International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-2, Issue-9, September 2016
ISSN: 2395-3470
www.ijseas.com

Authentication based two level Encryption & Decryption of an Image using Artificial Neural Network.

Mahesha NB
Senior Lecturer
Rai technology University, Bangalore.

Abstract

Due to advanced research in multimedia application ,huge amount of digital data is being exchanged over unsecured channels. Either it is confidential or private, need for security mechanisms to provide required protection.

presented work aims at secure image transmission and reception by doing two level encryption to original image, by adding additional impurities to make decryption difficult to cryptanalyst also gives authenticity of user in additional to extra security level , decryption of an image can be done by using Artificial Neural Networks(ANN) with Multi layer Feed Forward (MLFF) architecture, it eliminates the need for key exchange prior to data exchange ,also provide high security ,ability to work with non linear data &Faster training has been achieved by using the ‘ trainlm ’ function of MATLAB neural network tool kit & finds an application in medical imaging system , military image communication and confidential video conferencing ,also it can be implement in future in water marking of an image and video application.

Keywords:-Artificial neural networks, Multilayer feed forward ,Encryption ,Decryption ,cipher ,Back propagation algorithm ,.Advanced Encryption Standard Data Encryption Standard.

1. INTRODUCTION

Cryptography is the technique that can be used for secure transmission of data, This technique will make the information to be transmitted into an unreadable form by encryption so that only authorized persons can correctly recover the information. Even though so many of encryption & decryption methods are invited it is getting difficult to protect the confidential data misusing from unauthorized peoples, In order to address this issue, from past AES,DES,RSA ,different mechanisms are proposed in recent years Mirror-like image encryption algorithm ,Signature misuse detection, chaotic based neural network encryption, Digital Image Encryption Algorithm Based Composition of Two Chaotic Logistic Maps, has invited these are all good mechanisms but for nonlinear input data it doesn't work well, also even though all of methods are strong still cryptanalyst able to obtain the original data by tracing key.

ANN plays a very important role in information security Eliminates need for the key exchange, In the presented work ,in addition to security authenticity of user provided ,two level encryption creating more confusion and misguides the cryptanalyst to obtain the cipher. At the receiving end, it uses ANN with multi layer feed forward architecture to obtain the original image. The elimination of the key exchange and the usage of artificial neural network for high level security are the major strengths of the presented work ,shown in flow chart fig 2.

2. Artificial Neural Networks (ANN)

ANN are simplified models of the biological nervous system, which has a natural propensity for storing experimental knowledge and making it available for later use, Shown in fig 1.

An ANN provides a general, practical method for learning real, discrete, and vector-valued functions from examples. Each neuron is connected to other neurons by means of directed communication links called its activation level ,Typically, a

International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-2, Issue-9, September 2016
ISSN: 2395-3470
www.ijseas.com

neuron sends its activation as a signal to several other neurons.

2.1 Training the ANN

Training the neural network is to for produce the correct outputs for the given inputs is an iterative process, compare the output on this actual output with the desired output and Adjust the weights in the network to generate better output the next time it involves in 2 steps: Feed forward Phase,back propagation method.

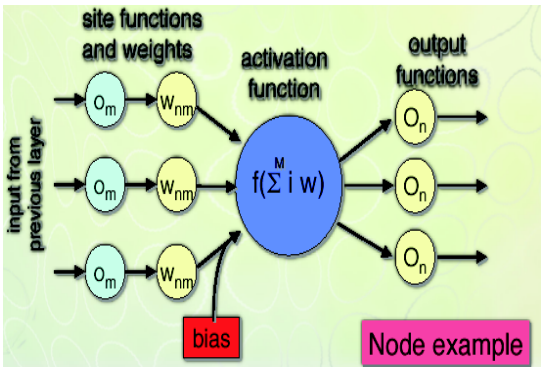


Fig 1. ANN Node Example.

Om: output from previous unit.

W: weight applied to om,

Bias additional weight applied to select

Inputs or layers, Responses are then fed to an activation function ,formula is,

$$a_{j(t+1)} = \frac{1}{1+e^{-(\sum_i w_{ij}\ o_{i(t)} - \theta j)}}$$

2.2 The back propagation neural network

one layer networks are seriously limited in their capabilities. Hence MLFF networks with Back propagation learning and non linear node functions are used These elements or nodes are arranged into different layers: input, middle and output. The output from one node feed forward to next node, using a procedure known as the forward pass ,this method shown in below 3 steps.

