Decision Tree Based Fingerprint Authentication

Lukesh N. Jain, Dr. R. G. Karandikar

***Abstract*— While passwords may be stolen, guessed, or forgotten and tokens may be lost or stolen, biometric authentication systems attempt to link authentication directly to the user. The oldest and widely used form of biometric identification is the fingerprints. It has been widely used in many applications. Though much progress and research has been made in fingerprint based authentication systems, the performance is still low. The aim of this paper is to propose a system for performing decision tree based authentication using two fingerprints.**

***Index Terms*— Fingerprint, biometrics, minutiae, orientation.**

I. INTRODUCTION

Due to the development of computers and increased usage of internet, leakage of personal information has become a serious problem. Traditionally, passwords (knowledge-based security) and ID cards (token-based security) have been used to restrict access to systems. However these approaches have a number of disadvantages like tokens may be lost, stolen, forgotten, or misplaced; PIN may be forgotten or guessed by impostors [1]. Given the inefficiency of PIN based systems, it has become increasingly important that a person be identified on the basis of some bio-metric feature which is unique to him. Bio-metrics acts as an ideal solution to the problem of digital identification. Bio-metrics is the measurement of a unique physical characteristics and acts as an ideal solution to the problem of digital identification. Of all the Bio-metrics available, including face, iris, retina and voice identification, the Fingerprint recognition is one of the most convenient and foolproof.

Fingerprint recognition has been widely adopted for user identification due to its reliable performance, usability, and low cost compared with other biometrics such as signature, iris and face recognition. Fingerprints can be used for personal identification because fingerprints of an individual are unique and do not change throughout one's life [2]. The purpose of such schemes is to ensure that the rendered services are accessible by a legitimate user, and not anyone else. Secure identification is needed in many areas such as security systems, banking systems, criminal investigation, e-commerce, and electronic personal ID cards, etc. The advantages of Fingerprint bio-metrics over other identification procedures are: Each of our ten fingerprints is unique, different from another and from those of every other person [3]. Unlike passwords, PIN codes and smart cards that we depend upon today for identification our fingerprints are impossible to lose or forget, and they can never be stolen. We have ten fingerprints as oppose to two eyes, one face and one voice. Hence fingerprints have been used for centuries upon which one can make a claim on the uniqueness of each fingerprint [4].

The fingerprint recognition problem can be grouped into two sub-domains: one is fingerprint verification and the other is fingerprint identification. In addition, different from the manual approach for fingerprint recognition by experts, the fingerprint recognition here is referred as AFRS (Automatic Fingerprint Recognition System), which is program-based. Fingerprint verification is to verify the authenticity of one person by his fingerprint. The user provides his fingerprint together with his identity information like his ID number. The fingerprint verification system retrieves the fingerprint template according to the ID number and matches the template with the real-time acquired fingerprint from the user. Usually it is the underlying design principle of AFAS (Automatic Fingerprint Authentication System). Fingerprint identification is to specify one person's identity by his fingerprint(s). Without knowledge of the person's identity, the fingerprint identification system tries to match his fingerprint(s) with those in the whole fingerprint database [5]. It is especially useful for criminal investigation cases. And it is the design principle of AFIS (Automatic Fingerprint Identification System).

This paper explores the possibility of mixing two different fingerprints, pertaining to two different fingers, at the image level in order to generate a new fingerprint [6]. In the enrollment, two fingerprints are captured from two different fingers. We extract the minutiae positions from one fingerprint and orientation from the other. Based on this extracted information, a combined minutiae template is generated and stored in a database [7]. During authentication, the system requires two query fingerprints from the same two fingers which are used in the enrollment. Matching the two query fingerprints against a combined minutiae template will be performed using Decision tree method. This approach has following benefits: (a) it can be used to generate virtual identities from two different fingers (b) it can be used to obscure the information present in an individual's fingerprint image prior to storing it in a central database [8].

II. THE PROPOSED FINGERPRINT AUTHENTICATION SYSTEM

1. Main Menu:

The Main menu diagram of proposed fingerprint authentication system is shown in Figure 1. First the system reads the name of the person to be authenticated from the user and checks that name in the database. If the name if found in database it starts authentication; otherwise it starts with database entry.

