http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 5 (6): 1063-1067, 2006
ISSN 1812-5638

Fingerprint Verification System Using Artificial Neural Network

[1]Md. Mamunur Rashid and [2]A.K.M. Akatar Hossain
[1]School of Science and Technology, Bangladesh Open University, Gazipur, Bangladesh-1705
[2]Department of Computer Science and Engineering, University of Rajshahi, Bangladesh

Abstract: A fingerprint is typically classified based on only the first type of features and uniquely identified based on the second type of features. The fingerprint verification system is the most perfect process to identify a person. The digital values of these features (Minutiae, ridge ending and bifurcation) are applied to the input of the neural network for training purpose using back propagation algorithm of Artificial Neural Network. During the training period, the values of the nodes are updated and stored in a relational knowledge base. For fingerprint recognition, the verification part of the system identifies the Fingerprint of a person with the help of the previous experiential values, which was stored in the relational knowledge base system. Finally, it is concluded that the performance of recognition of fingerprint using the minutiae features-based fingerprint verification system is better.

Key words: Minutiae, ridge ending, bifurcation, global ridge

INTRODUCTION

A biometric system is a pattern recognition system that recognizes a person. In the present study it is needed to ensure only the right people. There are many commercial systems designed for person identification. The most popular systems are based on fingerprint, facial image, retina colour and signature recognition techniques etc. Fingerprint is the rigid and furrow patterns on the tip of a finger (Fig. 1). It is a distinctive feature and remains invariant over a person's lifetime, excepts for cuts and bruises. The fingerprints are permanent and unique. Fingerprint authentication requires acquiring and digitizing a fingerprint image (Jaing and Yau, 2000). The digital image of the fingerprint includes several unique features in terms of rigid bifurcation and rigid ending, collectively referred to as minutiae. According to the method of acquisition of fingerprint data, there are two types of fingerprint verification system (i) On-line and (ii) Off-line. In this system, we consider only the Off-line fingerprints. The objective of this study is to investigate the criminals.

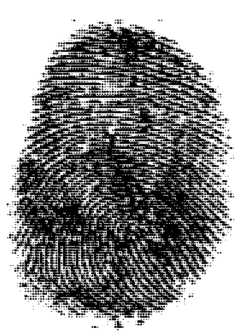

Fig. 1: A sample fingerprint image

FINGERPRINT VERIFICATION SYSTEM

The design of a fingerprint verification system consists two-stage (1) Enrollment Phase and (2) Verification Phase. Each phase has four steps: (i) Fingerprint collection, (ii) Preprocessing, (iii) Feature extraction and (iv) Training or matching as shown in Fig. 2. At first the static image of a fingerprint is applied to the input of the system. The image of the fingerprint is preprocessed and fingerprint features are extracted. The network is trained by using backpropagation neural network algorithm. A reference database is used to store the acquired knowledge and used to verify unknown fingerprint images (Jain *et al*., 1997).

Fingerprint collection: The fingerprint image acquired by the off-line process is known as the inked fingerprints while the image acquired by the on-line process is known as live-scan fingerprints. In the inked fingerprint acquisition method ink is applied to the finger and then pressed onto a paper to form an impression. The paper is then scanned at 500 dpi resolution by a standard grayscale scanner. A live-scan fingerprint is obtained directly from the finger without the intermediate use of paper. Typically, live-scan sensors capture a series of dab fingerprints when a fingertip is pressed on the sensor

Corresponding Author: Md. Mamunur Rashid, School of Science and Technology, Bangladesh Open University, Gazipur, Bangladesh-1705 Tel: +880152358995

