Fingerprint Verification System – A Fusion Approach

M.Mani Roja
Research Scholar
Sant Gadge Baba Amravati University
Amravati

Sudhir Sawarkar, Ph.D
Principal
Datta Meghe College of Engineering
Mumbai, India

ABSTRACT

The primary objective of this paper is to implement fingerprint recognition system using minimum resources for online application. Fingerprint recognition is done using minutiae extraction in time domain method and using Discrete Cosine Transform (DCT) in frequency domain method. The fingerprint image was restricted to size of 256 x 256 pixels. The True Acceptance rate (TAR) has been increased using fusion between time domain method and frequency domain method.

General Terms

Biometrics, Pattern Recognition

Keywords

Minutiae, Discrete Cosine transform, Fusion

1. INTRODUCTION

The overall objective of this paper is to develop a finger print recognition system based on minutiae marking algorithm. A point in the fingerprint image is designated as a minutia [1-3] if it belongs to an ending, isolation, crossing or bifurcation of a ridge. Over the recent decades, the role of image in communication of information has been increasing steadily. Advances in technology to capture, transfer, and store and display images has made it technologically and economically feasible to use images as means of communication. Some of the various applications of fingerprint recognition system are: E fund transfer, ATM, E-commerce, Customs and immigration, Smart cards and voter cards, driving license, personalized door locks, and Railway reservations.

Biometrics are used to prevent unauthorized access to ATM, cellular phones , laptops , offices, cars and many other security concerned things. Biometric have brought significant changes in security systems making them more secure than before, efficient and cheap. They have changed the security system from what you remember (such as password) or what you possess (such as car keys) to something you embody (retinal patterns, fingerprints, voice recognition). Biometrics is the science of verifying the identity of an individual through physiological measurements or behavioural traits.

Fingerprints recognition has been present for a few hundred years. Due to tremendous research, this field has reached such a point where the purchase of fingerprint security system is quite affordable. For this reason these systems are becoming more widespread in a variety of applications. Fingerprints offer an infallible means of personal identification. The science of fingerprint Identification stands out among all other forensic sciences for many reasons, including the following [1-4]:

•Has served all governments worldwide during the past 100 years to provide accurate identification of criminals. No two fingerprints have ever been found alike in many billions of human and automated computer comparisons. Fingerprints are the very basis for criminal history foundation at every police agency on earth.

•Continues to expand as the premier method for identifying persons, with tens of thousands of persons added to fingerprint repositories daily in America alone - far outdistancing similar databases in growth.

•Other visible human characteristics change but fingerprints do not.

1.1 Literature Review

Fingerprints have been scientifically studied for many years in our society. The characteristics of fingerprints were studied as early as 1600s.Meanwhile, using fingerprints as a means of identification, first occurred in the mid-1800s. Sir William Herschel, in 1859, discovered that fingerprints do not change over time and that each pattern is unique to an individual [3, 4]. With these findings, he was the first to implement a system using fingerprints and handprints to identify an individual in 1877. By 1896, police forces in India realized the benefit of using fingerprints to identify criminals, and they began collecting the fingerprints of prisoners along with their other measurements.

As fingerprints began to be utilized in more fields, the number of requests for fingerprint matching began to increase on a daily basis. At the same time, the size of the databases continued to expand with each passing day. Therefore, it soon became difficult for teams of fingerprint experts to provide accurate results in a timely manner. In the early 1960s, the FBI, Home Office in the United Kingdom, and Paris Police Department began to devote a large amount of resources in developing automatic fingerprint identification systems. These systems allowed for an improvement in operational productivity among law enforcement agencies.

1.2 Advantages of Fingerprint Recognition

Following are the various advantages of fingerprint system [1-4]

- Fingerprints do not change over time.
- Fingerprints stop unauthorized access.
- All fingers are unique, which allows each person to have ten easy uses of identifiers.
- Base of all world-wide identification.
- Fast and easy to use.
- We do not forget our fingers.
- Users respect them, fraudsters are afraid of them.
- Protects privacy.