Lukesh N. Jain, Department of Electronics & Telecommunication, K. J. Somaiya College of Engineering, Mumbai, India, 9029042754.
Dr. R. G. Karandikar, Department of Electronics & Telecommunication, K. J. Somaiya College of Engineering, Mumbai, India, 9869218446.

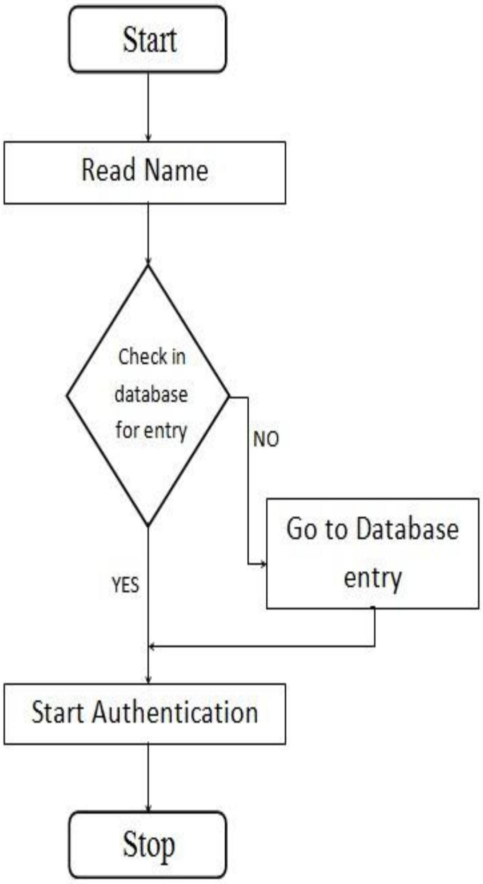


Figure 1: Main menu

2. Database entry:

The block diagram for database entry is shown in Figure 3. The detailed explanation of the same is as follows:

A. Read Index Fingerprint Image:

First the index fingerprint image obtained using image acquisition devices like scanners or other fingerprint reader devices is read from a specific path and then further processing is performed on that image. Figure 2 below shows the original index fingerprint image, on which further processing is performed.

Figure 2: Original index fingerprint image

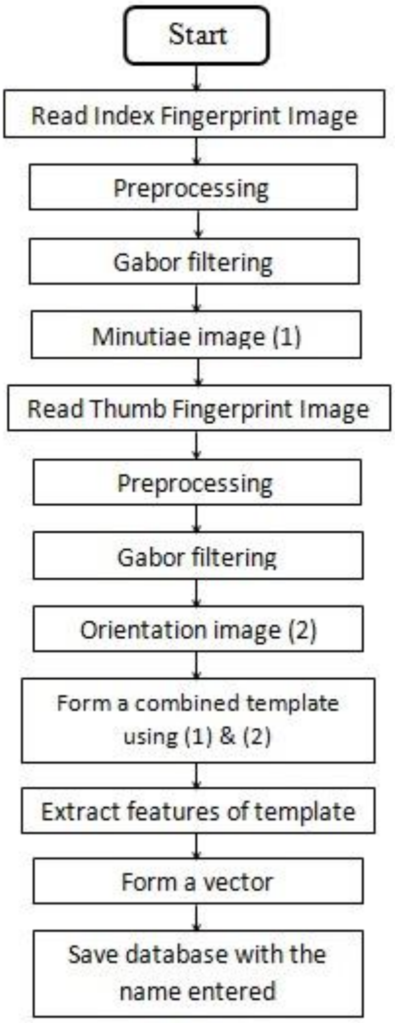

Start
Read Index Fingerprint Image
Preprocessing
Gabor filtering
Minutiae image (1)
Read Thumb Fingerprint Image
Preprocessing
Gabor filtering
Orientation image (2)
Form a combined template using (1) & (2)
Extract features of template
Form a vector
Save database with the name entered

Figure 3: Database entry

B. Preprocessing on index fingerprint image:

Preprocessing consists of converting an image into gray scale as shown below in Figure 4.

