Robust Fingerprint Identification System Using Backpropagation and ART Neural Networks

A A Ilumoka, Ph.D[1] and M. Talluri, M.Eng[2] *

1- University of Hartford- Department of ECE
West Hartford, CT 06117 - USA
2- University of Hartford- Department of ECE
West Hartford, CT 06117 - USA

Abstract

This paper describes a robust minutiae-based fingerprint identification method suitable for use in small populations. System employs two serially connected neural networks in which fingerprint feature extraction is carried out by the first network – a backpropagation neural network and matching by the second - an adaptive resonance theory network which performs the decision making task of matching acquired fingerprint to templates in a database. The approach has been applied to a real database of noisy fingerprints derived from the 2002 Fingerprint Verification Competition (FVC2002) and has achieved error rates as low as 4% at penetration rates of 100%.

1 Introduction and Related Work

Biometric systems are pattern recognition systems that recognize an individual based on unique physiological or behavioral characteristics – called *biometric identifiers* - presented by the person. Biometric identifiers should be universal (applicable to all persons), distinctive and invariant. Additionally, identifiers should be quantifiable. Scientific investigations and rigorous study of fingerprints in the late 19th century revealed that no two individuals possess the same fingerprints thus opening up the field of identification via visual and later automated inspection of fingerprints. Law enforcement agencies were the first to develop systems of acquiring fingerprints through electronic media, spearheading technology for registration, feature identification and matching. Although research in the area of fingerprint recognition has been actively pursued in the last 4-5 decades [1-6], fingerprint recognition is still very much a challenging pattern recognition problem, particularly in today's world of identity theft, privacy issues and global terrorism. High levels of accuracy and speed are desirable also robustness and fraud resistance. Capelli et al review developments in fingerprint verification systems in [1] based on their features, computational constraints and performance. In [2] an image-based approach based on features extracted from integrated Wavelet and the Fourier-Mellin Transform is described. In [3], a hierarchical data structure based on the Multi-space KL transform specifically designed for locally correlated data is used to index multidimensional data. Artificial

* Work is funded by a corporate teaching grant from Neuralware Inc., Pittburgh PA

intelligence methods are employed in [4] in an optimization approach to fingerprint authentication in which fingerprint parameters are determined using genetic algorithms. In [5], fingerprint minutiae coordinates are encoded as elements in a smart card and a secret key encoded in a polynomial evaluated at minutiae locations. Given a matching fingerprint, a valid user can reconstruct the polynomial and hence the original secret key. Robustness of identification is enhanced in [6], where prints from fake fingers are distinguished from real ones based on analysis of skin distortion as finger is moved during fingerprint registration. In the work reported here, a neural network-based fingerprint identification system has been developed for the purpose of recognizing an individual from a small population (<100 persons). System extracts important minutiae-based features in the fingerprint and conducts a comparison with a template database for a match. Due to limited size of population, database is small, identification is therefore fast – carried out in real time. A two-stage neural network was employed. The first stage consisted of a backpropagation network optimized for feature extraction, specifically the extraction of locations of ridge endings and bifurcations in a high resolution digitized image of the fingerprint. During training of the backpropagation network to perform this task, noise – both spatial noise and brightness perturbation - was applied to enhance system robustness. Neural networks are particularly well suited to identifying underlying trends buried within noisy data, hence their selection for the fingerprint system. The second stage consisted of an adaptive resonance theory network (ART) [7] used for matching the features identified by the first stage to a single record in the template database. The approach taken was to search the database for the closest match. ART networks are known to exhibit considerable stability – after a collection of input patterns has been learned, categorization of those patterns is not perturbed by an arbitrary barrage of new inputs. By selection of the appropriate architecture for the ART network, correct identification rates of 96% were achieved at penetration rates* of 100%.

2. Neural Networks

Backpropagation neural networks have a multi-layer feedforward architecture and are trained by the backpropagation learning rule. In the fingerprint identification system reported here, feature identification is carried out using a backpropagation network. The inputs to the network are the gray levels of each pixel in a digitized fingerprint. The desired outputs supplied are the locations of ridge endings and bifurcations. After sufficient training, the neural net learns to extract the locations of ridge endings and bifurcations in the fingerprint presented. This information is distilled down to a compact set of parameters presented to a second neural network for comparison with previously stored features. Fingerprint matching – essentially a pattern recognition task - is better resolved by a different neural architecture - adaptive resonance theory network (ART). ART [7] are neural networks that perform clustering by associating patterns with previously stored prototypes. Invented by Grossberg and Carpenter, they model neural activity by a set of continuous differential equations with the

* Penetration rate is average percentage of database searched during matching

objective of resolving the stability-plasticity dilemma: a network should be able to retain previously learned knowledge while still being responsive to novel data. ART networks have a minimum of two layers of nodes with feedforward connections from the first layer of input nodes to the second layer of output/prototype nodes. There are also feedback connections from output to input nodes. The input layer contains as many nodes as the size of the pattern vector while the second layer contains a variable number of nodes representing the number of clusters. Resonance is the process by which a new input vector is matched to one of the cluster prototypes stored in the second layer. Signals travel repeatedly between output and input layer until the output returns a pattern that is similar to the input. i.e. a match is discovered. If there is no match, a new cluster of patterns is formed around the new input – a process controlled by a user-controlled vigilance parameter.