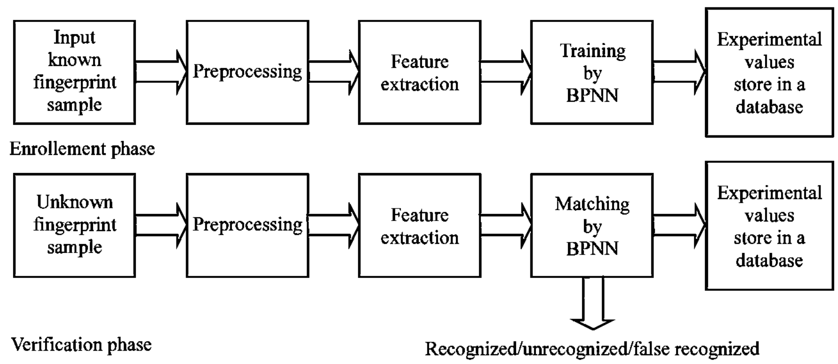

Fig. 2: Block diagram of an off-line fingerprint verification system

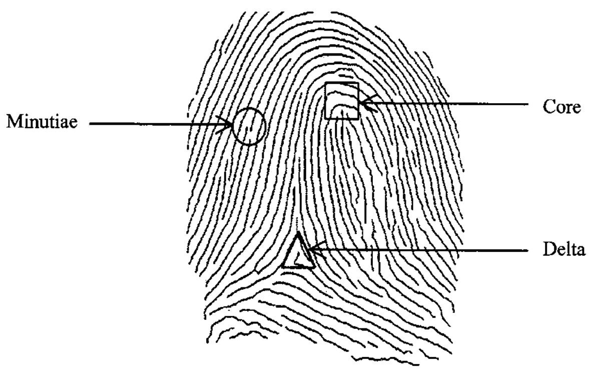

Fig. 3: Features of a fingerprint

surface. For the present research work, fingerprints are collected from different person by using the "inked" fingerprint method.

Fingerprint preprocessing: The system deals with the static scanned image of the fingerprints. Unwanted images i.e., noises may include during the production of fingerprint images on paper or during the scanning process of the fingerprint. The preprocessing of fingerprint image is related to the removal of noises, detecting edges and image scaling. To remove noises and enhance the fingerprint rigid patterns, the images are preprocessed by using the filtering feature of a graphics editor (Prabhakar, 2001). An algorithm is developed to detect the boundary of the fingerprint image and scaled to 480×360 pixel image (Fig. 3).

Feature extraction: Fingerprint verification system we consider only the minutiae features of a fingerprint. In this research rigid endings, rigid bifurcations, dots and bridges are considered. Other minutiae types such as island, enclosures, trifurcations, etc. are very rare. In order to extract fingerprint features, noise is eliminated from the fingerprint image by using a graphics editor. Then the fingerprint image is transformed to 480 × 360-pixel image by using image-scaling process (Rashid and Hossain, 2001). An extraction algorithm is used to extract the minutiae from the gray scale fingerprint image by examine the neighborhood pixels around each pixel of the thinned ridges. At the same time the minutiae points are located (Fig. 4) and these locations of the *minutiae* are preserved for fingerprint matching purpose (Maio and Maltoni, 1997).

Backpropagation neural network: The Backpropagation Neural Network (BPNN) is a multi-layered, feed-forward neural network that is fully interconnected by layers. Thus, there are no connections that bypass one layer to go directly to a later layer. The BPNN is called a mapping network because it is able to compute some functional relationship between its input and output. Figure 5 shows the three-layer BPNN architecture.

The input vector is represented by X[a][i]. Where a is the fingerprint of Mr. X or Y or Z and i is the pattern matrixes, i.e., 16×16 array (i = 0, 1, 2, 3, - - - -, 256). The target output is represented by T[a][i].

The learning of this network has been accomplished by error Back Propagation Neural Network. How this learning rule was used to train the network, it has been described below:

The weight vectors W_{ij} and W_{jk} and the threshold values for each PE in the network were to be initialized with random numbers (Freeman and Skapura, 1991). The network was provided with the input patterns and also the desired respective output patterns. The input patterns were connected to hidden (PEs) through the weights W_{ij}. In the hidden layer, each PE computed the weighted sum according to the equation, which is given by

$$net_{aj} = \Sigma\, w_{ij}\, o_{ai} \quad (1)$$

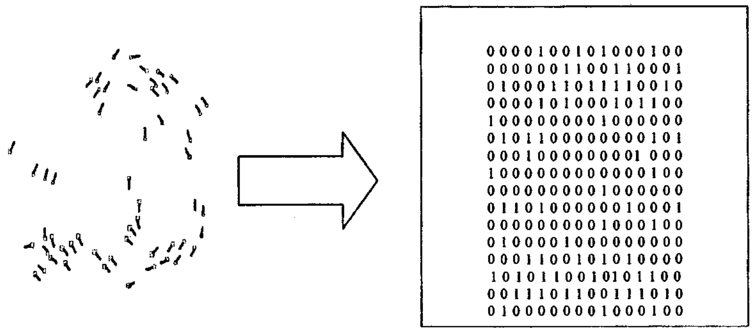

Fig. 4: Minutiae extraction from a sample fingerprint image of 16×16 feature matrixes