Figure 4: Preprocessed index fingerprint image

C. Gabor filtering on preprocessed index fingerprint image: In image processing, a Gabor filter, named after Dennis Gabor, is a linear filter used for edge detection. Gabor filters are used to obtain an enhanced fingerprint image. The filters are used as band pass filters to remove the noise and preserve true ridge/valley structures. Figure 5 below shows the image obtained after Gabor filtering.

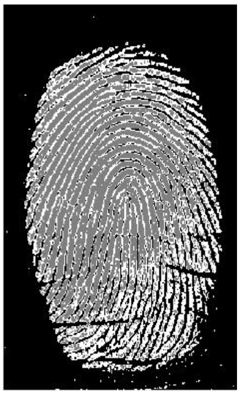


Figure 5: Gabor filtered index fingerprint image

D. Minutia image detection:

Minutiae are the major features of a fingerprint, so comparisons of one fingerprint with another can be made using them. In general, minutiae are characteristic points in a fingerprint image. The commonly used minutiae are ridge endings and ridge bifurcations. Figure 6 shows a minutiae image obtained for the original fingerprint image as seen in Figure 2.

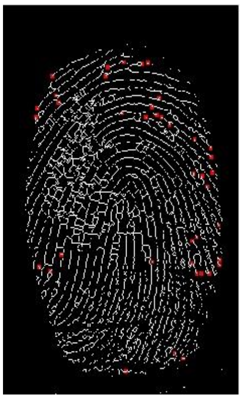


Figure 6: Minutiae image

E. Read Thumb Fingerprint Image:

The thumb fingerprint image obtained using image acquisition devices like scanners or other fingerprint reader devices is read from a specific path and then further processing is performed on that image. Figure 7 below shows the original thumb fingerprint image, on which further processing is performed.

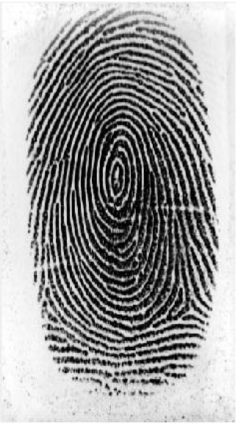


Figure 7: Original thumb fingerprint image

F. Preprocessing on thumb fingerprint image:

Preprocessing consists of converting an image into gray scale as shown below in Figure 8.

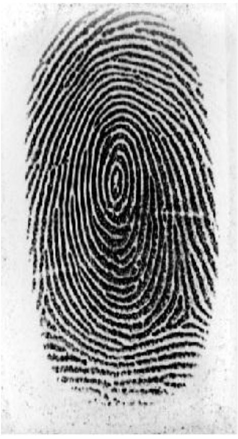


Figure 8: Preprocessed thumb fingerprint image

G. Gabor Filtering on preprocessed thumb fingerprint image:

Figure 9 below shows the image obtained after Gabor filtering.

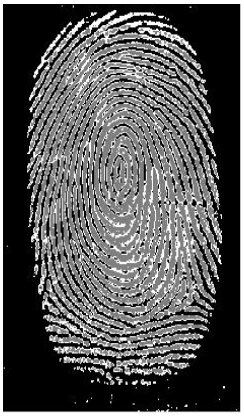


Figure 9: Gabor filtered thumb fingerprint image

H. Orientation image detection:

A major obstacle in fingerprint recognition is that the images obtained are not usually perfectly aligned. Usually rotation and displacement of some sort is evident. Attempting to compare two fingerprints with different orientations will affect the result significantly. To adjust for this, rotation of the input image is performed. Figure10 shows an orientation image obtained for the original fingerprint image as seen in Figure 7.

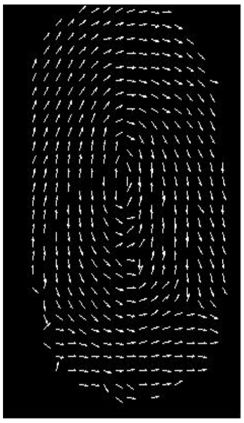


Figure 10: Orientation image

I. Combined template formation:

A combined template is formed by performing AND operation on minutiae image and orientation image. Figure11 below shows the image of combined template obtained.

