we use real time applications for e.g. image data .In this we use three step protections to protect the original image and user has to enter 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 that is binary representation of hexadecimal key.
5) $X(1) = (S_1+S_2+S_3) \bmod 1$, where

$$S_1 = \frac{a_{17} \times 2^0 + \cdots + a_{84} \times 2^7 + a_{124} \times 2^{23}}{2^{24}}$$

$$S_2 = \frac{a_{13} + a_{14} + \cdots + a_{18}}{16 \times 6}$$

$$S_3 = Entered$$

6) Determine parameter μ.
7) Generate the chaotic sequence x(1), x(2), x(3)…..x(M) by the formula $x(n + 1) = \mu x(n)(1 - x(n))$ and 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) form = 1, 2,.. . .,M.
8) Weights and theta are decided for n=0 to M-1.

for n = 0 to M – 1

$$g(n) = \sum_{i=0}^{7} d_i 2^i$$

for i = 0 to 7

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

$j \in \{0, 1, 2, 3, 4, 5, 6, 7\}$

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

end

for i = 0 to 7

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

where f(x) is 1 if x >=0

end

$$g'(n) = \sum_{i=0}^{7} d_i' 2^i$$

end

9) Various Images properties are takes place on original and decrypted image.

3.1.2 Power Consumption during Encryption and Decryption

The performance metrics for this purpose are based on computation time. The computation time .The Computation time for encryption and decryption depends on the complexity of equations and the value of state variable.

The Complexity of Equations:-

The lower the complexity of the equation the shorter the computation time and this will leads' to less consumption of power. If the complexity of equation was low, it would obviously reduce the computation time which will leads to less power consumption during data encryption and data decryption. On the other hand if the complexity of equation was high, a longer time would be needed for data encryption and decryption, which will leads will leads to more consumption of power. It is necessary that we must choose an equation with lower complexity, a discrete map is suggested .If the nature of Chaotic equation was a discrete map , it would only involve in basic arithmetical operations like multiplication, summations and division etc.On the other hand if the nature of chaotic equation was a continuous flow ,it would involve differential or integration type operations when calculate the value of next state variable.

The value (S) of State(S) Variable:-From the complexity point of view an integral value of state variable is more preferable .If the value of state variable was an integer it would take shorter time for computing the value of next state variable .This integer value will leads to less power consumption and efficient utilization of resources. On the other hand if the value of state variable was floating point number then it would need a longer time for computing the value of next state variable this will leads to more consumption of power and inefficient utilization of resources.

4. SIMULATION AND RESULTS EXPERIMENTAL DATA

4.1 Effects on Real Time Applications during encryption and decryption using "Chaotic Neural Network"

For this purpose we consider an image data for encryption and decryption .Image is encrypted and decrypted using session key ='A6C3D7F6D21E96B85B33S', S3=9 and μ=3.8,result is shown in the following figure .If the session key initial and control parameter are unknown then result is not upto the standard mark so cryptanalyst unable to hack the information .In order to identify the encryption quality correlation coefficient is calculated. The co-relation coefficient of original and encrypt image are 0.7747 and -0.0749 respectively .Furthermore we can understand the whole process with the help of following figure:-

Original Image (1) Decrypted Image (1)

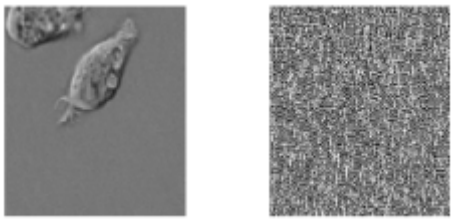

Fig. 3.1: Decrypted Image with known μ and x

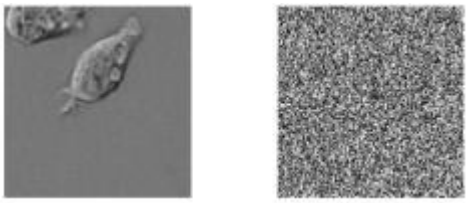

Fig. 3.2: Decrypted Image with unknown μ and x

Besides this to analyze the original image and decrypt image, various image properties are taken into concern like entropy, histogram, mean etc. Results obtained from these properties are exactly same so this is 100% correct and guaranteed highly secured method.

