

ANN for Overlapped Fingerprint Authentication

Neha

Dept. of Electronics & Telecommunication

MIT, COE , Pune ,Maharashtra

Prof. P. P. Gundewar

Dept. of Electronics & Telecommunication

MIT, COE, Pune , Maharashtra

ABSTRACT:

The design and implementation of an automatic identity authentication system which uses a database of overlapped fingerprint to establish the identity of an individual. In the field of science, biometric is used for recognizing the identity of a person. The proposed algorithm is for separation and identification of one of the fingerprint from the overlapped fingerprint image. Considering the fingerprint as an image and create the database for all the images. After creation of the database the input fingerprint image will be compared for perfect matching with the database templates to recognize the identity. The result of this research work will achieve a good performance on these databases. Finally Results we will analyzed between input and recognized fingerprint image using Region of interest (ROI), training plot (between the no. of targets), Regression.

KEYWORDS:

ANN, ROI, Training plot, Regression.

INTRODUCTION

The human fingerprint is one of the most reliable ways to identify a person, as no two fingerprints from different persons are the same. Through the years the police were known as the major user of fingerprints in their quest to identify criminals. Due to the large volume of fingerprints and recent advances in technology, there has been increasing interest in automatic classification of fingerprints. An example of an application which is ideally suited for automatic fingerprint recognition is access control. Normal methods of fingerprint recognition use the small unique features (known as minutiae) in the fingerprint pattern to identify the fingerprint. Features such as minutiae, crossover, core, burification, delta, ridge ending, island, pore.

Many fingerprint classification methods have been proposed till now like orientation field flow curves method and quality based method Few of them shows graph based representation and few of them shows structural representation In this paper we have use a standard fingerprint database to classify fingerprint images into six classes arch, tented arch, right loop, left loop, whorl and twin loop using back propagation algorithm.



Fig 1: Overlapped fingerprint image

Fig. 1 shows an overlapped fingerprint image extracted by a well-known commercial fingerprint recognition algorithm, This example indicates that overlapped fingerprints constitute a serious challenge to the state-of-the-art fingerprint recognition algorithms. Manually marking features in overlapped fingerprints is also very difficult even for latent experts. Although a basic Fourier domain band-stop filtering technique can be used to

remove overlapping repetitive lines in latent images separating overlapped fingerprints, which are not composed of straight lines, is much more complicated. Therefore, it is desirable to develop a technique that can automatically separate overlapped fingerprints into their individual fingerprints to improve the matching performance.[6]

A. EXISTING SYSTEMS

Ratnakaranandraokharade, M.S. Kumbhar, [1] Michigan State University and the National Institute of Standards and Technology NIST 9 fingerprint data bases have been used to estimate the performance numbers. The experimental results reveal that system can achieve a good performance on these data bases. Also have demonstrated that our system satisfies the response-time requirement. A complete authentication procedure, on average, takes about 1.4 seconds on a Sun ULTRA 1 workstation (it is expected to run as fast or faster on a 200 HMz Pentium 7).

Arun Jain, Mukesh Kumar, Anil Kumar, [2] A pattern-recognition system that is used to identify a user. There are three levels of computer security schemes. Level 1 relies on something a person carries, such as an ID badge with a photograph or a computer cardkey. Level 2 relies on something a person knows, such as a password or a code number. Level 3, the highest level, relies on something that is a part of a person's biological makeup of behavior, such as a fingerprint, a facial image, or a signature.

Anil jain and Lin Hong, [3] In the proposed system on two sets of fingerprint images. Set 1 contains 10 images (380*380) per finger from 18 individuals for a total of 180 images, which were captured with a scanner manufactured.

Fanglin Chen, JianjiangFeng, Anil K. Jain, Jie Zhou and Jin Zhang [5] proposed a fingerprint biometric system based on texture descriptors. For this, it requires an image of high PSNR value so that complete features must be extracted and all matching points will be obtained. For this, it uses an contrast based enhancement algorithm for improving PSNR value. We have considered the factors relating to obtaining high performance feature points detection algorithm, such as image quality, separation, image improvement and featuredetection. Commonly used features for increasing fingerprint image quality are features vectors and local orientation. Accurate separation of fingerprint ridges from noisy background is necessary. A pre-processing method containing of field orientation, frequency estimation, filtering, segmentation and enhancement is performed. Image normalization is also done for equalizing the features values. Also area of interest is also found out. All simulations are done in MATLAB tool.