3. Fingerprint Feature Identification & Matching Procedure

3.1 Feature Identification

High resolution gray scale fingerprint images having 256 levels of gray were obtained from the FVC2002 competition and loaded into an experimental database. For each print, a 625 pixel (25X25) region of the print was digitized and saved as a text file – a numerical representation of the fingerprint (see fig 1). The system is designed to extract features closest to the centroid of the print as these on the whole tended to be of better quality than features on the periphery of the print. Numbers in the text file denote brightness/gray levels ranging from "0" (white) to "255" (black), further ridge and bifurcation thresholds were defined using a minimum gray level of 128. Based on this, a ridge for example was clearly identifiable as an extended linear region of numbers greater than "128" surrounded by "0"s. Bifurcations were clearly identifiable as "T-junctions" in the ridge structure. Typical prints in the database contained a minimum of 6 minutae or features (# of ridge endings + # of bifurcations ≥ 6). A decision was made to select 3 ridges in each fingerprint, those 3 with the minimum perpendicular distance from the centroid of the print. For each ridge selected, four equally spaced points were selected each having 3 attributes: normalized Cartesian co-ordinates (x,y) and brightness level (0-255). Thus for each fingerprint presented, 3 ridges were selected for the extraction of 4 points/ridge each having 3 attributes/point giving a total of 36 features. Additionally, a decision was made to employ 3 bifurcations from each fingerprint – those 3 with the minimum Euclidean distance from the centroid of the fingerprint. As with ridge endings, 4 points were selected per bifurcation (see fig 1) comprising the center of the bifurcation and 3 additional points equidistant from it. Each bifurcation point was described by 3 attributes giving a total of 36 bifurcation features. Thus each 25X25 pixel fingerprint was associated with 72 distinctive feature data items, 36 of which were associated with ridges and 36 with bifurcations. To ensure robustness of the system, i.e. noise tolerance, noise was added to fingerprint images through spatial and brightness perturbation of digitized fingerprint text file. Perturbation applied was consistent with blurring and small rotations of each fingerprint. Supervised learning techniques used to train the backpropagation net in the presence of noise ensured that a given noise-free fingerprint and its perturbed or noisy versions resulted in extraction of identical features (bifurcation and ridge ending data).

3.2 Fingerprint Matching

Automatic fingerprint identification requires that the input fingerprint be matched with one authorized fingerprint in the database with a high degree of confidence. This is a very challenging task, heavily dependent on quality of original fingerprint – in fact false match errors are often due to poor quality fingerprints which result in erroneous feature extraction. Most matching algorithms compare features of two fingerprints and return a degree of similarity (0-100%). Many matching approaches are in use today including correlation based techniques [8] and neural network methods [1,2]. The novel neural network approach presented here exploits the adaptive resonance theory (ART) network paradigm – particularly ART's capability to compare an input vector and a previously established set of authorized prints stored as patterns or categories with plasticity and stability by virtue of the vigilance parameter. A high vigilance means that any differences will establish a new category, while a low vigilance means that input queries are placed in existing categories. The fuzzy ART net used (advanced form of ART network for classification problems) accepts the feature information output by the backpropagation network and performs a one-to-many search in the template database. As it searches, the fuzzy ART net uses its match tracking subsystem to gradually modify vigilance until either a match is made or NO MATCH output declared.

4. Results

A core database of 30 raw unperturbed fingerprints was digitized, then an additional 300 fingerprints generated from these after random perturbation with spatial and brightness (gray-level) noise ranging from 0-10% consistent with rotation and blurring. To complete the database, a further 270 fingerprints not related to the core set was included. Thus a total of 600 fingerprints were available for training and testing the backpropagation feature extractor. 80% of these fingerprints were used to train a 625-100-72 backpropagation network for feature extraction (remaining 20% fingerprints were reserved for test/validation). The Neuralworks Professional II Plus software (version 5.3) was employed. A 625-120-72 backpropagation network architecture was experimentally found to produce optimal results with minimal rms error – 0.027 for training and 0.047 for test after 120,000 random presentations of the data. Figure 2 is a block diagram of the two-tier system of serially connected neural networks employed in the fingerprint identification system. Once trained, the backpropagation network was able to output with 97% accuracy a 6 X12 matrix of features corresponding to data associated with 3 ridge endings and 3 bifurcations as described in section 3. A typical feature matrix for a single bifurcation - 36 elements in total - extracted by backpropagation network for a randomly selected fingerprint in the database is shown in table 1.

