Encryption And Decryption Algorithm Based on Neural Network

Mrs.K. Krishna Jyothi[1], Gopi Somjiyani[2], B. Thulasi[3], V. Yashaswini[4], and P. Shivani[5]
[1]*Associate Professor, Hyderabad institute of technology and management, Medchal, Telangana*
[2,3,4,5] *UG student, Hyderabad institute of technology and management, Medchal, Telangana*

Abstract— The project is aimed to implement artificial neural network method in cryptography. Cryptography is a technique to encrypt simple message into cipher text for secure transmission over any channel. The training of the neural network has been done using the input output set generated by the cryptosystem, which include shift and RSA ciphers. The training patterns are observed and analysed by varying the parameters of Levenberg Marquardt method and the count of neurons in the hidden layer. Using the converged network, the model is first trained, and one may obtain the desired result with required accuracy. In this respect, simulations are shown to validate the proposed model. As such, the investigation gives an idea to use the trained neural network for encryption and decryption in cryptography

INTRODUCTION

The rising growth of technology in the communication sector has always created an increased demand of secure channel for the transmission of data. Cryptography has always served as a successful means to build such channels. These channels find numerous applications, as in mobile phones, internet, digital watermarking etc. and also for secure transmission protocols. There are several encryption-decryption techniques which may be improvised for a secure transfer of data, like public and private key cryptosystems. However, the risk of attack by an intruder is still very high. A novel approach has been adopted here by applying neural network to cryptography. As such, in case of shift ciphers, the transfer of message would not be safe if the key is public. So sending it over a neural network, where in, keeping the key private, the transfer becomes secure. Also, in the case of RSA cryptosystem, where two keys are involved which may be easily retrieved by solving the factor problem, the implementation of neural network serves as an efficient method.

The primary objective of this project is to implement encryption and decryption of shift and RSA cryptosystems, in artificial neural network. The network construction depends solely on the parameters used in the training algorithm and the number of hidden neurons. The aim is to obtain an efficient training pattern with the help of proper algorithm and parameters, such that the errors are minimised with better accuracy.

LITERATURE SURVEY

Previously many investigations have been carried out by various researchers in Cryptography using Neural Networks. As such, few literatures are discussed below:

Zurada has discussed artificial neural network with respect to different learning methods and network properties. Supervised and unsupervised learning has been elaborated in detail with the help of network architecture. The usage of parameters for training is illustrated. The minimization of error functions in multilayer feedforward networks have been explained using the backpropagation algorithm.

Koshy has emphasized on the problem-solving techniques and their applications. With the help of Fermat's Little Theorem, we may find the least residues. Different cryptosystems and their algorithms illustrate the encryption-decryption methods. Depending on the key usage, the cryptosystem has been subdivided and explained in detail. Kanter and Kinzel presented the theory of neural networks and cryptography based on a new method by the synchronisation of neural networks for the secure transmission of secret messages. The encryption based on synchronisation of neural networks by mutual learning has been implemented which involves construction of two neural networks, where the synaptic weights are synchronised by the exchange and learning of mutual outputs for the given inputs. The network of one may be trained by the output of the other. In case, the outputs do not adhere with each other, the weights are adjusted and updated using the Hebbian learning rule. The

synchronisation of those two networks occurs in a definite time which tends to decrease with the increasing size of inputs. The author focuses on accelerating the synchronisation process from hundreds of time steps to the least possible value and maintaining the security of the network at the same time Laskari et al. studied the performance of artificial neural networks on problems related to cryptography based on different types of cryptosystems which are computationally intractable. They have illustrated various methods to address such problems using artificial neural networks and obtain better solutions. The efficiency of a cryptosystem may be judged by its computational intractability. This paper deals with the study of three problems, namely, discrete logarithmic problem, Diffie-Hellman key exchange protocol problem and factorisation problem. The artificial neural networks have been utilized to train a feedforward network for the plain and ciphered text using backpropagation technique. It aims to assign proper weights to the network in order to minimise the difference between the actual and desired output. The normalised data is fed to the network and then its performance is evaluated. The percentage of trained data and its near measure is evaluated.

