

Technique for Security of Multimedia using Neural Network

Shyam Nandan Kumar¹

¹M.Tech. Scholar, Computer Science and Engineering, LNCT, Indore, MP, India, shyamnandan.mec@gmail.com

Abstract

With the increased popularity of multimedia applications, there is a great demand for secured data storage and transmission techniques. Security is a prevalent concern in information and data systems of all types. In order to satisfy secure multimedia data transmission between sender and receiver, this paper proposes technique for Security of Multimedia using Neural Network. Since the encryption process is one way function, the artificial neural networks are best suited for this purpose as they possess features like high security, no distortion and its ability to perform for nonlinear input-output characteristics. To protect from attack, the paper introduces a Model for Cryptosystem Using Neural Network, which is of high security and low cost. Based on this model separate Encryption and Decryption Algorithm is presented. Also Training Algorithm for Multi-layered Neural Network is provided to hold secure multimedia data. The proposed work finds its application in medical imaging systems, military image database communication and confidential video conferencing, and similar such application. The results are obtained through the use of MATLAB 7.0.1.

Keywords: Security, Multimedia, Encryption, Decryption, Neural Network.

1. INTRODUCTION

In today's advanced and technology adapted society, the concept of multimedia is ever present in many facets of life. Multimedia information applications such as mobile TV, online chatting, digital library, video-conference etc. [1][2] became more and more popular in human being's life. Generally, a multimedia communication system enables the generation, management, communication and consuming of multimedia data such as texts, images, audios, videos, animations, etc. Multimedia may be broadly divided into linear and non-linear categories. Linear active content progresses often without any navigational control for the viewer such as a cinema presentation. Non-linear uses interactivity to control progress as with a video game or self-paced computer based training. Hypermedia is an example of non-linear content. Multimedia presentations can be live or recorded. A recorded presentation may allow interactivity via a navigation system. A live multimedia presentation may allow interactivity via an interaction with the presenter or performer [3].

Security protection is an important issue for multimedia information systems [2], which aims to protect the multimedia content, service interaction and user privacy, etc. For example, the content related to commercial secret needs to be protected against unauthorized users, the payment interactions between the user and the seller are sensitive to the third party, and the user profiles are private and should not be published. Neural network [4] and cryptography [5] together can make a great help in field of networks security. The key formed by neural network is in the form of weights and neuronal functions which is difficult to break. Here, content data would be used as an input data for cryptography so that data become unreadable for attackers and remains secure from them. The ideas of mutual learning, self-learning, and stochastic behavior of neural networks and similar algorithms can be used for different aspects of cryptography, like public-key cryptography, solving the key distribution problem using neural network mutual synchronization, hashing or generation of pseudo-random numbers. Another idea is the ability of a neural network to separate space in non-linear pieces using "bias". It gives different probabilities of activating or not the neural network. This is very useful in the case of Cryptanalysis.

Encryption is the conversion of data into a form, called a cipher text, which cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood. The aim of this research is to build a ciphering technique by using artificial neural network to protect data against unauthorized access to the data being transferred.

In this paper sections are organized as follows: Section 2 describes Neural Network concepts. Section 3 reviews some related works. Section 4 describes proposed technique. In section 5 an analysis of proposed technique is presented. Section 6 concludes the paper and presents avenues for future work. References for this paper are given in section 7.

2. NEURAL NETWORK

An Artificial Neural Network [6] is a massively connected structure of Artificial Neurons that has a natural tendency for strong experiential knowledge and making it available
for use. Neural Networks are Data Dependent and are suited for non linear applications. Each neuron is connected to other neurons by means of directed communication links each with an associated weight. Each neuron has an internal state, called its activation or activity level, which is a function of the inputs it has received. Typically, a neuron sends its activation as a signal to several other neurons. A simple Artificial Neuron is as shown in Fig. 1. Basic computational unit is called as a neuron. It receives the inputs $X_1$, $X_2$, $X_3$, .........., $X_n$, which are associated with weights $W_1$, $W_2$, $W_3$, ..........., $W_n$. This unit computes:

$$Y_i = f(\Sigma_i(W_jX_j))$$

Where, $W_j$ refers to the weights from unit j to unit i and function is unit’s activation function.

$$f(t) = \frac{1}{1+e^{-t}}$$

Where, $-\infty < t < \infty$.