Fingerprints are imprints formed by friction ridges of the skin and thumbs [5]. They have long been used for identification because of their immutability and individuality. Immutability refers to the permanent and unchanging character of the pattern on each finger. Individuality refers to the uniqueness of ridge details across individuals; the probability that two fingerprints are alike is about 1 in 1.9x10^{15}. Each individual has its own fingerprint with permanent uniqueness. That's why fingerprints have been used for identification and forensic investigation for a long time**.**

Fingerprints are graphical flow-like ridges present on human fingers. They are fully formed at about seven months of fetus development and finger ridge configurations do not change throughout the life of an individual except due to accidents such as bruises and cuts on the fingertips. This property makes fingerprints a very attractive biometric identifier. Fingerprint recognition system can be separated into two categories:

Identification: Identification system recognizes an individual by searching the entire template database for a match [5]. It conducts one-to-many comparisons to establish the identity of the individual. In an identification system, the system establishes a subject's identity (or fails if the subject is not enrolled in the system database) without the subject having to claim an identity. The identification process results in establishing the identity of the user, that is, answering the question, "Who is this person?"

Authentication: This is the process of identifying a person using one-to-one (1:1) matching with their stored biometric template and validating that the claimed identity belongs to the user [3]. Authentication answers the question, "Is this person who she says she is?" This process is used in applications for authorizing legitimate users access to secure facilities, for managing time attendance, and for verifying users during financial transactions to reduce fraud.

2. PROPOSED SYSTEM

A fingerprint recognition system is done using three steps known as Image acquisition, Minutiae extraction and Minutiae matching. The block diagram of basic fingerprint recognition system is shown in fig 1.

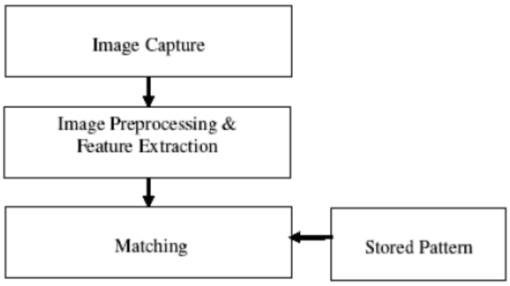


Fig 1: Fingerprint Recognition System

In Image acquisition, sensors are widely used. We have used SecuGen Hamster Fingerprint Reader for collecting fingerprints. SecuGen provides biometric solutions for physical and network security employing advanced fingerprint recognition technology.

Fig 2: SecuGen Hamster Fingerprint Reader

Minutiae extractor requires a pre and post processing steps which includes image resizing, image binarization, thinning and crossing number algorithm. Minutiae matching compare the two images. If both the images are from the same fingerprint they are matched otherwise they are unmatched. The overall process is implemented using MATLAB7. Each of these steps and sub-section are explained in detail below.

2.1 Pre-processing Steps

The performance of a fingerprint recognition system basically depends upon the quality of the input image. Therefore to ensure the accurate working of the system, the image is first resized to size (256*256) pixels using inbuilt MATLAB function 'imresize' and then further image processing techniques are applied on it.

2.2.1 Fingerprint Image 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. First, a threshold value from the image is selected using 'thresholding algorithm'. This value is then used to convert the grey image to a black and white image. The value of pixel which is less than the above threshold value calculated is taken as 0 representing the ridge in black colour.

A value of the pixel in the image which is greater than the threshold value calculated is then converted to 1 representing the white colour valley or furrow. The following image shows the image before and after binarization.

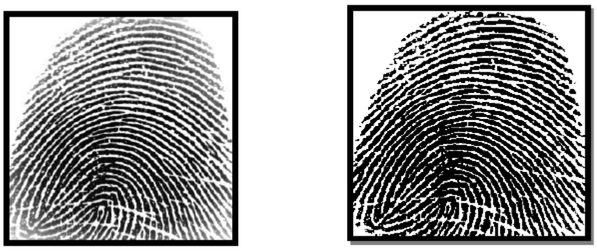


Fig 3: Finger print Images before and after binarization

2.2.2 Finger print Ridge Thinning

Ridge Thinning is used to eliminate the redundant pixels of ridges till the ridges are just one pixel wide. This function repeats operation on the ridges until they are one pixel wide and are suitable for minutiae extraction phase. The image obtained after thinning operation is shown in fig 4.