Meletiou et al. has discussed RSA cryptography and its susceptibility to various attacks. The author has used the artificial neural network for the computation of the Euler totient function in the determination of deciphering key and hence, RSA cryptography may be easily forged. The multilayer feedforward network is used for training the data set with backpropagation of errors. Learning rate of network may not be ideal but is asymptotically approachable. The network performance is measured by using the complete and near measure of errors. Also, the result has been attested for prime numbers ranging from high to low values.

METHODOLOGY

Models of an Artificial Neural Network An artificial neural network model encompass the following components:

- Input layer – It consists of all the input data that has been supplied to the network.
- Hidden layer – It consists of all the passive inputs that have been supplied by the preceding layers.
- Output layers – It contains the outputs of the neural network.
- Weights and biases – They have the effect of increasing or lowering the net input of the activation function depending on whether it is positive or negative respectively.
- Epochs – The number iterations in a neural network.
- Activation functions – It is an abstraction that represents the rate of firing in the cell. It is used for transforming the input signal of a neuron into the output signal

In a feedforward network, perceptrons may be arranged in layers. The input is taken by the first layer and output is produced by the last. Also, the middle layers are not connected to the external world and referred as the hidden layers. Each perceptron in the first layer is associated to the other perceptron in the next layer. Hence, information is always fed forward from one layer to the next. That is why it is referred as feedforward network.

The Levenberg Marquardt method may be used in concomitance with the backpropagation method to train a neural network. It has been designed to approach the second order training speed without computing the Hessian matrix in a way similar to that of quasi-Newton methods.

IMPLEMENTATION

TRAINING OF SHIFT CIPHERS

A shift cipher is a substitution cipher where we substitute each letter by another. The plain text may be encrypted by using the relation C P k ≡ + (mod 26) where C is the cipher text, P is the plain text and k is the shift factor, (0 25) ≤ ≤ k.

For training of the neural network, initially a sentence is selected. The following phrase has been used for training:

"SILENCE IS GOLDEN."

Then the letters are assembled into blocks of two and the adjacent number to each letter is written. In this instance, we use a shift factor (k) = 2 and the generated input output data is given in Table 1. This data set is accustomed to train a neural network taking input as P and target output as Normalised C . The neural network may be trained using the plain text (P) and the normalised C presented in Table 1 using MATLAB. The training starts as follows:

- Launch neural network toolbox, nntool in MATLAB.
- Import all the input (P) and target output value (Normalised C).

• Create a 2-layer feedforward network, with a known number of neurons in the hidden layer. Also, select a transfer function. For present problem, sigmoid function is selected.
• Simulate the test point values for networks with varying parameters. Number of hidden neurons is taken as 15.

TRAINING OF THE RSA CIPHERS

In this section RSA ciphers have been trained using neural network. RSA is an asymmetric public key cryptosystem, whose efficiency is based on the practical difficulty of solving factor problems. The algorithm to generate RSA cipher from plain text has been elaborated below:

Algorithm
• Select prime numbers p and q .
• Compute the product n p q = × .
• Compute Euler totient function ϕ = − − (1)(1) p q .
• Select public exponent e , 1< <e ϕ such that gcd(,) 1 e ϕ = .
• Compute the private exponent d by ( ) mod 1 d e × = ϕ .
• Public key is { , } n e and private key is { }d . For encryption: C P e n ≡ (^) (mod) For decryption: P C d n ≡ (^) (mod) where P is plain text and C is cipher text. The RSA cipher for the sentence (1) as stated above is generated using the following MATLAB code. The value of n=2773 and e=21.

MATLAB CODE:

```
a=input('Enter the value of a');
 m=mod(a,2773);
 for i=1:20
s=a*m;
 m=mod(s,2773);
end fprintf('Mod value %f',m);
```

Again, arranging the text into blocks of two and writing its corresponding numerical values, the plain text and ciphered text are accustomed for training which are given in Table 2.