Back propagation network is one of the most complex neural networks for supervised learning. Regarding topology, the network belongs to a multilayer feed forward neural network as shown in Fig. 2. Architectures of this class, besides possessing an input and an output layer also have one or more intermediary layers called hidden layers. Here the neurons of one layer are connected to the neurons of the next layer and so on till the output layer. The hidden layer aids in performing useful intermediary computations before directing the input to the output layer [7]. However, there are no connections between neurons of the same layer. Back propagation neural networks are those feed forward networks which use back propagation learning method for their training. Back propagation algorithm usually uses a logistic sigmoid activation function as follows:

$$f(t) = \frac{1}{1+e^{-t}}$$

An epoch is one cycle through the entire set of training vectors. Typically, many epochs are required for training a Back propagation Neural Network.

### 2.1 Neural Network’s Properties Suitable for Multimedia Content Protection

#### 2.1.1 One-way Property:
One-way property means that it is easy to compute the output from the input while difficult to access the input from the output. In Neural Network n different inputs produce single output as shown in Fig. 1. So it is not easy to decrypt the code by unauthorized person.

#### 2.1.2 Learning Ability:
Neural network has the possibility of learning. Given a specific task to solve and a class of functions, neural network can use a set of observations to solve the task in an optimal sense. Generally, according to the learning task, neural network's learning ability can be classified into three categories, i.e., supervised learning, unsupervised learning and reinforcement learning [8][9][10]. Supervised learning is the learning with a "teacher" in the form of a function that provides continuous feedback on the quality of solutions. These tasks include pattern classification, function approximation and speech or gesture recognition, etc. Unsupervised learning refers to the learning with old knowledge as the prediction reference. These tasks include estimation problem, clustering, compression or filtering. Reinforcement learning refers to the learning with dynamic estimation and decision. These tasks include control tasks, games and other decision making tasks. This property can be used to detect the intruders that enter a secret system without permission.
2.1.3 Random Outcomes: According to the complex relation between the nodes of neural network, neural network can produce the sequences with random properties.

Based on the one-way property and learning ability of neural network, the multimedia content authentication scheme based on neural network is presented in section 4.

3. RELATED WORK

Many security issues in the multimedia have been identified and demonstrated in many studies. Due to limited of resources, researchers face challenge to create or define a suitable technique for optimal security. Previously proposed methods focused on individual data encryption but failed to solve complex multimedia data with low cost, noise free data, file format integrity. While a very few attempts focused on achieving these majors concepts together fairly.

The study of Shiguo Lian, Jinshe Sun, Zhongxin Li and Zhiquan Wang [11] suggests Fast MPEG4 Video Encryption Scheme Based on Chaotic Neural Network. This scheme encrypts video object layers (VOLs) selectively. That is, the motion vectors, subbands, code blocks or bit-planes are encrypted partially. A stream cipher based on chaotic neural network is used in all these encryption processes, which is of high security and low cost.

Ismail I.A, Galal-Edeen, Khattab S and El Bahtity [12] proposed Satellite image encryption using neural networks backpropagation. The central contribution is using fixed, arbitrary keys in the training process as in classical symmetric and asymmetric cryptography. The used network is of NaMxN neurons representing the input, hidden, and output layers, respectively. The network is trained by adjusting the weights while the bias is given a constant value between 0 and 1 after normalizing the values.

A color image encryption method [13] is proposed with the removal of noise generated during the transmission based on Cohen-Grossberg neural networks, where the color image is expressed in terms of the standard red-green-blue (RGB) space, and the corresponding pixel matrix is hidden by Arnold transform (AT). The Cohen-Grossberg neural network is added to store the hidden message as the stable equilibria, which achieves the noise removal. The hidden message without noise is recovered by performing AT with accurate iteration numbers.

Damageless image hashing using neural network [14] is proposed by Naoe K and Takefuji Y. It uses a new key generation model for image hashing using neural network, which does not embed any data into the content but is able to extract meaningful data from target image. This model trains artificial neural network to assign predefined code and uses this trained artificial neural network weight and the coordinates of the selected feature sub blocks of target image as keys to extract the predefined code. In this model, the observed output signal from the trained neural network is used as image hash value which distinguishes the target image from other images.

Most business networks protect sensitive data and systems by attempting to disallow external access. Enabling wireless connectivity reduces security if the network uses inadequate or no encryption. In order to choose secure communication with multimedia data, in the paper, inspired by above related work, we propose a secure cryptosystem technique for multimedia data based on neural network.

4. THE PROPOSED TECHNIQUE

Based on the one-way property and learning ability of neural network, the multimedia content authentication scheme is presented. Firstly, this chapter introduces Model for Cryptosystem using Neural Network. Secondly, the chapter gives an introduction to neural network training algorithm based on protection of multimedia data. Thirdly, an image or video authentication scheme (Encryption/Decryption Method) based on neural networks is presented.

