Image/Data Encryption-Decryption using Neural Network

Shweta R. Bhamarea, Dr. S.D.Sawarkarb

aDepartment of Computer Engineering, PG Student, Datta Meghe COE, Airoli
bPrincipal, Datta Meghe COE, Airoli

Abstract

Today, the encryption and decryption of data/image has reached to new heights of security. Inclusion of Neural Network has given a vast scope for this technology. Neural network includes training the network by using algorithms like backpropagation, feedforward, RBF etc. This paper uses backpropagation technique with the use of ‘trainlm’ function in MATLAB. The system designed can be split into four modules encryption, decryption, interface module, and the authentication module. Whenever the sender wishes to send an image, he feeds the image to be sent to the encryption module. The image data is encrypted in the encryption module and the encrypted data is fed to the interface module. This module transfers the encrypted image data to the remote system. At the receiving end the user in the remote system decrypts the image data by feeding the received data to the decryption module. Decryption is done using Artificial Neural network. This requires training of the network. In Biometric case authentication is provided using fingerprint recognition method of biometric authentication and using RMI for image. All the above four modules have to be present in every user’s system who wish to use of secured image transmission and reception facility.

Keywords: Encryption, decryption, Neural network, authentication.

1. Introduction

Neural network has been attracting more and more researchers since the past decades. The properties, such as parameter sensitivity, random similarity, learning ability, etc., make it suitable for information protection, such as data encryption, data authentication, intrusion detection, etc. Here, by investigating neural networks’ properties, the low-cost authentication method based on neural networks is proposed and used to authenticate images or videos. The authentication method can detect whether the images or videos are modified maliciously. Firstly, this work introduces neural networks' properties[9], such as parameter sensitivity, random similarity, diffusion property, confusion property, one-way property, etc. Secondly, it gives an introduction to neural network based protection methods. Thirdly, an image or video authentication scheme based on neural networks is presented, and its performances, including security, robustness and efficiency, are analyzed.

2. Neural Network Properties

- Learning Ability
- One-way Property
- Random Similarity
- Parameter Sensitivity

2.1 Content Protection Based on Neural Networks

2.1.1 Data Authentication

The one-way property makes neural network a suitable choice for hash function. Hash function is a technique for data integrity authentication[8], which takes a message of arbitrary length as input and produces an output of fixed length. The hash value is often much shorter than the message, which makes it suitable for digital signature or data authentication. As a hash function, it should be easy to compute the hash value from the message, while difficult to compute the message from the hash value. This property is called one-way property. According to this case, neural network may be used to design hash function. Till now, some hash functions based on neural network have been presented[26], which were reported to have some advantages compared with existing schemes, such as high time-efficiency or flexible extension.

For example, a hash function based on multi-layer neural network is presented [21], as shown in Figure which produces the hash value with the message as input.

*Corresponding author.
E-mail address: shwetabhamare@gmail.com
2.1.3 Data Encryption

According to the properties of random similarity and parameter sensitivity, neural network has been used in data encryption. Data encryption is the technology that converts a message into unintelligible form under the control of the key. Till now, two kinds of encryption algorithms have been reported, i.e., stream cipher [18] and block cipher [18]. Stream cipher uses neural network to generate a pseudorandom sequence that modulates a message and uses the parameter as the key. The general architecture is shown in Figure.

For example, the ciphers are constructed based on the random sequences generated from the neural networks. As a combination of neural networks and chaos, chaotic neural networks (CNN)[11] are used in secret communication. Chan et al took advantage of Hopfield neural networks’ chaotic property to produce pseudo-random sequence that is used to encrypt messages. Karras et al. proposed the method to evaluate the property of the pseudorandom sequence generated from chaotic neural networks[21], and Caponetto designed a secure communication scheme based on cell neural networks. Block cipher makes use of neural networks’ properties to encrypt a message block by block. In this cipher, the initial value or control parameter acts as the key. For example, Yue et al. constructed the image encryption algorithm based on chaotic neural networks, Yen et al. used perception neurons[23] to construct a block cipher, Lian et al. proposed an image cipher based on chaotic neural network, and Yee et al. designed a symmetric block cipher based on the multi-layer perception network.

2.2 Need of Artificial Neural Networks

ANNs provide exciting alternatives, and many applications could benefit from using them. These include massive parallelism, distributed representation and computation, learning ability[17], generalization ability, adaptivity, inherent contextual information processing, fault tolerance, and low energy consumption.

ANN models attempt to use some “organizational” principles believed to be used in the human brain. Modeling a biological nervous system using ANN can also increase our understanding of biological functions. State-of-the-art computer hardware technology (such as VLSI and optical) has made this modeling feasible.[16]

2.3 ANN Overview

2.3.1 Network architectures

ANN’s can be viewed as weighted directed graphs in which artificial neurons are nodes and directed edges (with weights) are connections between neuron outputs and neuron inputs. Based on the connection pattern (architecture), ANN’s can be grouped into two categories
1) feed-forward networks, in which graphs have no loops, and[7]
2) recurrent (or feedback) networks, in which loops occur because of feedback connections.