B. EXISITING SOLUTIONS AS AN APP

After Fingerprint recognition is widely used in various applications ranging from law enforcement and international border control to personal laptop access. Almost all law enforcement agencies worldwide routinely collect fingerprints of apprehended criminals to track their criminal history .To enhance border security in the United States, the US-VISIT program acquires fingerprints of visa applicants to identify high profile criminals on a watch list and detect possible visa fraud. India'sUIDAI project was initiated to issue a unique 12-digit identification number to each resident.

Fingerprint recognition systems are now pervasive in our daily life. Disney Parks, for example, captures fingerprints of visitors when they initially enter the park to link the ticket to the ticket holder's fingerprint. Fingerprint verification is performed whenever the same 5 ticket is presented for reuse to prevent fraudulent use of the ticket (e.g., sharing of a ticket by multiple individuals). Many automated teller machines (ATMs) in Brazil use fingerprint recognition as a replacement for personal identification numbers (PINs). Also, several laptop computer models are equipped with fingerprint sensors and authenticate users based on their fingerprints. [7]

C. FINGERPRINT CLASSIFICATION

Fingerprint classification involves (i) the extraction of features of given fingerprint image, (ii) Feature Orientation (iii) labeling of each oriented fingerprint in to six class like arch, tented arch, right loop, left loop, twin loop, whorl. The fingerprints have been traditionally classified into categories based on information in the global patterns of ridges. Fingerprint classification provides an important indexing mechanism in a

fingerprint database. An accurate and consistent classification can greatly reduce fingerprint matching time from a large database. We present a fingerprint classification algorithm which is able to achieve an accuracy better. Efforts in automatic fingerprint classification have been exclusively directed. The fingerprint classification architecture that has shown classification of fingers into the six classes. It consists of user interface to provide interaction for user with system, the system database is the collections of the recorded data and enrolment module and authentication module is present for system input and verification of the fingerprint image given by user.

Below figure 2 depicts the block diagram of the complete system :

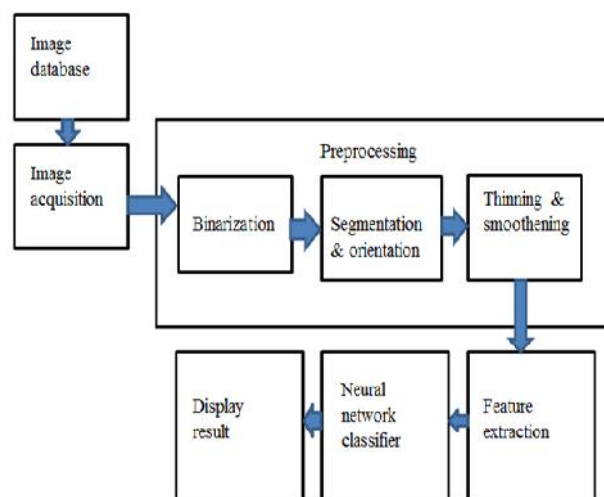


Fig 2: Block diagram of the system

In table 1, the image is uploaded from the data base. From the given 10 samples one of image is selected and browse it. The image is browsed in the GUI (graphical user interface).

Image Acquisition The first step in the minutiae extraction stage. They have high efficiency and acceptable accuracy except for some cases that the users finger is too dirty. So in this project the samples are taken from Livdet- Fingerprint liveness detection from where the researchers take the samples for testing purposes. Since various data acquisition conditions such as impression pressure can easily change one type of minutia into the other, most researchers adopt the unification representation for both termination and bifurcation.

Binarization: Fingerprint image binarization is to transform the 8-bit Gray fingerprint image to a 1-bit image with 0-value for ridges and 1-value for furrows. After the operation, ridges in the fingerprint are highlighted with black colour while furrows are white. A locally adaptive binarization method is performed to binarized the fingerprint image.