Model for Cryptosystem using Neural Network is shown in Fig. 3. System model can be split into two modules-Encryption and Decryption. Whenever the sender wishes to send video, he feeds the video file to be sent to the encryption module. The video file is encrypted in the encryption module using neural network. The ciphers are constructed based on the random sequences generated from the neural networks. At the receiving end the user in the remote system decrypts the video data by feeding the received data to the decryption module using artificial neural networks.

Here, the media data, original authentication code and key are used to feed a neural network, which produces a secret parameter. Compared with media data, the secret parameter is of small size. Then, the secret parameter and the key are stored or transmitted in a secure way, while the media data are distributed freely. During distribution, media data may be tampered maliciously. In authentication, the received media data, secret parameter and key are used to feed the same neural network, which produces the computed authentication code. By comparing the original authentication code and the computed one, the authentication result is produced. That is, if there is only slight difference between them, then the multimedia data are not tampered, otherwise, they are tampered. To authenticate multimedia data successfully, two conditions are required. Firstly, the secret parameter and key are correct. Secondly, the received media data are same to or not very different from the original media data.

Media data are partitioned into blocks, and each bit of the authentication code corresponds to a block and a simple
neuron. For each simple neuron, a code bit s (s=0 or 1) and the media block composed of n pixels act as the input and control parameter. The pixels of a media block are normalized into the pixels $X_{0i}, X_{1i}, \ldots, X_{ni}$ ranging in [-1,1] by subtracting the mean and dividing them a ximal amplitude. To compute the secret parameter, the neuron layer is fed by the parameters $X_{0i}, X_{1i}, \ldots, X_{ni}$ and $W_{0w}, W_{1w}, \ldots, W_{nw}$ as shown in Fig. 1 and Fig. 2. The random sequence $W_{0w}, W_{1w}, \ldots, W_{nw}$ is generated by a random number generator with K as the random seed.

![Fig-3: Model for Cryptosystem Using Neural Network](image)

**4.1 Algorithm for training the Neural Network**

The training of a network by back propagation involves three stages: the feed forward of the input training pattern, the calculation and back propagation of the associated error, and the adjustment of the weights. Once the process converges, the final weights are stored in a file. After training, application of the network involves only the computations of the feed forward phase. As shown in Fig. 2. During feed forward, each input unit ($X_i$) receives an input signal and broadcasts this signal to each of the hidden units $Z_i, Z_1, \ldots, Z_n$ through the $w$ weights. Each hidden unit then computes its activation and results in its signal $Z_i = f(Z_i^*)$ to each output unit through the $v$ weights. Each output unit ($Y_k$) computes its activation ($Y_k^*$) to form the response of the net for the given input pattern. During training, each output unit compares its computed activation $Y_k^*$ with its target value $T_k$ to determine the associated error for that pattern with that unit. Based on this error, the factor $\delta_k$ is computed, $\delta_k$ is used to distribute the error at output unit $Y_k$ back to all units in the hidden layer. It is also used (later) to update the weights between the output and the hidden layer. The foregoing algorithm updates the weights after each training pattern is presented.

**Algorithm:**

1. $v_{ij} = p; w_{ij} = q; \{(p<100, q<100, i>0, j>0) // Initialize weights with random small value.
2. for(i=1; i<n; i++) // n is total number of input unit in input layer
3. {
4. $X_i = x_i; //Each input unit X_i has input signal x_i$
5. }
6. //Now $x_i$ is broadcasted to all unit in hidden layer
7. for((i=1; j<n; j++)
8. {
9. $Z_j^* = v_0 + \sum_{i=1}^{n} x_i \cdot v_{ij}; // Calculation at hidden layer$
10. $Z_i = f(Z_i^*); // Activation function is used to calculate the output signal of hidden layer$
11. }
12. // Now output signal is sent to all units in the output layer.
13. for(k=1; k<n; k++)
14. {
15. $Y_k^* = w_{ik} + \sum_{j=1}^{n} Z_j^* \cdot w_{jk}; // Calculation at Output layer.$
16. $Y_k = f(Y_k^*); // Activation function is used to calculate output signal of output layer.$
17. }
18. // If target output $T_k$ is not achieved, calculate the error $\delta_k$ during training
19. for(k=1; k<n; k++)
20. {
21. $\delta_k = (T_k - Y_k) f'(Y_k^*);$
22. $\Delta w_{jk} = \alpha \delta_k Z_j; // Weight Correction$
23. $\Delta w = \alpha \delta_k; // Bias Correction$
24. }
25. // Now $\delta_k$ is sent back to hidden layer for recalculation.
26. for(j=1; j<n; j++)
27. {
28. $\delta_j^* = w_{0j} + \sum_{k=1}^{n} k \cdot w_{jk};$
29. $\delta_i = \delta_j^* f(Z_j^*);$  
30. $\Delta v_{ij} = \alpha \delta_i x_i;$
31. $\Delta v_{0j} = \alpha \delta_j;$
32. }
33. // Now Each Output Unit updates its bias and weights
34. for(k=1; k<n; k++)
35. {
36. for(j=1; j<n; j++)
37. {
38. $w_{jk}(new) = w_{jk}(old) + \Delta w_{jk};$
39. }
40. }
41. for(j=0; j<n; j++)
42. 
43. for(i=0; i<n; i++)
44. {
45. \( v_{ij}(\text{new}) = v_{ij}(\text{old}) + \Delta v_{ij}; \)
46. }
47. }