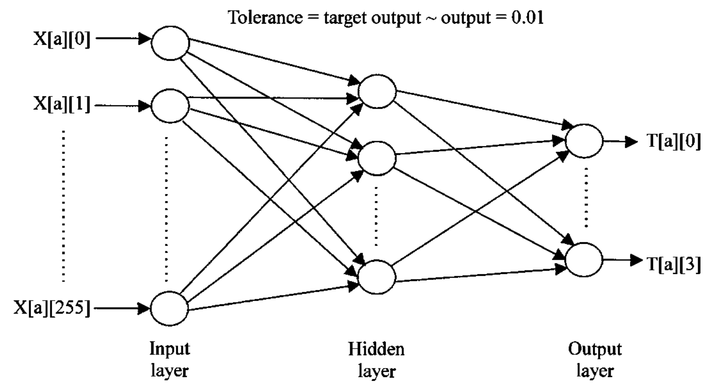

Fig. 5: Three layer neural network

Where O_{ai} is the input of unit i for pattern number a. The threshold of each PE was then added to its weighted sum to obtain the activation active (j) of that PE i.e.,

$$activ_j = net_{aj} + uh_j \quad (2)$$

Where uh_j is the hidden threshold weight for jth PEs. This activation determined whether the output of the respective PE was either 1 or 0 (fires or not) by using a sigmoid function,

$$O_{aj} = 1 / (1+e^{-k1*activ_j}) \quad (3)$$

Where k_1 is called the spread factors, these O_{aj} were then served as the input to the output computation. Signal O_{aj} were then fan out to the output layer according to the relation,

$$net_{ak} = \Sigma\, W_{jk} O_{aj} \quad (4)$$

and the output threshold weight uo_k for kth output PEs was added to it to find out the activation $activo_k$

$$activo_k = net_{ak} + Uo_k \quad (5)$$

The actual output O_{ak} was computed using the same sigmoid function, which was

$$O_{ak} = 1/(1+e^{-k2*activeok}) \quad (6)$$

Here another spread factor k_2 has been employed for the output units.

In the second stage, after completing the feed-forward propagation, an error was computed by comparing the output O_{ak} with the respective target t_{ak}, i.e

$$\delta_{ak} = t_{ak} - O_{ak} \quad (7)$$

This error was then used to adjust the weight vector W_{jk} using the equation

$$\Delta w_{jk} = \eta_2 k_2 \delta_{ak} O_{aj} O_{ak} (1-O_{ak}) \quad (8)$$

Where $\int (activo_k) = k_2 O_{ak} (1-O_{ak})$ the derivation of sigmoid function.

The weight vector W_{jk} was then adjusted to $w_{jk}+\Delta w_{jk}$. For the threshold weight of the output PE, similar equation was employed,

$$\Delta uo_k = \eta_2 k_2 \delta_{ak} O_{ak}(1-O_{ak}) \quad (9)$$

and the new threshold weight equaled $uo_k + \Delta uo_k$.

In the next step, this error and the adjusted weight vector W_{jk} were feedback to the hidden layer to adjust the weight vector W_{ij} and threshold weight uh_j. In this layer change in weight vector W_{ij} was computed by using equation,

$$\Delta w_{ij} = \eta_1 k_1 O_{ai} O_{aj}(1-O_{ai}) \, \Sigma \, \delta_{ak} W_{jk} \quad (10)$$

Where $\int$ (activh_j) = $k1 O_{aj}(1-O_{aj})$. The weight vector W_{ij} was then adjusted to $W_{ij} + \Delta W_{ij}$. For the threshold weights of the hidden PEs, similar equation was employed

$$\Delta uh_j = \eta_1 k_1 (1-O_{aj}) \, \acute{O} \, \delta_{ak} W_{jk} \quad (11)$$

and new threshold weights were calculated $uh_j + \Delta uh_j$.