Segmentation and orientation:

Segmentation and orientation in general, only a ROI is useful to be recognized for each fingerprint image. The image area without effective ridges and furrows is first discarded since it only holds background information. Then the bound of the remaining effective area is sketched out since the minutia in the bound region is confusing with those spurious minutia's that are generated when the ridges are out of the sensor.

For directional map, orientation flow of estimation is done. The direction for each block of the fingerprint image with $W \times W$ in size is estimated. The algorithm is the gradient values along x- direction and y-direction for each pixel of the block is calculated.

Thinning and smoothing:

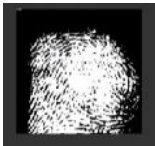
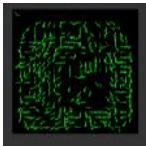



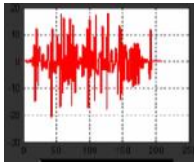
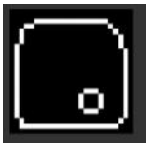
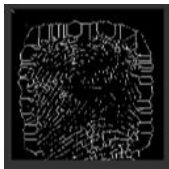
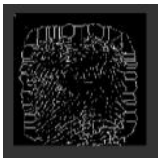
Ridge thinning is to eliminate the redundant pixels of ridges till the ridges are just one pixel wide. An iterative, parallel thinning algorithm is used. In each scan of the full fingerprint image, the algorithm marks down redundant pixels in each small image window. And finally removes all those marked pixels after several

scans. The thinned ridge map is then filtered by other three operations to remove H breaks isolated points and spikes.

Given two set of minutiae of two fingerprint images, the minutia match algorithm determines whether the two minutia sets are from the same finger or not. An alignment based match algorithm is used.

Feature extraction Feature extraction is the process to extract important attribute from the input image. Propose a distributed and load-balancing framework for fingerprint identification, is done by Gabor filter. This proposal is two-fold: the feature extraction is carried out on the Hadoop Image Processing Interface, and the features are stored. [4]

Table 1:Methodology Used

ORIGINAL IMAGE	ISOLATION	FEATURE EXTRACTION	CLASSIFICATION
 Overlapped fingerprint	 orientation flow	 Extracted feature	 Prescribed result genuine or fake
	 Reconstructed edges and broken curves	 Feature plot through Gabor filter	
	 Overlapped part	 Extracted features	
	 Reconstructed image		

Gabor filter: To compute the ridge width and valley width from the discrete signal x-signature more accurately, we resort to a fitting method to acquire the first and second order derivatives. Based on the trade-

off between accuracy and efficiency, the discrete Chebyshev polynomials introduced by Haralick (1984) and Tico and Kuosmanen (1999) are employed to perform the fitting. The zero crossings of the second order derivatives and magnitude of the first. Order derivatives are together considered to determine the ridge width and valley width. In other words, the distance between two zero crossings of the second order derivatives is regarded as the ridge width or valley width if the magnitude of the corresponding first order derivative is larger than a threshold. Then, the signs of the second order derivatives specify whether it is ridge or valley. Thereby, the information of ridge width W_r and valley width W_v is associated to each block. In application, ridge width and valley width fall into a certain interval. If exceeding the interval, they are replaced by the mean of those available in neighbouring eight blocks. [5]

Artificial neural network: an artificial neural network is used to do the classification. In this network, number of fingerprints in the input layer have been taken as 10 (samples), number of basis on the one which is selected in the hidden layer as and thus it is compared one by one with the other samples.

RESULTS:

Artificial neural networks can be defined as a group of interconnected neurons used for information processing as a computation model. It is an adaptive system capable of transforming its arrangement according to input and output sequence that flows in the network.