The learning rate(\(\alpha\)) is taken equal to 0.01, and the momentum constant is taken equal to 0.9 [15]. Momentum is a standard technique that is used to speedup convergence and maintain generalization performance [16]. An epoch is one cycle through the entire set of training vectors. Typically, many epochs are required for training a back propagation neural network.

### 4.2 Encryption and Decryption Algorithm

One means of providing security in communications is through encryption. The ciphers are constructed based on the random sequences generated from the neural networks. By encryption, data are transformed to unrecognizable data. This data can be recovered only by decryption. The idea of encryption and decryption processes is by splitting the testing algorithm used in NN into two parts. The first part is used for encrypting data, by sending the input vector to the hidden layer. The second part was used for decrypting data by sending the encrypted vector to the output layer. The algorithm of encryption and decryption are:

**Encryption Algorithm:**

1. \( v_i = p; w_{ij} = q; (p<100, q<100, i>0, j>0) \) // Initialize weights with random small value.
2. for(i=0; i<n; i++)
3. Set activation of input unit \( x_i \)
4. for(j=1; j<n; j++)
5. {
6. \( Z_j^* = v_{0j} + \sum_{l=1}^{n} x_l \cdot v_{lj}; \) // Encryption at hidden layer
7. \( Z_j = \frac{1}{1 + e^{-2Z_j^*}} - 1; \)
8. }

**Decryption Algorithm:**

1. for(k=1; k<n; k++)
2. {
3. \( Y_k^* = (w_{0k} + \sum_{j=1}^{n} z_j \cdot w_{jk}); \) // Decryption at output layer
4. \( Y_k = Y_k^*; \)
5. }

The final weights must be known after training. Then it will be divided into two portions. The first portion is from input layer to hidden layer for encryption side, and then the encrypted data are obtained from the output layer after launching the output layer with the hidden data vector. The second portion is from hidden layer to output layer for decryption side, and then the decrypted data are obtained from the output layer after launching the output layer with the hidden data vector.

The suggested Cryptosystem can efficiently ciphering different types of Multimedia data. See Fig. 4, Fig. 5 and Fig. 6 for signal before and after encryption process, and signal after decryption process. Text encryption can encrypt any type of string symbol such as: characters, numbers, arithmetic symbols, etc.

![Fig-4: Signal before Encryption.](image)

![Fig-5: Signal after Encryption](image)
5. ANALYSIS OF PROPOSED TECHNIQUE

5.1 Security Analysis
In the proposed technique, the authentication code is computed under the control of the key and the secret parameter. Without them, it is difficult to compute the authentication code correctly. The authentication code can be computed correctly when media data are not changed during transmission or distribution. The proposed scheme is robust to some operations applied to the media data, such as adding noise or recompression. The performance depends on two parameters, i.e., the adjustable parameter and the block size.

Based on the one-way property and learning ability of neural network, it is not easy to decrypt the multimedia data by unauthorized person.

5.2 Network Performance: The training of the neural network is based on dynamic and fast algorithm. Due to this, the proposed techniques, handle the data quickly. It also reduces the overload on the network by active and fast operation of encryption and decryption.

5.3 Data Integrity: File format of content are not changed. Data are fully secure and pure.

6. CONCLUSION AND FUTURE WORK
Multimedia has wide popularity. As multimedia applications are used increasingly, security becomes an important issue. In this paper, by investigating neural networks’ properties, the low-cost authentication method based on neural networks is proposed and used to authenticate images or videos. Encrypted data are highly secure due to one-way property and learning properties of neural network. Crypto system also keeps the file format unchanged. The accuracy of the system has been found very high. These properties make it suitable for real-time applications, such as video-on-demand system, video-conference system, mobile or wireless multimedia, and so on.

In the future, we can work on Big Multimedia data handling technique.

7. REFERENCES
[7]. Khalil Shihab,”a back propagation neural network for computer network security”