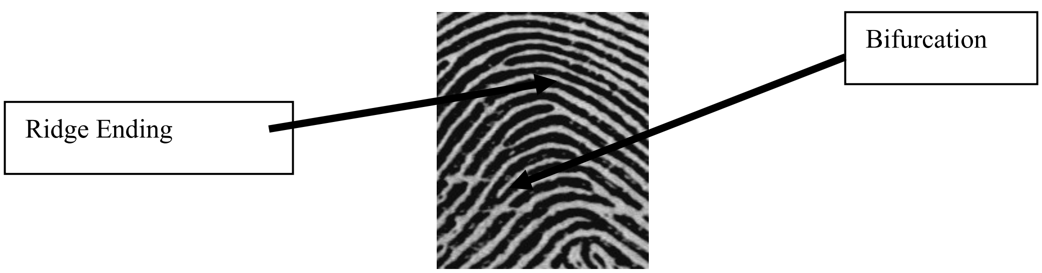
The fuzzy ART network is supplied with a feature matrix as input in order to generate an output which is the index of a matching template 1-30 (or 0 for NO MATCH). Stored prototypes in the fuzzy ART network are the feature matrices of all authorized fingerprints. The fuzzy ART network was created with 72 processing elements (PEs) in the input layer, 120 PEs in the category layer and one PE in the output layer (since objective is to find the single closest match to the input query).

Beginning with a baseline vigilance parameter of 0.12 and an error tolerance of 10^{-4}, , the fuzzy ART network was trained using 80% out of the 600 feature sets output by the backpropagation network. Template fingerprints in the ART training database were uniquely numbered from 1 to 30. Data was presented 70,000 times in random order until network was trained. Testing was then carried out using remaining 20% of fingerprint database. Matching accuracy was high - 96% probability of correct matching - was achieved at 100% penetration rate.

5 Conclusions

The work reported here demonstrates the efficacy of serially connected backprop and fuzzy ART neural networks for fingerprint identification in the presence of noise. A backpropagation network successfully extracted locations of minutae (ridge endings and bifurcations) in the presence of noise consistent with blurring and spatial perturbation. A fuzzy ART network was used to perform the task of matching the extracted features to a single fingerprint in a template database whereupon a correct match was obtained with 96% probability.

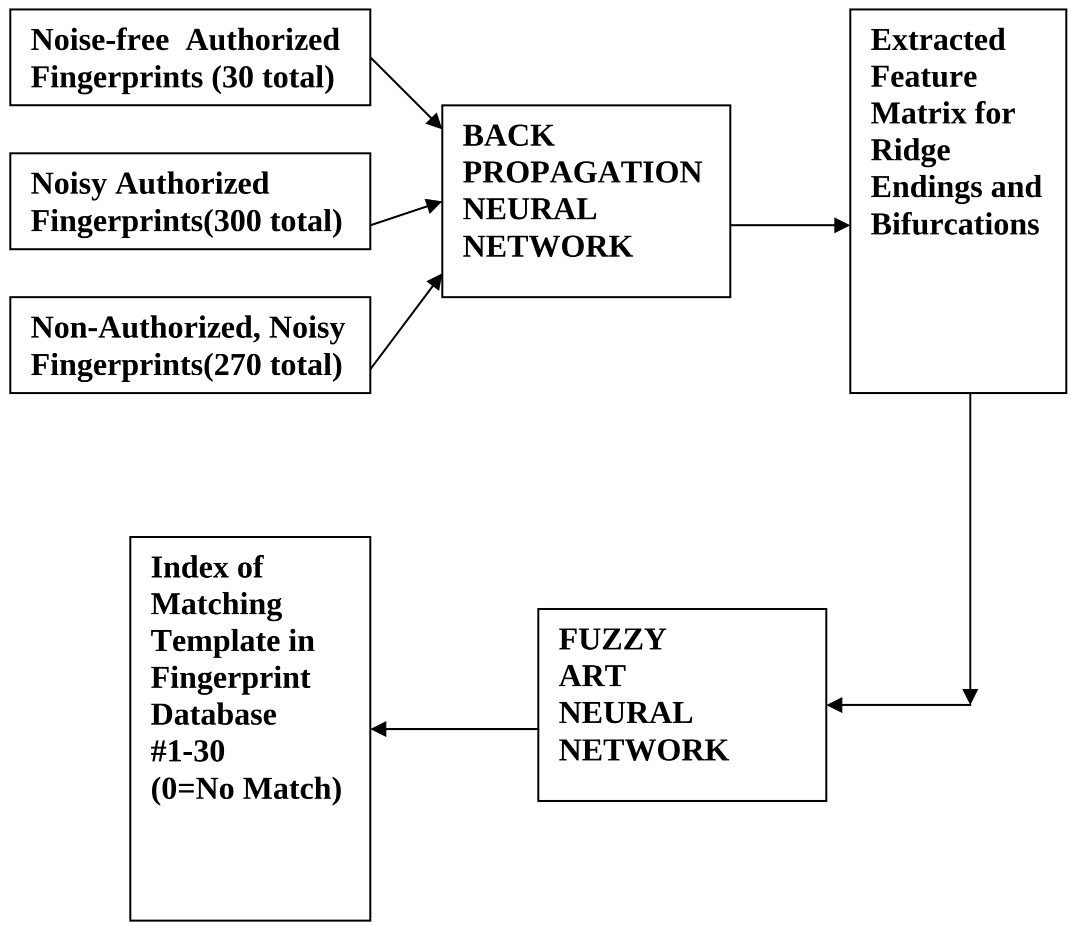
Fig. 1: Sample of Fingerprint & Digitized Equivalent