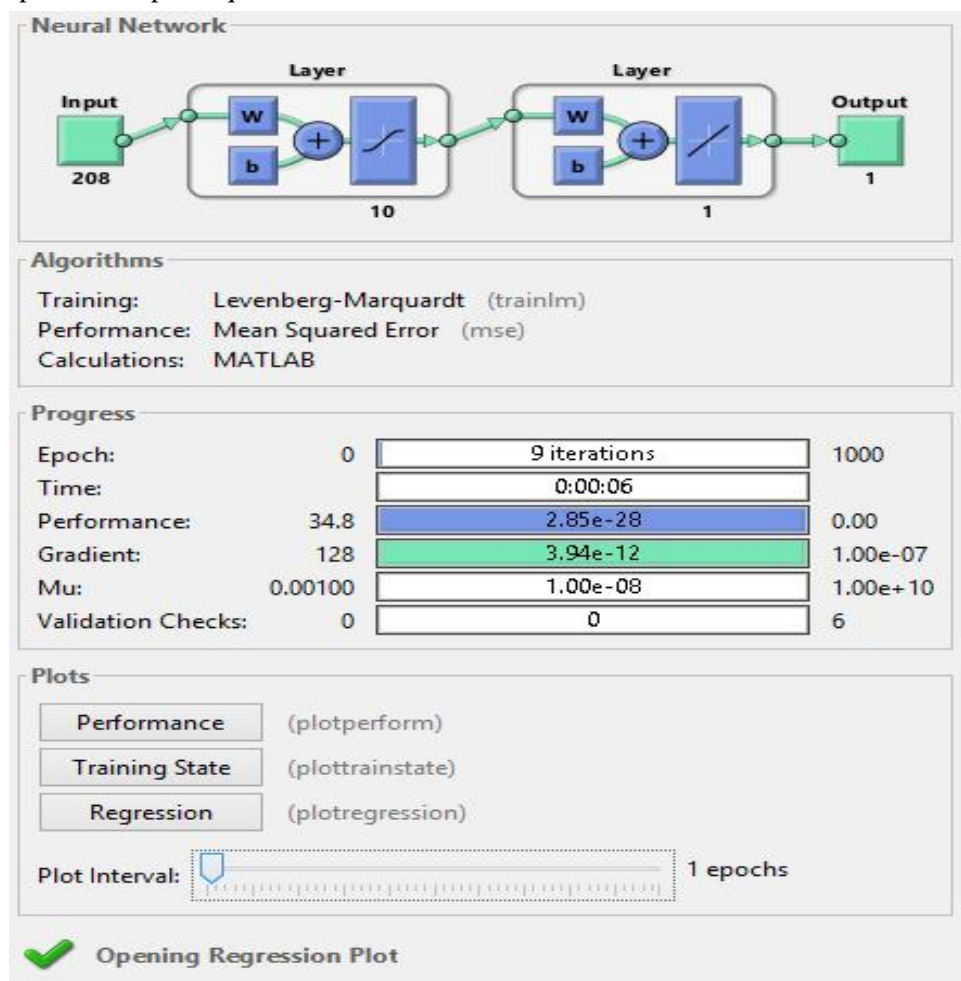


Fig 3: Neural network

1. The Output graph shows clear overlap among the values expected, and the values computed

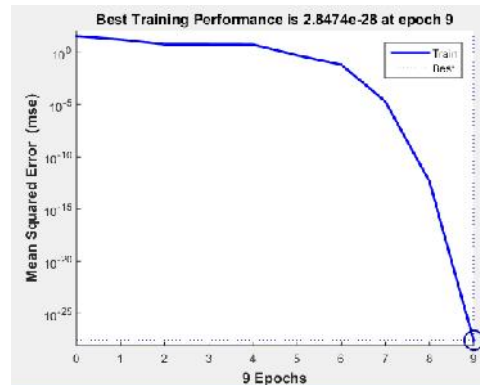


Fig 4: Performance graph

2. Time to train the network with the solution dataset that we have with us. After that simulate the network with training data set to see whether the answers match with expected values.