We train a neural network for 15 hidden neurons and obtain the simulations at different test points, for different values of μ , μ _ dec and μ _ inc . The subsequent tables show the test results for the different parameters taken.

DATA FLOW DIAGRAM AND FLOW CHART

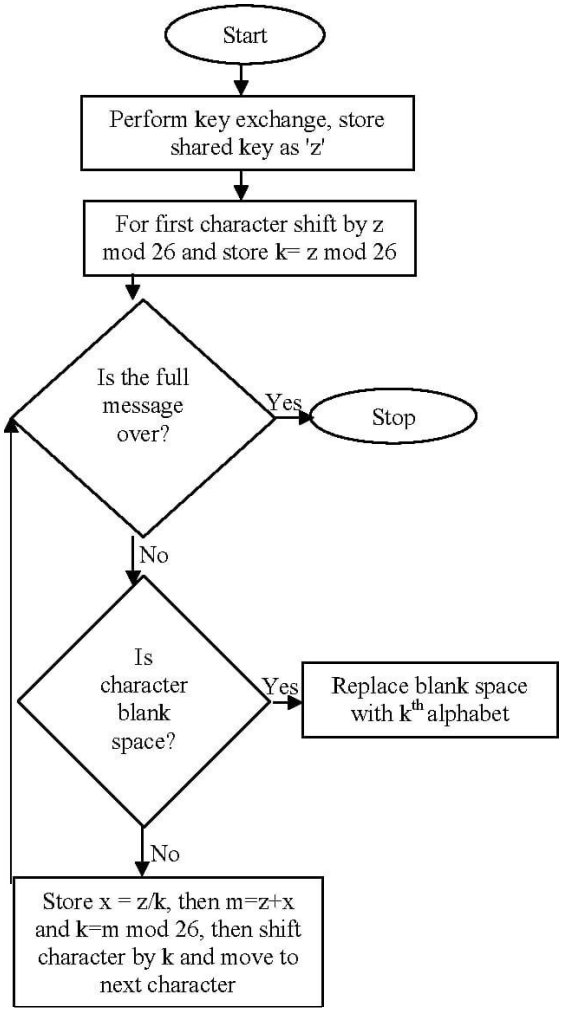

DIAGRAM 1: SHIFT CIPHER FLOW CHART

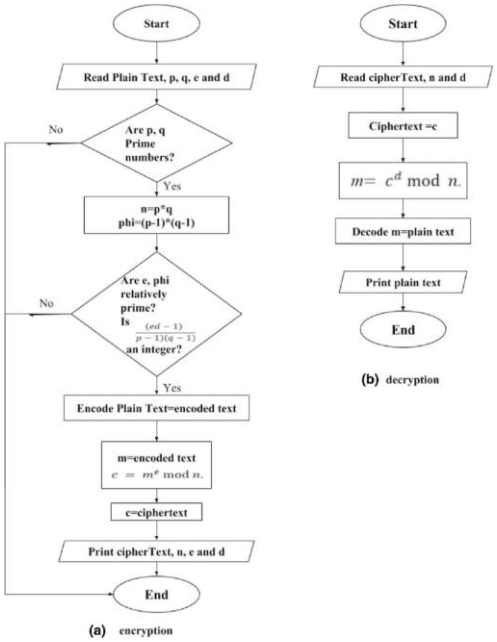

DIAGRAM 2: FLOW CHART FOR RSA ALGORITHM

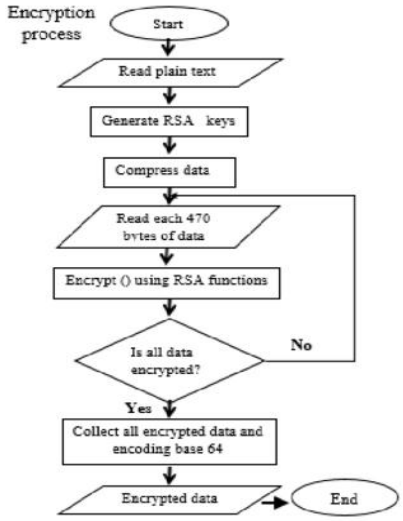

DIAGRAM 3: DATA FLOW CHART FOR RSA ENCRYPTION

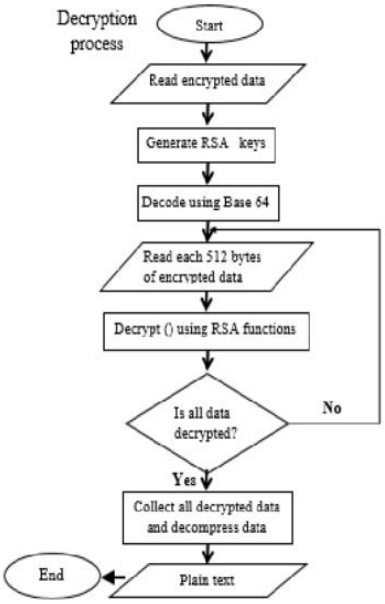

DIAGRAM 4: DATA FLOW CHART FOR RSA DECRYPTION

RESULTS

TEXT	P	C	NORMALISED C
SI	1808	2010	0.766
LE	1104	1306	0.4977
NE	1302	1504	0.5732
EI	0408	610	0.2325
SG	1806	2008	0.7652
OL	1411	1613	0.6147
DE	0304	506	0.1928
NT	1319	1521	0.5796
HE	0704	906	0.3453

TABLE 1 Values obtained from trained network for shift cipher

TEXT	P	C	NORMALISED C
SI	1808	10	0.0037
LE	1104	325	0.1207
NE	1302	2015	0.7482
EI	0408	2693	1
SG	1806	2113	0.7846
OL	1411	2398	0.8905
DE	0304	2031	0.7542
NT	1319	1760	0.6535
HE	0704	1879	0.6977

TABLE 2: Values obtained from trained network for RSA cipher

CONCLUSION AND FUTURE WORK

A neural network-based cryptography technique has been implemented to study encryption and decryption techniques. Accuracy is enhanced by proper selection of network topology and parameters in the training algorithm. Related model has been simulated for various example problems. Finally, the accuracy has been demonstrated in form of Tables.