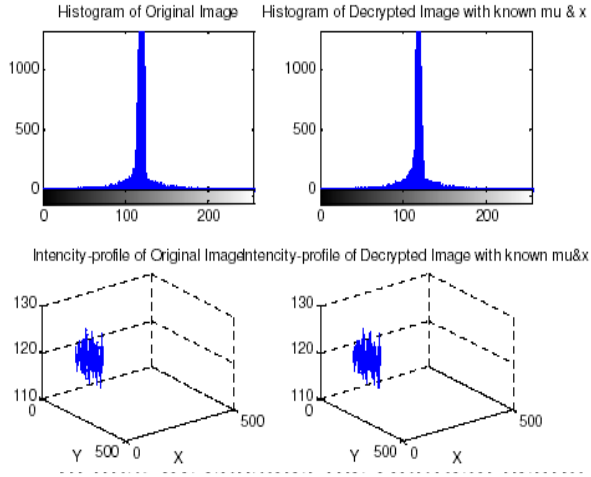

Fig. 3.3 Histogram and intensity profile of original image and decrypted image

4.2 Power Consumption using chaotic neural network

In the field of cryptography by complexity of equations in which "time" being the important factor

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

$$x'_i(t) = -c_i x_i(t) + \sum a_j f_i(x_i(t)) + \sum b_j f_j(x_j(t-\tau_j(t))) + I_i, \quad i=1,2,3\ldots\ldots n$$

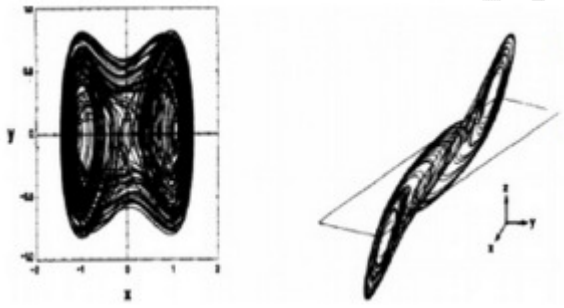

Fig 4.1. Chaotic Trajectories

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

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

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

$\tau(t) = \tau_{ij}(t)$

i,j=1,2,3….n are time delays.

5. CONCLUSIONS AND FUTURE RESEARCH

Chaos is statistically indistinguishable 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 behaviour 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 x(0) and μ. Hence ,CNN is one of the guaranteed high security. This time we are much concern about security aspects but in future we move our focus much towards on power consumption by providing security aspects also .This time also we are giving a little emphasis on power consumption but with only one prime factor that is time consumption but in future we tried our best to provide not only security with the help of chaotic neural network but we consume power also using chaotic means of cryptography by using other factors also such as throughput, time etc.

REFRENCES

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

[2] Shweta B.Suryawanshi and Devesh D Nawgage ,'Chaotic Neural Network for cryptography in image processing',IJCA Proceedings on 2nd National Conference on Information and Technology.

[3] Srividya G.Nandakumar,P 'A Triple Key Chaotic Image Encryption Method', Communication & signal Processing (ICCSP), [2011].

[4] International Journal of Advanced Science and Technology "An Intelligent Neural Wireless Sensor Network Based Schema for Energy Resources Forecast " by Aaqif Afzaal Abbasi & Asif Kamal, Vol 33, Aug, [2011].

[5] Decryption of Chaotically Encrypted Signals using Neural Networks Gaig Tainter Faculty Sponsor: - Jeffrey Baggett, Department of mathematics Uw-L Journal Of Undergraduate Research X [2007].

[6] Wenwu Yu Jinde Cao –Cryptography based on delayed chaotic Neural networks Dept of mathematics, southeast university Nanjing 210096 China Received, Communicated by A.R. Bishop, Feb-2006, Revised 10 Mar2006 accepted 28 March 2006.

[7] International Journal of Information Technology & knowledge Management Cryptography using chaotic neural network by Harpreet Kaur & Tripaljot Singh Panag, Vol 4 No-2 PP-417-422, July December [2011].