- **The input layer propagates a particular input vector's components to each node in the middle layer.**
- **Middle layer nodes compute output values, which become inputs to the nodes of the output layer.**
- **The output layer nodes compute the network output for the particular input vector.**

3. SYSTEM DESIGN

System designed can be split into four modules- Authentication, encryption, decryption and Interface. MATLAB GUI provides interface from sender to receiver

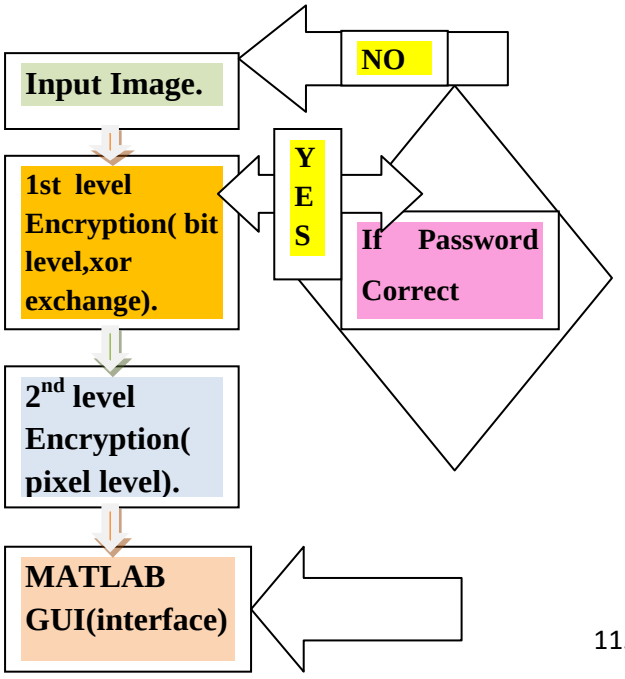
using Remoting system ,Shown In Flowchart fig 2.

RECEIVER

3.1 Encryption Module

After confirm with correct password of the user ,The image to be encrypted is read pixel by pixel , Divide the pixel byte value into 4 nibbles(for 8 bits it divide into 4,in each nibbles 2 bits)then Exchange the nibbles and concatenate to form a byte, Calculate the impurity by EX-ORing the original nibbles ,shift the bits of impurities by 5 bits to right. Now we get 9 bit number, EX-OR the results, Add impurity to the obtained result in Impurity Value chosen any randomly like 220.next apply to 2nd level encryption.

SENDER



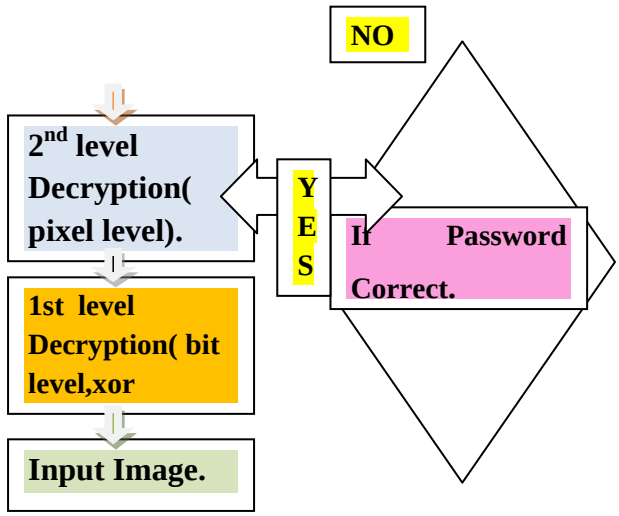


Fig. 2 Flow Chart of System Design.

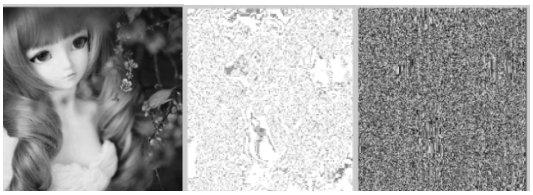


Fig 3 Sample Result of 2 level Encryption.