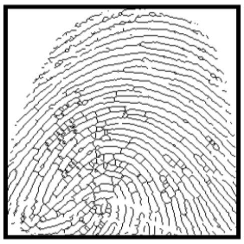


Fig 4: Fingerprint Image after thinning

3. IMPLEMENTATION STEPS

3.1. Time Domain Method

To implement this method, we have considered four different features-namely ending, bifurcation, isolation and crossing points. To calculate the count of each feature in a fingerprint image, we have used 3*3 structuring elements which run through the entire 256*256 image [5].For comparison we use Euclidean distance model which calculates the Euclidean distance between feature vector of the test signature and feature vector of the database. The formula for Euclidean distance is given as follows:

Let A (a_1, a_2 ... a_n) and B (b_1, b_2 …b_n) are two vectors of size n. We can calculate distance by equation 1 as

$$d = \sqrt{\sum_{i=1}^{n}(a_i - b_i)^2}$$

(1)

3.2 Frequency Domain Method

For frequency domain method, we have considered DCT (Discrete Cosine Transform) [6]. The locations of four minutiae features in a particular fingerprint image are combined and represented by an image on which DCT is performed. DCT is a well-known signal analysis tool used in compression due to its compact representation power. It's known that Karhunen-Loeve transform (KLT) is the optimal transform in terms of information packing, however, its data dependent nature makes it infeasible to implement in some practical tasks. Moreover, DCT closely approximates the compact representation ability of the KLT, which makes it a very useful tool for signal representation both in terms of information packing and in terms of computational complexity due to its data independent nature. DCT helps separate the image into parts (or spectral sub-bands) of differing importance (with respect to the image's visual quality). The general equation for a 1D (*N* data items) DCT is defined by the following equation

$$F(u)=\sqrt{\left(\frac{2}{N}\right)}\sum_{i=0}^{N-1}A(i)*\cos\left(\frac{u(2i+1)\pi}{2N}\right)*f(i)$$

(2)

Where, f *(i)* is the input sequence and

$$A(i)=\frac{1}{\sqrt{2}}$$ for u = and it is 0 otherwise

3.2.1 Implementation Steps

The Implementation of DCT based approach consists of the following steps.

- • The database consists of set of images of 25 persons. We have collected 5 finger print samples of left hand thumb out of which three are used for training phase and 2 are used for testing the accuracy.
- • The entire images are resized to 256*256. Four different features are extracted from the image and then DCT is applied to the image, it is then scanned in zigzag manner. Thus for size 256*256 we have 65536 coefficients. Out of which only 32 coefficients are considered due to the energy compaction property of DCT. These coefficients are collected in Zigzag manner.
- • The DCT is carried out on the query image and Euclidean distances between query image and data base images are calculated and sorted.
- • The smallest Euclidean distance is taken into account and if this Euclidean distance belongs to the sample of same person then it is considered as authentic or else forge.

4. FUSION METHODOLOGY

Some of the limitations imposed by unimodal biometric systems like noise in sensed data, non-universality can be overcome by using multimodal biometric system. Multimodal biometric systems integrate information presented by multiple biometric indicators. In the context of biometrics, three levels of fusion schemes have been suggested [7, 8].

i) Fusion at Feature level: Each individual biometric process outputs a collection of features. The fusion process fuses these collections into a single feature set or vector.

ii) Fusion at score level: Each individual biometric process outputs a match score. The fusion process fuses these into a single score, which is then compared to the system acceptable threshold.

iii) Fusion at decision level: Each individual biometric process outputs its own Boolean result. The fusion process fuses them together by a combination algorithm such as AND, OR etc.

To increase the accuracy and reliability of the system we have considered decision level fusion method in which we have used 'OR' logic.

4.1. Algorithm

In OR logic, an image is said to be a match if it is getting matched from either time domain method or frequency domain method. If it gets matched with either of the approach, then its flag is set and then both the flags are 'OR'ed and its value is stored and if this value is set then it's a match or else a no match.

