FINGER PRINT CLASSIFICATION WITH NEURAL NETWORK FOR PERSONAL AUTHENTICATION

Miss. Puja A.Ganthade [1], Mr.Vijay L. Agrawal[2]
[1]Student of HVPM'S College of Engineering and Technology Amravati (India)
[2]Associate Professor in Dept. (Electronic and Telecommunication) of HVPM'S
College of Engineering and Technology (India)

Abstract— Finger print classification with neural network for personal authentication, which uses the WHT transform over the entire finger print image as feature detector and a constructive one hidden layer feed forward neural network as a finger print classifier proposed technique is applied to a database consisting of images of 96 having Twelve man finger print images. Images of 72 are used for network training, and the remaining images of 24 are used for cross validation. It is demonstrated that the best recognition rates are 100% for the training as well as cross validation for 11 men finger print images except 1 men finger print image 50% for C.V and 88.88 for Train . Furthermore, The Average Classification Accuracy of GFF Neural Network comprising of one hidden layers with 7 PE's organized in a typical topology is found to be superior (100 %) for Training . Finally, optimal algorithm has been developed on the basis of the best classifier performance. The algorithm will provide an effective alternative to traditional method of facial captured image analysis for deciding the Human emotion.

Keywords— Neural solution, MatLab, Microsoft Excel, Finger print scan images.

INTRODUCTION

With the advent of electronic banking, e-commerce, and smartcards and an increased emphasis on the privacy and security of information stored in various databases, automatic personal identification has become a very important topic. Accurate automatic personal identification is now needed in a wide range of civilian applications involving the use of passports, cellular telephones, automatic teller machines, and driver licenses. Traditional knowledge-based (password or Personal Identification Number (PIN) and token-based (passport, driver license, and ID card) identifications are prone to fraud because PINs may be forgotten or guessed by an imposter and the tokens may be lost or stolen. Therefore, traditional knowledge-based and token-based approaches are unable to satisfy the security requirements of our electronically interconnected information society (see Figure 1.1). As an example, a large part of the annual $450 million Mastercard credit card fraud is due to identity fraud[7]. A perfect identity authentication system will necessarily have a biometric component. Eventually, a foolproof identity authentication systems will have all the three components (knowledge-based, token-based, and biometrics). In this thesis, we have only focused on the biometrics component of an automatic identification system in general, and a fingerprint-based biometric identification system in particular.

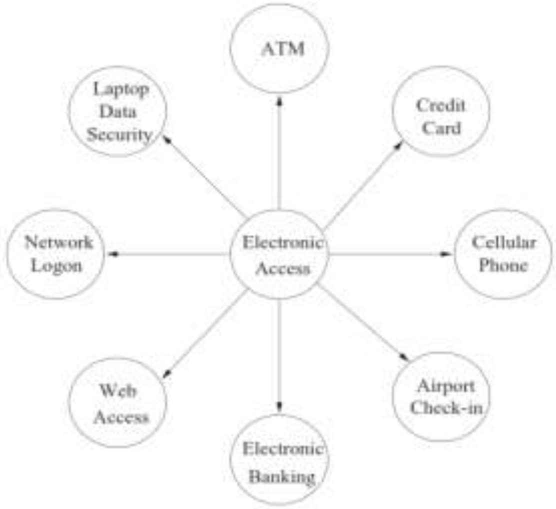

Figure 1: Various electronic access applications in widespread use that require automatic authentication

Fingerprints

Fingerprints are the ridge and furrow patterns on the tip of the finger[8] and have been used extensively for personal identification of people[9] . Figure 1.2 shows an example of a fingerprint. The biological properties of fingerprint formation are well understood and fingerprints have been used for identification purposes for centuries. Since the beginning of the 20th century, fingerprints have been extensively used for identification of criminals by the various forensic departments around the world [10]. Due to its criminal connotations, some people feel uncomfortable in providing their fingerprints for identification in civilian applications. However, since fingerprint-based biometric systems offer positive identification with a very high degree of confidence, and compact solid state fingerprint sensors can be embedded in various systems (e.g.,cellular phones), The availability of cheap and compact solid state scanners [11]as well as robust fingerprint matchers are two important factors in the popularity of fingerprint-based identification systems. Fingerprints also have a number of disadvantages as compared to other biometrics. For example, approximately 4% of the population does not have good quality fingerprints, manual workers get regular scratches on their fingers which poses a difficulty to the matching system, finger skin peels off due to weather, fingers develop natural permanent creases, temporary creases are formed when the hands are immersed in water for a long time, and dirty fingers can not be properly imaged with the existing finger print sensors. Further, since fingerprints can not be captured without the user's knowledge, they are not suited for certain applications such as surveillance.