2.3.2 Learning

The ability to learn is a fundamental trait of intelligence. Although a precise definition of learning is difficult to formulate, a learning process in the ANN context can be viewed as the problem of updating network architecture[13] and connection weights.
so that a network can efficiently perform a specific task. The network usually must learn the connection weights from available training patterns. Performance is improved over time by iteratively updating the weights in the network. ANNs' ability to automatically learn from examples makes them attractive and exciting. Instead of following a set of rules specified by human experts, ANNs appear to learn underlying rules (like input-output relationships) from the given collection of representative examples. This is one of the major advantages of neural networks[23] over traditional expert systems.

2.3.3 Image Encryption using Pixel shuffling

The advent of wireless communications, both inside and outside the home-office environment has led to an increased demand for effective encryption systems. The beauty of encryption technology comes out in more pronounced way when there is no absolute relation between cipher and original data and it is possible to rebuild the original image in much easier way. As chaotic systems[10] are known to be more random and non-predictable, they can be made utilized in achieving the encryption. The transposition technology of encryption systems requires scrambleness behaviour in order to achieve the encryption of the data. This scrambleness behaviour can be derived from the randomness property[15] of chaos which can be better utilized in the techniques like transposition system. In this paper we present a chaos based encryption algorithm for images. Here, the position of the data is scrambled in the order of randomness of the elements obtained from the chaotic map and again rearranged back to their original position in decryption process. The same algorithm is tested with two different maps and performance analysis is done to select best suited map for encryption.

2.3.4 Experimental Analysis

Here, image taken to test the algorithm is Lena image (225×225×3). Figure 3 a, b and c show the original image, pixel scrambled encrypted image and decrypted image with their RGB-levels[12].

![Figure 3 (a): Lena image and RGB intensity plots](image)

![Figure 3 (b): Encrypted image and RGB intensity plots after encryption](image)

![Figure 3 (c): decrypted image and RGB intensity plots after decryption](image)

2.3.5 Performance Analysis
To measure the performance of the encryption algorithm, if correlation coefficient is nearer to zero for an encrypted image, then algorithm is said to be better. To prove that decryption is possible only with one key, key sensitivity is calculated.

3. Related Work

Information security is very important task in the field of information and communication technology. Encryption is one way to secure information. Here, combined concept of pixel and position manipulation technique for image encryption is presented. The proposed technique involves three stages. In first stage pixel position manipulation is done by using pixel shuffling block where index value of each row is rearranged in bit-reversed order so that the positions of rows are manipulated. Similarly index value of each column is rearranged in bit-reversed order, which leads to manipulation of columns. This position manipulated image is used as input to the pixel manipulation block in second stage, where each pixel is rearranged in reverse order. In third stage, this scrambled image is again undergone pixel value manipulation by using bit-rotation concept leading to encrypted image. This proposed combined concept is implemented for different images using MATLAB. Decryption involves the reverse process of encryption.

In this fast-growing digital world there is a huge demand for information security. There are several areas which needs information security like, military application, medical information transmission during telemedicine, video conferencing, video on demand, and image database management system for satellite images and so on. There are several image encryption techniques with its own advantages and disadvantages. In general image encryption can be classified in two ways, fist one is image encryption by pixel manipulation and second is image encryption using pixel-position manipulation. In case of pixel manipulation technique, weight of a pixel is altered which leads to image encryption. Similarly in case of pixel-position manipulation technique, position of each pixel is changed by rearranging the pixel is pre-defined patterns.

4. Proposed Approach for the system

The system designed can be split into four modules encryption, decryption, interface module, and the authentication module. Whenever the sender wishes to send an image, he feeds the image to be sent to the encryption module. The image data is encrypted in the encryption module and the encrypted data is fed to the interface module. This module transfers the encrypted image data to the remote system. At the receiving end the user in the remote system decrypts the image data by feeding the received data to the decryption module. Encryption and decryption module are implemented using MATLAB 7.0.1. Authentication is provided using fingerprint recognition method of biometric authentication. All the above four modules have to be present in every user’s system who wish to use of secured image transmission and reception facility.

4.1 Modules of the proposed system
4.1.1 Encryption module
The image to be encrypted is read pixel by pixel and the transformation is done on these pixels using permutation, substitution and impurity addition. Two levels of encryption are used to obtain high level of image encryption[11]. Algorithm shows the necessary transformation:

**Algorithm:**

**First level of encryption (steps 1 to 8):**

1. Get the pixel value of the image file [01000011]
2. Divide the pixel byte value in two parts(nibbles) [0100] & [0011]
3. Exchange the nibbles and concatenate to form a byte [00110100]
4. Calculate the impurity by EX-OR ing the original ms nibble and ls nibble [0111]
5. Shift the bits of the impurity by 5 bits to the right. Now, we get 9 bit number [011100000]
6. EX-OR the result of step3 and step5. [011010100]=[212].
7. Add impurity to the obtained result in step 6. Impurity value chosen is 117, [212+117=329].
8. Continue step1 to step7 for all the pixels of the image file.

**Addition of two columns:**

9. Additional two columns are added and value of 117 is added to the first new column and 627 is added to the second new column. This is required for the normalization of the matrix.