The future work that may be done in this regard includes:

1) Minimisation of the error function by improved methods

2) Implementation of better training algorithms and network architectures

3) Increasing the efficiency of training for the generalised cryptosystems.

REFERENCES

[1] Jacek M. Zurada, Introduction to Artificial Neural Systems, West Publishing Company, St. Paul, 1992.

[2] Thomas Koshy, Elementary Number Theory with Applications, Elsevier, a division of Reed Elsevier India Private Limited, Noida, 2009.

[3] I. Kanter and W.Kinzel, "The Theory of Neural Networks and Cryptography," Quantum Computers and Computing, vol. 5, pp. 130-139, 2005.

[4] E.C.Laskari, G.C.Meletiou, D.K.Tasoulis, M.N.Vrahatis, "Studying the performance of artificial neural network networks on problems related to cryptography," Non linear Analysis: Real World Applications, vol.7, pp. 937-942, 2006.

[5] G.C.Meletiou, D.K.Tasoulis, M.N.Vrahatis, "A first study of the neural network approach in the RSA cryptography," in Sixth IASTED

International Conference on Artificial Intelligence and Soft Computing (ASC 2002), Banff, Alberta, Canada, July 17-19, 2002.
[6] [Online]. Available: http://www.wikipedia.org/.
[7] "Mathworks," The Mathworks, Inc., [Online]. Available: http://in.mathworks.com/help/nnet/ref/trainlm.html;jsessionid=a15fe82129a83dc8a92470543e5c.