Scholars Journal of Engineering and Technology (SJET) **ISSN 2321-435X (Online)**
Sch. J. Eng. Tech., 2015; 3(1B):94-97 **ISSN 2347-9523 (Print)**

(An International Publisher for Academic and Scientific Resources)
www.saspublisher.com

Research Article

Encryption Method of Gray Image Based on BP Neural Network

Lili Wang[1*], Xincheng Gao[2]
[1]School of Computer & Information Technology, Northeast Petroleum University, Daqing, China, 163311
[2]Modern Education Technique Center, Northeast Petroleum University, Daqing, China, 163311

***Corresponding author**
Lili Wang
Email: lily@nepu.edu.cn

Abstract: At present, the problem that exists in the gray image encryption is easy to be cracked. Aiming at it, this paper proposes a kind of encryption method based on BP neural network. This method uses the very strong nonlinear transform ability of neural network to improve the security of image information. This paper detailed describes the specific implementation process of encryption method based on BP neural network. Through the simulation experiment, good results have been achieved.
Keywords: Gray image ; Image encryption ; Neural network ; Simulation experiment.

INTRODUCTION

Digital image is one of the main medium for people to express and acquire information. How to ensure the information safety of digital image is always an important issue. At present, image encryption is one of the many safety measures which have been taken. The encryption idea is that changing the original location or color of image pixels and turning it into a messy image[1].

At present, the common encryption algorithm can achieve good encryption effect, but the encryption rule is easy to be cracked by exhaustive method. Artificial neural network is an effective technology and method in the field of intelligent information processing. It can carry on self-learning to find out the inherent laws of samples, and according to the stored knowledge to identify new sample[2]. Therefore, this paper proposes an encryption method based on BP neural network, which using the strong nonlinear transform ability of neural network. The third party is difficult to find out the relationship to crack the image when they don't know the network transformation model. At the same time, if the network takes different structure parameters, the encryption of the same image is different. In the same way, the parameters of digital image recovery are also different. So it can greatly improve the security of image information.

SEVERAL COMMON ENCRYPTION METHODS

At present, the common digital image encryption methods include Arnold transform, Hilbert curve, Baker transform, etc.

Arnold Transform

Arnold transform is a common image processing technology. The transform formula is [3]:

$$\begin{pmatrix} X' \\ Y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} (\text{mod } n) \qquad (1)$$

(X, Y) is the original coordinate of image pixel, (X', Y') is the new coordinate of image pixel, n is the image order, namely the image size. After all coordinates of image pixels are transformed by the formula, the encryption image is generated.

Hilbert Transform

Hilbert curve is found by mathematician David, which is a fractal curve to fill the whole square in accordance with the move rule [4]. The formation of Hilbert curve is as follows:

(1) According to the move rule of Hilbert curve to traverse all pixels of the image, and store them in the matrix A.
(2) Using transform formula [(m-1) /n, (m-1) mod n] to rearrange the elements in A, m is the serial number of element.
(3) According the modified element to generate the final encryption image.

Baker Transform

Baker transform is a kind of chaotic mapping, it can produce very wonderful chaos phenomenon. Through Baker mapping, image can be disrupted and the energy spectrum is evenly distributed.

$B\left(\frac{1}{2},\frac{1}{2}\right)$ is a generalization of Bernoulli change, its definition is as follows:

$$T(X_k,Y_k)=(X_{k+1},Y_{k+1})=\begin{cases}(2X_k,\frac{1}{2}Y_k), & \\ (2X_k-1,\frac{1}{2}(Y_k+1)),\end{cases} \quad (2)$$

(X_k,Y_k) represents a value which is through K times mapping.

The Comparison of Three Methods

Arnold transform use the matrix transformation, Hilbert transform use matrix encryption transformation in according to curve generated matrix and image pixel matrix, and Baker transform use chaos mapping[5]. They all can quickly disperse the adjacent pixels by taking a small amount of calculation. But because these three kinds of transformation are based on fixed rules, the encryption rule can be found through directly comparing plaintext with cipher text of pixels. So they are easy to be cracked in application and security is low.

BP NEURAL NETWORK

BP neural network is a kind of multilayer neural network with three or more than three layers. Each layer is composed of a number of neurons, and these neurons realize feed forward connection[6]. It can learn and store a large amount of nonlinear mapping relationship between input samples and output samples, and make output error minimum through continuous automatically adjust parameters.

Typical BP neural network model includes Input Layer, Hidden Layer and Output Layer. As shown in figure 1.

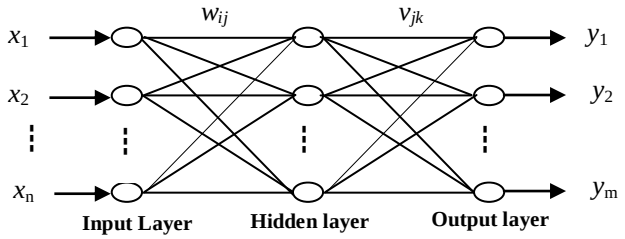

Fig.1 BP neural network model

(1) (X,Y) is 1-dimensional sample space, X is input sample, Y is output sample.

(2) $W=(w_1,w_2,\Lambda,w_n)$ is connection weights and threshold of arbitrary multilayer BP network.

(3) Excitation function adopts Sigmoid, its definition is $g(x)=1/(1+e^{-x})$.