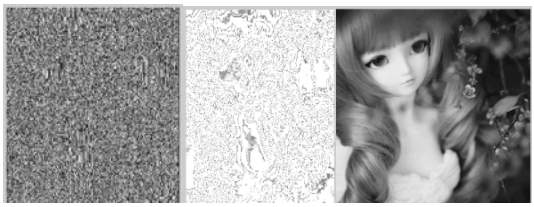


Fig 4 Sample Result of 2 level Decryption.

a) Second level encryption: In this step we are calculating normalization After that Add another level of impurity to the resultant matrix obtained in after adding 720(randomly taken num) such that impurity

changes with respect to the position of the pixel ,shown in fig 3

3.2 Decryption

Mat lab GUI Remoting system provide interface from sender to receiver**,** At the receiver end decryption is achieved using an ANN with MLFF & Back propagation. Using hidden layers it derive the relation & decrypts the original image data.

The decryption is achieved in 3 steps.1) password can be added by receiver then the impurity which was varying with respect to position of pixel is removed.2) the additional columns from the matrix which were added during the encryption is deleted. 3)the received image data and weights which were stored after the training are used to stimulate the network. The output of this stage is the recovered image ,shown in fig 4.

4. Two level of Encryption

1st level of encryption image can be still visible Shown in fig 5.

To overcome this problem 2nd level of encryption is used. Here the impurity changes with respect to the pixel position it means pixel with same original value will have two different values after the second level of encryption depending on the pixel position. The output after 2nd level of encryption is as shown in Fig 6.

Fig 5 I/O of 1st level Encryption.

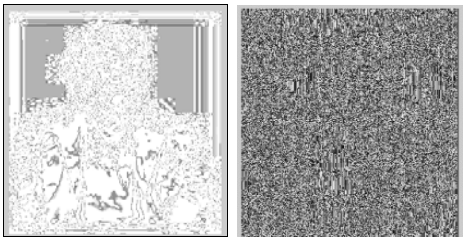


Fig 6 output of 2nd level encryption.

5. Performance Analysis

5.1 Normalization:-

ANNs require training before they are used for any application. The results of training were not converging for the given input data set having 256 values. This problem was solved by the normalization of the input data. Normalization is the process of transforming the data set to the values ranging from -1 to 1,in this work it can be done by adding two coloumns.formula is

$$Normalized\ (e_i) = \frac{e_i - E_{min}}{E_{max} - E_{min}}$$

where

E_{min} = the minimum value for variable E.

E_{max} = the maximum value for variable E.

If E_{max} is equal to E_{min} then Normalized (e_i) is set to 0.5.

CONCLUSION

The presented work helps to give secure image transmission while sending confidential info on network media using two level encryption & authentication of user Provided in addition to extra level of security, also eliminate the need of key exchange, neural network helps to secure image reception, also work with non linear input and output, gives higher accuracy of an image with less time & lower the error rate in output data. The present work thus provides a means of robust, flexible, accurate and secure image data transmission and reception, we can find real time application in medical, military, banking system, also there is a lot of scope in water marking and video field, in biometrics.

References:-

1. J.Park,I.W. Sandberg, Universal Approximation Using Radial Basis Function Networks, Neural Computation, Cilt 3, 246- 257, 1991.
2. William Stallings," network security essentials ,applications & standards".
3. StewanW.Smit," Scientist and Engineers Guide to Digital Image processing", Second Edition, (1999).
4. Chang-Mok Shin, Dong-Hoan Seo, Kyu-Bo Chol, Ha-Wmn Lee, and Smng Kim, — Multilevel Image Encryption by Binary Phase XOR Operations , IEEE Proceeding in the year 2003.
5. Semi-Fragile JPEG Image Authentication Scheme Based on Discrete Cosine Transform".

6. Qais H. Alsafasfeh , Aouda A.Arfoa, Image Encryption Based on the General Approach for Multiple Chaotic Systems Journal of Signal and Information Processing, 2011.
7. S.R Dorling and M.W Gardner, ANN (the multilayer perceptron) —a review of applications in the atmospheric sciences. Volume 32, Issues 14–15, 1 August 1998, Pages 2627–2636.
8. http://en.wikipedia.org/wiki/Authenticated_encryption.
9. http://en.wikipedia.org/wiki/Encryption.
10. www.mathworks.com.