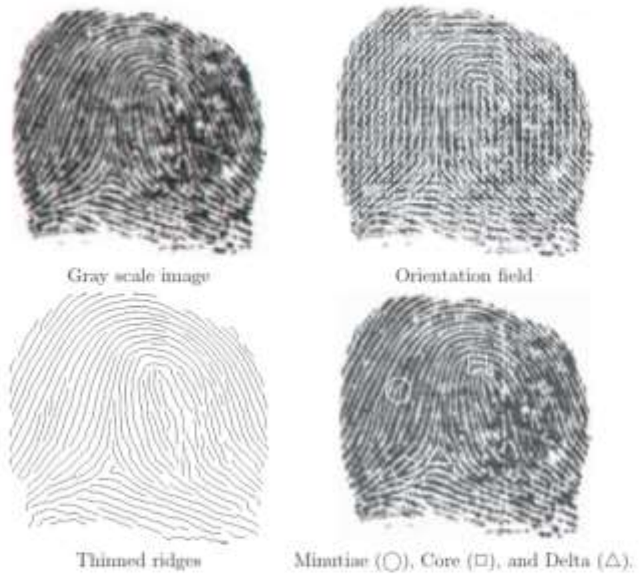

Figure 1.2: Orientation field, thinned ridges, minutiae, and singular points.

1) **Neural Networks**

Following Neural Networks are tested:

a) Feed-Forward Neural Networks

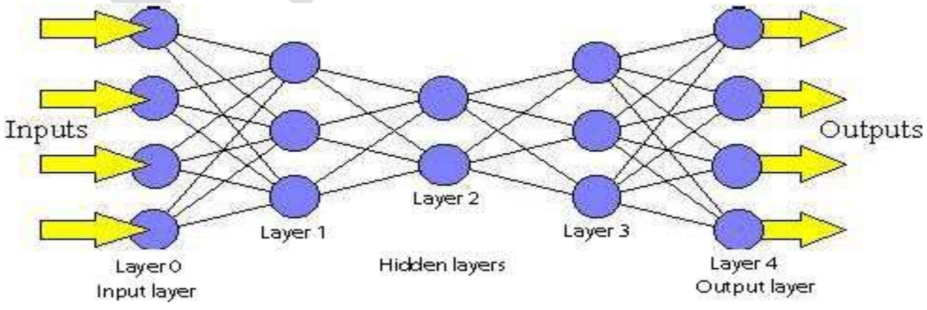

Figure 1.3: A feed-forward network.

Feed-forward networks have the following characteristics:

1. Perceptrons are arranged in layers, with the first layer taking in inputs and the last layer producing outputs. The middle layers have no connection with the external world, and hence are called hidden layers.

2. Each perceptron in one layer is connected to every perceptron on the next layer. Hence information is constantly "fed forward" from one layer to the next., and this explains why these networks are called feed-forward networks.

3. There is no connection among perceptrons in the same layer.

A single perceptron can classify points into two regions that are linearly separable. Now let us extend the discussion into the separation of points into two regions that are not linearly separable. Consider the following network: [10]

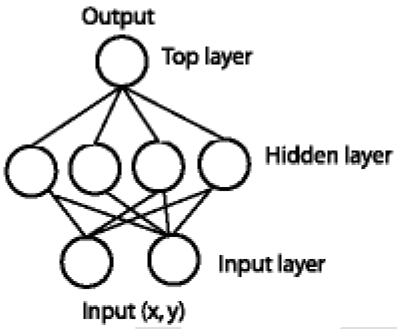

Figure 1.4 A feed-forward network with one hidden layer.