(4) The standard training form of the BP algorithm is:

$$W^{k+1}=W^k-h\nabla E(W^k) \quad W^0=W_0$$

Among them: $h>0$ is learning step, $E=\|Y_X-Y\|^2$, Y is expected output, Y_X is actual output of sample X, $\nabla E(W^k)$ is gradient of $E(W^k)$ in point W^k.

IMAGE ENCRYPTION METHOD BASED ON BP NEURAL NETWORK

The method of image encryption and recovery based on BP neural network is as following. Two kinds of neural network model are set up respectively. Encryption model is the transformation relation from original image to encryption image to encrypt image. Recovery model is the inverse transformation relationship from encryption image to original image to recover image. The step of image encryption algorithm based on BP neural network is as follows:

(1) The original image with N*M pixels is divided into h sub graph with n*m pixels. The gray values of each sub graph are taken out in row as an input sample. After transforming all sub graph in order, we get all input samples (h*n=N, h*m=M).

(2) The encryption image with N*M pixels is divided into h sub graph with n*m pixels. The gray values of each sub graph are taken out in row as output sample. After transforming all sub graph in order, we get all output samples (h*n=N, h*m=M).

(3) Preprocess all input and output samples.

(4) Set connection weights, error function, calculation accuracy and maximal learning times of the neural network.

(5) Train the network using all input and output samples.

(6) Save the connection weights and thresholds.

At this point, the encryption network model from original image to encryption image is completed. We can put an arbitrarily image as input samples in the network model, and can get the corresponding encryption image.

Image recovery is similar with above. Input samples are the gray values of encryption image pixels, and output samples are the gray values of original image pixels. Submit the input and output sample into network to train, store the network

connecton weights and thresholds, and then establish the recovery model from the encryption image to the original image.

SIMULATION EXPERIMENT

According to the above algorithm, we carry on an image encryption and recovery experiment. The experiment selects the original image and encryption image with 128*128 pixels as shown in figure 2 and figure 3.

Fig.2 Original image

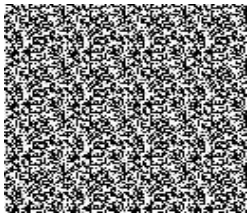

Fig.3 Encryption image

Acquire Training Sample

The two images are respectively divided into 16 sub graphs with 32*32 pixels. Getting the gray value of each sub graph in row, because R, G, B values of gray image pixel are the same, so we save one value of them into a two-dimensional array. When we want to get encryption model, the gray values of original image are as input samples and the gray values of encryption image are as output samples. When we want to get recovery model, the input samples and output samples are exchanged.

Neural Network Training

We choose BP neural network with three layers. The node number of input and output is 1024, the node number of hidden layer is 100, and the number of training sample is 16. Error is 0.05, learning speed is 0.08, inertia coefficient is 0.2, and incentive function is sigmoid. Using the prepared training sample to train network, store the connection weights and thresholds after training, and get the corresponding model. The training convergence diagram of encryption train is shown in figure 4. Thus far, we can get encryption model and recovery model.

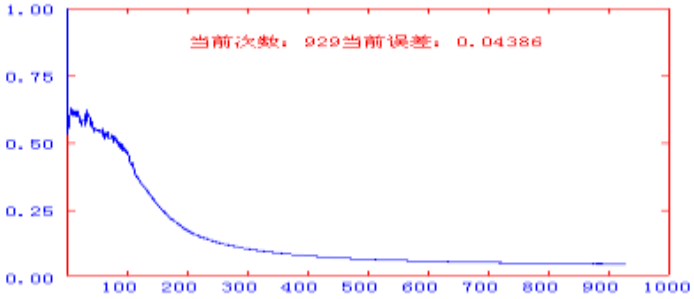

Fig.4 Training convergence diagram

Image Encryption and Recovery Using The Trained Network

Using the trained neural network in section 5.2, we carry on image encryption and restoration. The gray values of figure 5 are as input samples, we can get encryption image as shown in figure 6 through the encryption neural network. When we put the figure 6 into recovery neural network, we can get the recovery image as shown in figure 7.

Fig.5 Original Image

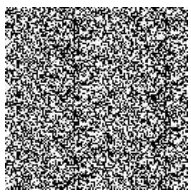

Fig.6 Encryption Image

Fig.7 Recovery image

CONCLUSION

This paper proposed a kind of image encryption method based on BP neural network. We can see from the experimental results that the encryption effect is better. It is very difficult to see the original image from the encryption image, and at the same time, there is not obvious difference between original image and recovery image. So it can effective solve the security problem of image information.

REFERENCES

1. Zhuxiuhua; BP Neural Network and Its Application in Web Document Automatic Classification. Journal of Modern Information, 2009; 29(5):163-166.
2. Wenchangci, Wangqin, Miaoxiaoning; Digital Image Encryption: A Survey. Computer Science, 2012; 39(12):6-9.
3. Renhonge, Shangzhenwei, Zhangjian; An algorithm of digital image encryption based on Arnold Transformation, Optical Technique, 2009; 35(3):384-388.
4. Zhangyunpeng, Zzuofei, Zhaizhengjun; Survey on image encryption based on chaos. Computer Engineering and Design, 2011; 32(2):463-466.
5. Yangjingbo; Quality Evaluation of University Librarians Based on the Neural Networks. Journal of Modern Information, 2008, (12):144-146.
6. Chenxinge; Study of Image Watermarking through Neural Network. Journal of Baoshan University, 2013; (5): 64-66.