12	13	225	15	10	255	18	8	255	21	6	255	12	14	255	9	15	225	6	17	255
12	13	225	15	10	255	18	8	255	21	6	255	12	14	255	9	15	225	6	17	258
12	4	255	9	2	255	6	2	255	3	2	255	11	6	255	8	7	255	5	11	255
12	4	255	9	2	255	6	2	255	3	2	255	11	6	255	8	7	255	5	11	255
10	11	225	13	10	255	16	8	255	19	7	255	11	13	255	14	12	255	17	11	225
10	11	225	13	10	255	16	8	255	19	7	255	11	13	255	14	12	255	17	11	225
14	18	255	17	17	255	20	17	255	23	16	255	14	20	255	17	21	225	20	23	255
14	18	256	17	17	254	20	17	255	23	16	255	14	20	255	17	21	225	20	23	256
13	21	225	10	21	255	7	21	255	4	21	225	13	11	255	16	10	255	19	8	255
13	21	225	10	21	255	7	21	255	4	21	224	13	11	255	16	10	255	19	8	255
12	2	225	9	2	255	6	4	255	3	7	255	5	10	255	8	8	255	11	6	255
12	2	222	9	2	255	6	4	255	3	7	254	5	10	255	8	8	254	11	6	255
15	2	255	12	2	255	9	2	255	6	3	225	12	6	255	9	6	255	6	7	255
15	2	256	12	2	255	9	2	256	6	3	224	12	6	260	9	6	255	6	7	256

NSTI-Nanotech 2008, www.nsti.org, ISBN 978-1-4200-8504-4 Vol. 2

Fig 2 Feature Identification (Backpropagation Learning) and Matching (Fuzzy Art)



X (mm)	Y (mm)	Brightness (0-255)
6	15	205
14	24	204.9
13	18	255
20	32	208
14	7	255
2	24	254.9
3	18	69
4	32	255
17	11	255
21	6	254.9
33	18	69
14	48	255

Table 1: Typical Extracted Partial Features for single bifurcation

5 References

[1] R. Cappelli, D. Maio, D. Maltoni, J.L. Wayman and A.K. Jain, *"Performance Evaluation of Fingerprint Verification Systems"*, IEEE Transactions on Pattern Analysis Machine Intelligence, vol.28, no.1, pp.3-18, January 2006.

[2] T. Andrew and M. David, Integrated Wavelet and Fourier-Mellin invariant feature in fingerprint verification system, Proc. 2003 ACM SIGMM Workshop on Biometrics, pp 82-88, 2003

[3] R. Cappelli, A. Lumini and D. Maio, *"MKL-tree: a hierarchical data structure for indexing multidimensional data"*, in proceedings 13th International Conference on Database and Expert Systems Applications (DEXA2002), Aix en Provence (France), pp.914-924, September 2002

[4] Scheidat et al, *Parameter optimization for biometric fingerprint recognition using genetic algorithms,* International Multimedia Conference, Proceeding of the 8th workshop on Multimedia and security, pp 130-134, 2006

[5] Clancy et al, *Secure smartcard-based fingerprint authentication,* Proc. 2003 ACM SIGMM Workshop on Biometrics, pp 45-62, 2003

[6] A. Antonelli, R. Cappelli, D. Maio and D. Maltoni, *"Fake Finger Detection by Skin Distortion Analysis",* IEEE Transactions on Information Forensics and Security, vol.1, no.3, pp.360-373, September 2006

[7] Carpenter and Grossberg, "*The Art of adaptive pattern recognition by a self-organizing neural network*"' Computer, March, 77-88, 1988

[8] Maltoni et al, "Handbook of Fingerprint Recognition", Springer,2003