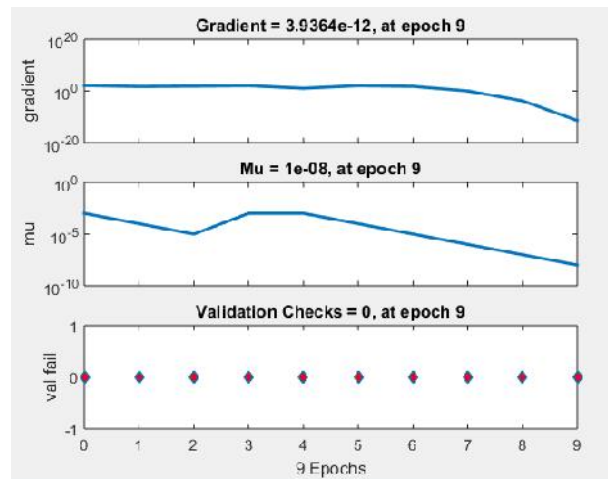


Fig 5: Training State

3. This is used to validate the network performance. ROC=1

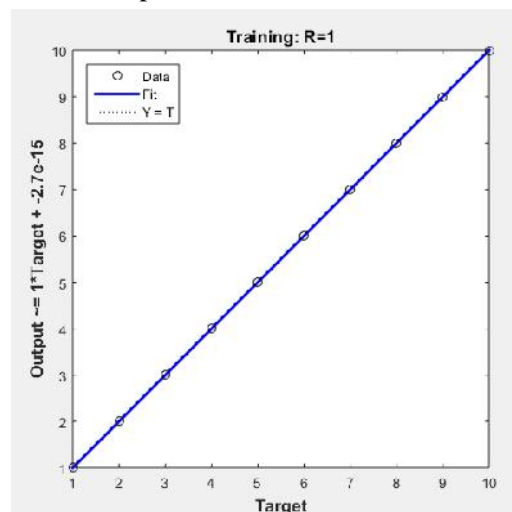


Fig 6: Regression graph

CONCLUSION AND FUTURE SCOPE:

Proposed an algorithm for separating overlapped fingerprints, which outperforms the state of the art method in both accuracy and efficiency. In addition, our method does not require the information of singular points, and thus costs less human labor. At the end through classification which done by neural network tool, states that the predicted class is genuine or fake. The class is predicted on the basis of region of performance graph, training state and regression graph. The FAKE result shows that none of person's fingerprint is in the database or can say the distortion is too much because of which it cannot be recovered. In the prescribed algorithm the image of one of the overlapped fingerprint should be retrieve.

For future recommendation and development, the system should be improved to be more practical, dynamic and user-friendly. GUI for matching techniques which is the completion of this project can also be developed.

Apart from separating the two fingerprints in future we can recognize the fingerprint of a person in adult age but the record was taken in the childhood.

REFERENCES

- [1] Mr.Ratnakaranandraokharade, Mr. M.S. Kumbhar,"An Identity-Authentication System Using Fingerprints,"*International Journal of Engineering Research and Applications*,Vol. 2, Issue 6, November- December 2012, pp.303-311.
- [2] Arun Jain, Mukesh Kumar, Anil Kumar," A Proposed Architecture for Biometrics Fingerprint Recognition and Authentication Using NN Command Line," *International Journal of Advance Engineering and Research Development*, Volume 2,Issue 6, June -2015.
- [3] Anil Jain and Lin Hong,"On-line Fingerprint Verification,"*Pattern Recognition and Image Processing Laboratory*,Department of computer science Michigan State University East Lansing.
- [4] Ravi BhushanTiwari, Sanjay Sharma and Sidhu,"Biometric authentication using fingerprint,"*Youth Education and Research Trust*,J. Acad. Indus. Res. Vol. 1(8) January 2013.
- [5] Yuan Shi, JianjiangFeng, Jie Zhou,"Separating Overlapped Fingerprints Using Constrained,"*Relaxation Labeling Department of Automation*, Tsinghua University, Beijing, China. 2014
- [6] Fanglin Chen, JianjiangFeng, Anil K. Jain, Jie Zhou and Jin Zhang, "Separating Overlapped Fingerprints", *IEEE Transactions On Information Forensics And Security*, vol. 6, no. 2, june 2011
- [7] Mr. Abhay N. Adapanawar,"Finger print recognition using MATLAB," 2011