**Second level encryption:**

10. Add another level of impurity to the resultant matrix obtained in step9 such that the impurity changes with respect to the position of the pixel.

Table 2 shows the transformation of sample pixel values after First Level of Encryption

<table>
<thead>
<tr>
<th>Original Pixel Value</th>
<th>Pixel Value after 1st level Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>165</td>
</tr>
<tr>
<td>6</td>
<td>277</td>
</tr>
<tr>
<td>45</td>
<td>473</td>
</tr>
<tr>
<td>67</td>
<td>329</td>
</tr>
</tbody>
</table>

Table 2: Sample First Level Encryption Results

Table 3 shows how the pixel value (12) changes with respect to its position during the Second Level of Encryption.

<table>
<thead>
<tr>
<th>Pixel Position</th>
<th>Original Pixel Value</th>
<th>Pixel Value after 1st level Encryption</th>
<th>Pixel Value after 2nd level Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1,1)</td>
<td>12</td>
<td>437</td>
<td>537</td>
</tr>
<tr>
<td>(4,68)</td>
<td>12</td>
<td>437</td>
<td>708</td>
</tr>
<tr>
<td>(10,34)</td>
<td>12</td>
<td>437</td>
<td>1050</td>
</tr>
<tr>
<td>(15,29)</td>
<td>12</td>
<td>437</td>
<td>1335</td>
</tr>
<tr>
<td>(19,8)</td>
<td>12</td>
<td>437</td>
<td>1563</td>
</tr>
</tbody>
</table>

Table 3: Sample results of a pixel after Second Level Encryption

4.1.2 Decryption Module

At the receiving end, decryption is achieved using an ANN. The neural network is trained for the standard mapping value and the weights and the biases are stored before applying the input to it. MATLAB’s neural network tool box[26][21] is used for implementing and training the neural network.

![Figure 13: Block diagram of 3 layer backpropagation net](image)
Shweta R. Bhamare .et.al.

Wi: weight matrix of the ith layer
f: activation function
bij: bias of the jth neuron in the ith layer

The system is designed for three layers: input, output and the hidden layer. The input and output layers have only one neuron and the hidden layer has 695 neurons. Large numbers of neurons are essential for achieving high accuracy. The decryption process is achieved in three steps. During the first stage, the impurity which was varying with respect to the position of the pixel is removed. In the second stage, the additional columns from the matrix which were added during the encryption are deleted. During the third stage, the received image data and weights which were stored after training are used to simulate the network. The output of this stage is the recovered image which is shown in Figure.

4.1.3 Interface module
The system is tested by connecting two computers in the network. File transfer from the host system to the remote system was done using the JAVA remote method invocation.

4.1.4 Authentication module
Biometric recognition authenticates a person based on his biological and behavioral (biometric) traits. Biometric recognition forms a strong link between a person and his identity because biometric traits cannot be easily shared, lost, or duplicated. Hence, biometric recognition is intrinsically superior and more resistant to social engineering attacks (e.g., phishing) than the two conventional methods of recognition, namely, passwords and tokens. Since biometric recognition requires the user to be present at the time of authentication, it can also deter users from making false repudiation claims.

4.2 Results and Discussion

4.2.1 Need for two levels of Encryption
The reason behind including two levels of encryption is that, although the pixel value changes after the first level of encryption all the pixels with same original value will have the same encrypted value, because of which intensity changes but image can still be visible.

To overcome this problem, the second level encryption is used. During the second level encryption the impurity changes with respect to pixel position. It means that the pixel with same original value will have two different values after the second level of encryption depending on pixel position.

4.2.2 Need for Normalization
As mentioned earlier ANN is used for decrypting the image. ANNs require training before they are used for any application[14]. The results of training were not converging for the given input data set having 256 values. This problem was solved by the normalisation of the input data. Normalization is the process of transforming the data set to the values ranging from -1 to 1.

4.2.3 Requirement of additional two columns during encryption
The image matrix was treated as series of vectors (one row as one row input) while simulating the network. Thus it became mandatory to have a minimum and maximum pixel values in each row for achieving accurate normalization of the vector[4].

5. Conclusion
Cryptography is used in transmitting images in a safe way. The cryptography process occurs by applying the inverse of the same encoding method used, for decoding on the transmitting side. Nowadays, in the light of continuous update in encoding methods, the process becomes quite slow and difficult to apply. In this work, it is aimed to update code automatically using Artificial Neural Network (ANN) and decode without any additional computation on the transmitted side.

Here, in order to make decryption difficult for eavesdropper, a random algorithm has been used for encryption. Using the neural network at the receiver end has made random encryption possible at the senders end. Also the need for key exchange prior
to data exchange has been eliminated. The transmission and reception of the image is made more secure by using fingerprint recognition method of biometric authentication.

There is lot of scope for enhancing this work to video encryption and decryption.

References:
[1] Saraswati D. Joshi, Dr. V.R. Udupi, Dr. D. R. Joshi “A Novel Neural Network Approach for Digital Image Data Encryption/Decryption”
[2] Hüsamettin UYSAL, Sinem KURT, Tülay YILDIRIM “Automatic Decryption of images through Artificial Neural Network”