The properties of sum-squared error equation dictate that as output approaches its maximum or minimum value, adjustments to individual weights become less pronounced. This is a testament to the stability of the BackPropagation algorithm. The significance of the training process is that, as the network trains, the nodes in the intermediate layers organized themselves such that different nodes learn to recognize different features of the total input space (Chung and Sulong, 2001).

EXPERIMENTAL STUDY AND DISCUSSION

To test the fingerprint verification system, fingerprints are taken from 20 different people. For each person, 5 fingerprints of a finger (Thumb) are collected. From the fingerprint file each fingerprint is separated from its neighbors to produce a fingerprint database. After extracting the features from each fingerprint, the feature matrix is applied to the input of backpropagation neural network for training purpose. The learning rate of the network is set to $\eta_1 = \eta_2 = 0.6$ and spread factor is $\kappa_1 = \kappa_2 = 0.7$.

During the recognition period, the error tolerance level is set to 0.01. After completing the training, the updated weights and threshold values are stored in a file, which are used in the fingerprint verification process. To verify fingerprint, new fingerprint image is taken from a person and features are extracted to form a feature matrix.

Table 1: Experimental data of fingerprint verification system

No. of person	40
No. of fingerprint samples from each person	4
Total no. of fingerprint samples	160
No. of recognized samples	148
No. of unrecognized samples	4
No. of false recognized samples	8
Accuracy of the system (%)	92.5

The feature matrix is then applied to the input of the backpropagation neural network to observe whether the system recognized the fingerprint or not or show false recognition.

$$\%\text{ of accyracy of the system} = \frac{\text{Total No.of recognized fingrprint samples}}{\text{Total No.of fingrprint samples}} \times 100$$

The result of fingerprint recognition is shown in Table 1.

CONCLUSIONS

This study accomplished that the off-line fingerprint verification system is not difficult but it is not easy to detect distorted fingerprint exactly. The proposed Minutiae features-based fingerprint verification system gives an acceptable accuracy in off-line fingerprint verification system. Several factors are responsible for correct result of neural computing. The convergence of the solution depends heavily on initialization with random numbers and accuracy of the results depends on (i) spread factors (ii) learning rates and (iii) iterations. The accuracy of the system can be increased by increasing the number of hidden units of the backpropagation network. In this study, only the positions of minutiae are considered for training and verification process. By considering the orientations of minutiae we can increase the accuracy of the system (Adhami and Meenen, 2001). Other features of fingerprint such as core and delta may be taken into account for accurate verification of fingerprints. Other learning method such as ART-2 (Adaptive Resonance Theory-2), HMM, Genetic Algorithm will be used to verify the performance of recognition of fingerprints.

REFERENCES

Adhami, R. and P. Meenen, 2001. Fingerprints for security. IEEE Potentials, 20: 33-38.

Chung and G. Sulong, 2001. Finger Classification Approach. Proceedings of the ISSPA., 1: 13-16.

Freeman, J.A. and D.M. Skapura, 1991. Neural Networks. Addison-Wesley Longman Inc, Calefornia, pp: 89-124.

Jain, A.K., L. Hong, S. Pankanti and R. Bolle, 1997. An identity authentication system using fingerprints. Proceedings of the IEEE, 85: 1365-1388.

Jaing, X. and W.Y. Yau, 2000. Fingerprint minutiae matching based on the local and global structures. Proceedings of the 15th International Conference on Pattern Recognition. Barcelona, Spain, 2: 1042-1045.

Maio, D. and D. Maltoni, 1997. Direct gray-scal minutiae detection in fingerprints. IEEE Transactions on Pattern Analysis and Machine Intelligence, 19: 27-40.

Prabhakar, S., 2001. Fingerprint classification and matching using a filterbank. Ph.D. Thesis, Michigan State University, USA.

Rashid, M.M. and A.K.M.A. Hossain, 2001. An approach to implement bangla handwriter identification system using artificial neural network. M.Sc. Thesis, Rajshahi University.