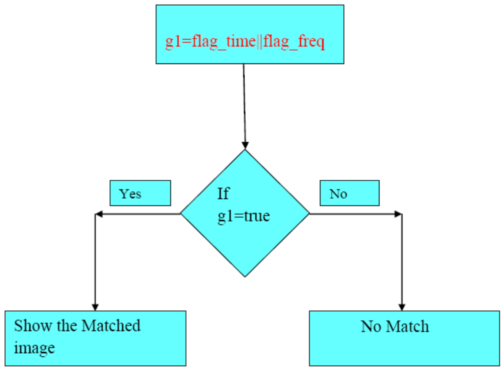


Fig 5: Algorithm for OR logic

5. RESULTS AND ANALYSIS

We have used three different methods of implementation and different results were observed based on features considered in
time domain method and DCT coefficients in frequency domain. In time domain method, we were able to get TAR of 58 %. Using DCT in frequency domain, we have got the better results of 92 %. According to the fusion algorithm, we were able to increase our results to 95%. If we compare in terms of time parameter, time domain technique needed least time as 3. 9 seconds and Fusion technique took the largest time as 19.9 seconds.

Table 1. Results of Fusion Approach

Method used	Time (secs)	Accuracy in %
Time domain	3.911304	58
Frequency domai	8.83	92
OR logic	19.9	95

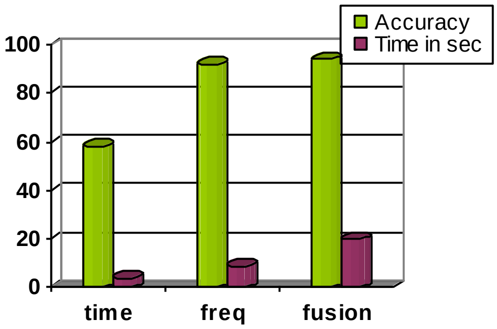


Fig 6: Comparison of Fusion approaches

Fig 7. shows the result corresponding to the acceptance of a true fingerprint and fig 8 shows the result when the access is denied.

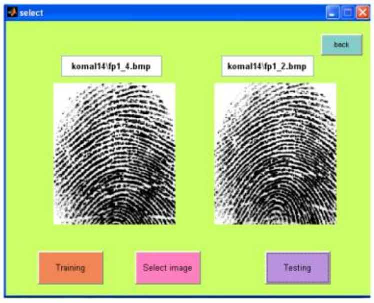
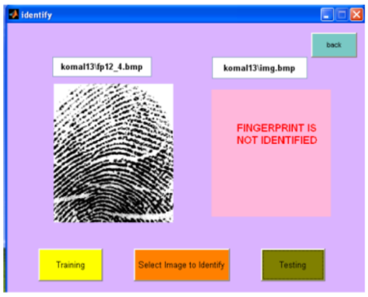


Fig 7: Successful Biometric Authentication



FINGERPRINT IS
NOT IDENTIFIED

Fig 8: Failure in Biometric Authentication

6. CONCLUSION

We have seen that fingerprint recognition system can be implemented using fusion between time domain method and frequency domain transform. We have also observed that accuracy of the system increases after using fusion method. The system developed still needs improvements for decreasing the time spent during fingerprint processing and the reduction in the number of false acceptances and true rejections made by the algorithm.

7. REFERENCES

[1] Anil K. Jain, Arun Ross and Salil Prabhakar, “An Introduction to Biometric Recognition”, Appeared in IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, Vol. 14, No. 1, January 2004.

[2] Arun Ross, Anil Jain, “Information fusion in Biometrics”. Pattern Recognition Letters 24 (2003) 2115–2125.

[3] D. Maltoni, D. Maio, A. K. Jain et S. Prabhakar, "Handbook of Fingerprint Recognition". New-York: Springer-Verlag, 2003. 1388, 1997.

[4] Jain, A.K., Hong, L., Bolle, R.,” On-line fingerprint verification”, IEEE Trans. Pattern Anal. Machine Intell. 1997 (4), 302–314.

[5] Salil Prabhakar, Anil Jain, Sharath Pankanti, “Learning Fingerprint Minutiae Location and Type”, IEEE Trans. Commun., Sept 09.

[6] C.Gonzalez ,Richard Woods, “Digital Image Processing”, 9th edition, Printice Hall, NewYork,Sept 09.

[7] Jain, A.K., Prabhakar, S., Chen, S., “Combining multiple matchers for a high security fingerprint verification system”, Pattern Recognition Lett. 20 (11–13)1999, 1371–1379.

[8] Arun Ross, Anil Jain, James Reisman, “A Hybrid Fingerprint Matcher”, IEEE Trans. Commun., Sept 09.

[9] Ravi, Raja, “Finger print recognition using minutia score matching”, International Journal of Engineering Science and Technology Vol.1(2), 2009, 35-42.