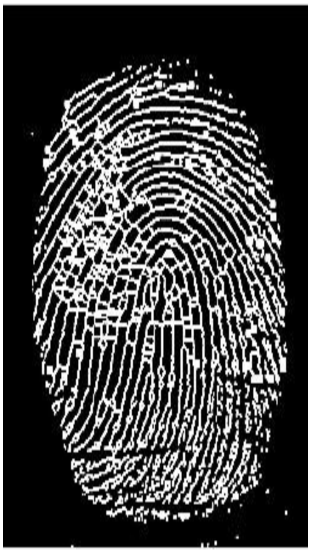


Figure 11: Combined template

J. Feature extraction:

Once the combined template is formed, features are extracted from it. Table 1 below shows the extracted features of combined template.

Features	Values
Mean	1.7798
Variance	90.2921
Entropy	1.5963
Std. Deviation	1.7992
Correlation	0.65041
Energy	0.50443

Table 1: Extracted features of combined template

Once the features are extracted from combined template, a vector consisting of the extracted features is formed and stored in a database with the name entered.

3. Authentication:

Figure 12 shows the block diagram of the authentication system used. In this system, first the index fingerprint image is read from a specific path and then preprocessing is performed on that image. After preprocessing, Gabor filtering is performed. After Gabor filtering, a minutiae image (1) is obtained. Similar steps are applied for index fingerprint image and orientation image (2) is obtained. A combined template is formed by performing AND operation on minutiae image and orientation image. Once the combined template is formed, features are extracted from the template. In this project, Decision tree method is used to check the authenticity of fingerprint images. The extracted features are given as input to Decision tree. Depending upon the output of Decision tree, a conclusion is drawn whether the fingerprint images belong to that of an authorized person or an unauthorized person.

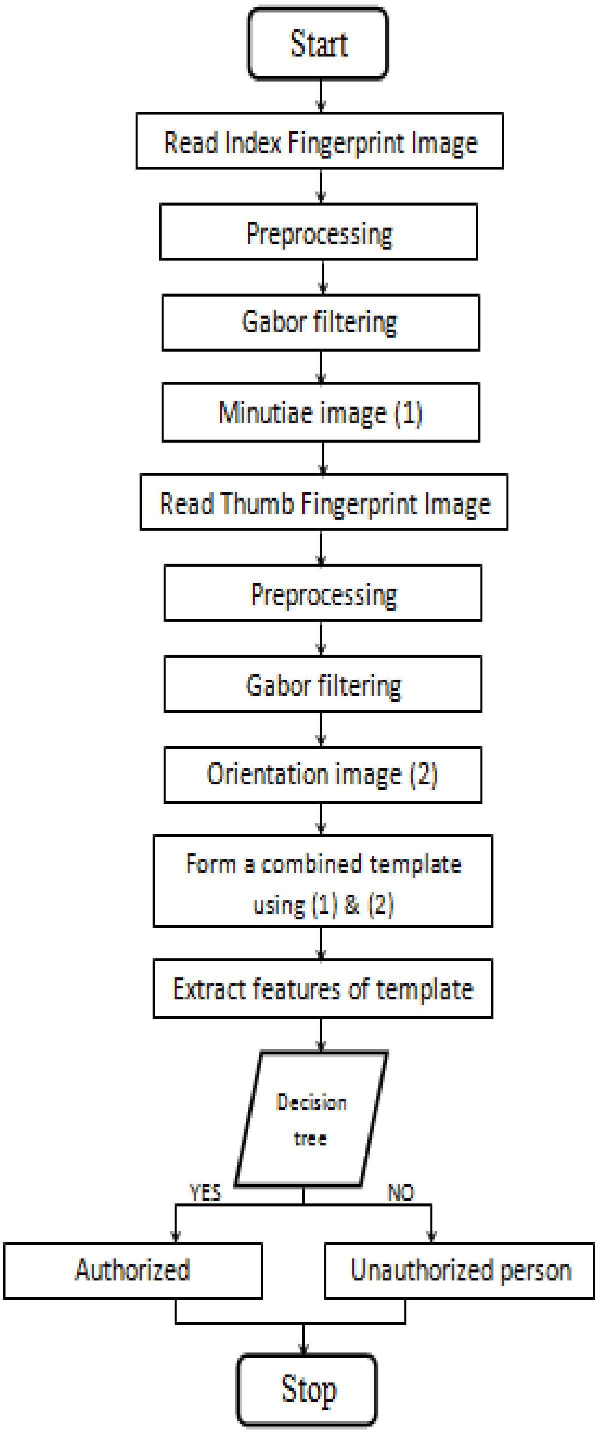
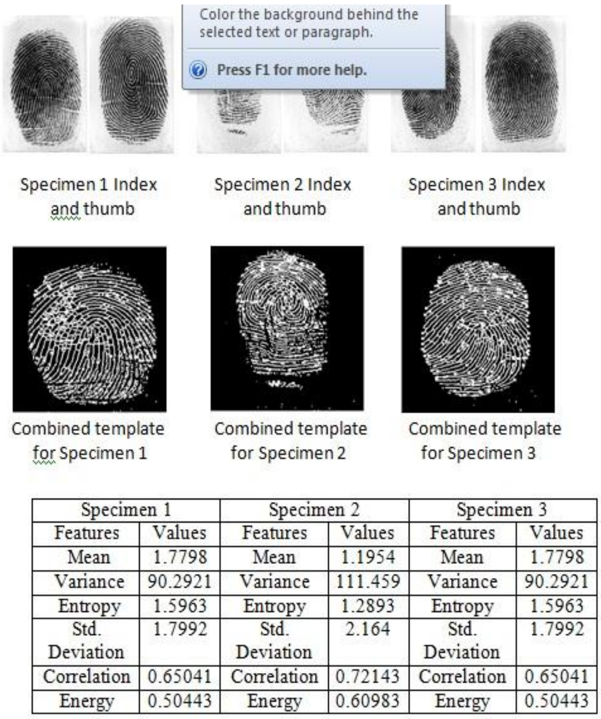