2)Learning Rules used:

a) Momentum

Momentum simply adds a fraction m of the previous weight update to the current one. The momentum parameter is used to prevent the system from converging to a local minimum or saddle point. A high momentum parameter can also help to increase the speed of convergence of the system. However, setting the momentum parameter too high can create a risk of overshooting the minimum, which can cause the system to become unstable. A momentum coefficient that is too low cannot reliably avoid local minima, and can also slow down the training of the system.

3)Simulation Results

The GFF neural network has been simulated for 96 finger print images out of which 72 were used for training purpose and 24 were used for cross validation.

The simulation of best classifier along with the confusion matrix is shown below :

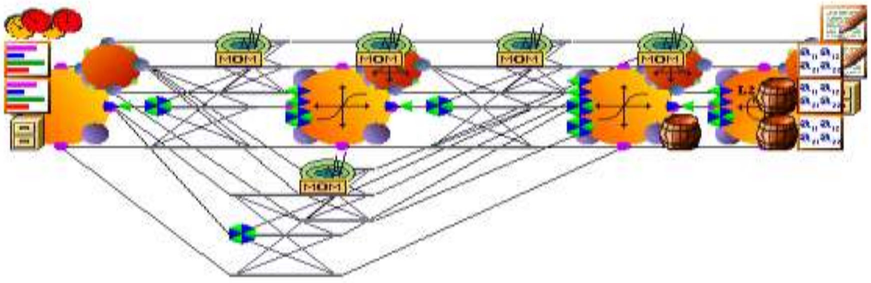

Figure1.5: The Best Neural network with maximum accuracy

4) Results

Best Networks	*Training*	*Cross Validation*
Hidden 1 PEs	49	7
Run #	2	1
Epoch #	1000	615
Minimum MSE	0.004017875	0.023769675
Final MSE	0.004017875	0.02399354

Table1: Processing Element Training Data Set

Test on Cross validation (CV):

Output /Desired	*MAN12*	*MAN11*	*MAN10*	*MAN9*	*MAN8*	*MAN7*	*MAN6*	*MAN5*	*MAN4*	*MAN3*	*MAN2*	*MAN1*
MAN12	2	0	0	0	0	0	0	0	0	0	0	0
MAN11	0	2	0	0	0	0	0	0	0	0	0	0
MAN10	0	0	2	0	0	0	0	0	0	0	0	0
MAN9	0	0	0	2	0	0	0	0	0	0	0	0
MAN8	0	0	0	0	2	0	0	0	0	0	0	0
MAN7	0	0	0	0	0	2	0	0	0	0	0	0
MAN6	0	0	0	0	0	0	2	0	1	0	0	0
MAN5	0	0	0	0	0	0	0	2	0	0	0	0
MAN4	0	0	0	0	0	0	0	0	1	0	0	0
MAN3	0	0	0	0	0	0	0	0	0	2	0	0
MAN2	0	0	0	0	0	0	0	0	0	0	2	0
MAN1	0	0	0	0	0	0	0	0	0	0	0	2

Table 2: Confusion matrix on CV data set

Performance	*Man12*	*Man11*	*Man10*	*Man9*	*Man8*	*Man7*	*Man6*	*Man5*	*Man4*	*Man3*	*Man2*	*Man1*
MSE	0.008	0.002	0.029	0.001	0.004	0.002	0.029	0.024	0.044	0.04	0.01	0.008
NMSE	0.115	0.033	0.386	0.020	0.053	0.027	0.37	0.32	0.58	0.59	0.22	0.10
MAE	0.06	0.036	0.079	0.036	0.053	0.037	0.10	0.10	0.11	0.12	0.07	0.063
Min Abs Error	0.01	0.0003	0.006	0.002	0.001	0.0001	0.002	0.004	0.008	0.002	0.002	0.002
Max Abs Error	0.38	0.129	0.764	0.063	0.163	0.10	0.62	0.42	0.83	0.65	0.47	0.305
r	0.96	0.987	0.83	0.99	0.97	0.98	0.79	0.84	0.68	0.65	0.88	0.945
Percent Correct	100	100	100	100	100	100	100	100	50	100	100	100

Table 3: Accuracy of the network on CV data set

Test on Training:

Output /Desired	*MAN12*	*MAN11*	*MAN10*	*MAN9*	*MAN8*	*MAN7*	*MAN6*	*MAN5*	*MAN4*	*MAN3*	*MAN2*	*MAN1*
MAN12	6	0	0	0	1	0	0	0	0	0	0	0
MAN11	0	6	0	0	0	0	0	0	0	0	0	0
MAN10	0	0	6	0	0	0	0	0	0	0	0	0
MAN9	0	0	0	6	0	0	0	0	0	0	0	0
MAN8	0	0	0	0	5	0	0	0	0	0	0	0
MAN7	0	0	0	0	0	6	0	0	0	0	0	0
MAN6	0	0	0	0	0	0	6	0	0	0	0	0
MAN5	0	0	0	0	0	0	0	6	0	0	0	0
MAN4	0	0	0	0	0	0	0	0	6	0	0	0
MAN3	0	0	0	0	0	0	0	0	0	6	0	0
MAN2	0	0	0	0	0	0	0	0	0	0	6	0
MAN1	0	0	0	0	0	0	0	0	0	0	0	6

Table 3: Confusion matrix on Train data set

Performance	***Man12***	***Man11***	***Man10***	***Man9***	***Man8***	***Man7***	***Man6***	***Man5***	***Man4***	***Man3***	***Man2***	***Man1***
MSE	0.018	0.0006	0.001	0.0009	0.001	0.00	0.001	0.001	0.001	0.001	0.001	0.001
NMSE	0.237	0.008	0.01	0.01	0.01	0.012	0.020	0.014	0.025	0.023	0.018	0.015
MAE	0.064	0.021	0.03	0.02	0.03	0.026	0.034	0.028	0.040	0.036	0.033	0.029
Min Abs Error	0.005	0.0005	0.001	0.001	0.002	0.0006	0.0001	2.98026 E-05	0.00028	0.0002	0.0007	0.0003
Max Abs Error	1.055	0.055	0.06	0.05	0.07	0.055	0.055	0.055	0.055	0.083	0.070	0.055
r	0.90	0.99	0.99	0.99	0.99	0.995	0.99	0.995	0.993	0.99	0.993	0.994
Percent Correct	100	100	100	100	83.33	100	100	100	100	100	100	100

Table 4: Accuracy of the network on Train data set

ACKNOWLEDGMENT

We are very grateful to our HVPM College of Engineering and Technology to support and other faculty and associates of ENTC department who are directly & indirectly helped me for these paper.

.CONCLUSION

From the results obtained it concludes that the GFF Neural Network with MOM (MOMENTUM) and hidden layer 1 with processing element 7 gives best results 11 finger print identify 100% only man8 finger print is identify 83.33% in Training as well as in Cross Validation it gives 11 finger print identify 100% only man4 finger print is identify 50%.

REFERENCES:

1) Mehtre B M, Chatterjee B. Segmentation of fingerprint image composite method Pattern Recognization,1989.22(4);381-385

2) Jain A K, Flynn P, Ross A. Handbook of biometrics.2007

3)Hashimoto J.," finger vein authentication tech. and its futer",Proceeding of Symposium on VLSI Circuit, 2006pp.5-8

4) Proceedings of the WSEAS International Conference on Signal, Speech and Image

5) Digital Image Processing ,second edition ,PHI publication a: Rafael C. Gonzalez

6) Digital Signal Processing –Principles ,Algorithms , and Applications, Fourth edition ,Pearson Education : John G.Proakis , Dimitris G. manolakis.

7) A. K. Jain, R. M. Bolle, and S. Pankanti (editors), Biometrics: Personal Identification in a Networked Society, Kluwer Academic Publishers, 1999.

8) H. C. Lee and R. E. Gaensslen (editors), Advances in Fingerprint Technology,Elsevier, New York, 1991.

9) A. K. Jain, L. Hong, S. Pankanti, and Ruud Bolle, "An Identity Authentication System Using Fingerprints," Proceedings of the IEEE, Vol. 85, No. 9, pp. 1365-1388, 1997.

10) Federal Bureau of Investigation. The Science of Fingerprints: Classification and Uses, U.S. Government Printing Office, Washington D.C., 1984.

11) Veridicom products. Available at: www.veridicom.com