Figure 12: Authentication

III. Results and Analysis

The experimental results reveal that our system identifies the most of minutiae and orientation present in the original acquired images. Formation of combined template from minutiae image and orientation image has been successful. Also the features are properly extracted from combined template. As shown below Figure 13 represents the index and thumb fingerprint images of three different specimens along with corresponding combined templates and extracted features. As the features match with those stored in database the authentication system is reliable.


Color the background behind the selected text or paragraph.
Press F1 for more help.
Specimen 1 Index and thumb
Specimen 2 Index and thumb
Specimen 3 Index and thumb
Combined template for Specimen 1
Combined template for Specimen 2
Combined template for Specimen 3

Specimen 1		Specimen 2		Specimen 3	
Features	Values	Features	Values	Features	Values
Mean	1.7798	Mean	1.1954	Mean	1.7798
Variance	90.2921	Variance	111.459	Variance	90.2921
Entropy	1.5963	Entropy	1.2893	Entropy	1.5963
Std. Deviation	1.7992	Std. Deviation	2.164	Std. Deviation	1.7992
Correlation	0.65041	Correlation	0.72143	Correlation	0.65041
Energy	0.50443	Energy	0.60983	Energy	0.50443

Figure 1: Representation of the index and thumb fingerprint images of three different specimens along with corresponding combined templates and extracted features

IV. CONCLUSION

With the widespread applications of fingerprint techniques in authentication systems, protecting the privacy of the fingerprint becomes an important issue. The existing finger print technology does not provide much accuracy in protecting the privacy of the fingerprint. thus resulting into implementation of fusion techniques in the existing technology. This paper explores the possibility of mixing two different fingerprints, pertaining to two different fingers, at the image level in order to generate a new fingerprint. The extraction of minutiae and orientation and formation of combined template has been successful. The combined template obscures the information present in an individual's fingerprint image prior to storing it in a central database. The features are extracted from combined template and have been used for authentication. Combination of different fingerprint images and final verification is a scope of study of the defined problem statement.

REFERENCES

[1] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancellable fingerprint templates," IEEE Trans.Pattern Anal. Mach. Intell., vol. 29, no. 4, pp. 561–72, Apr. 2007.

[2] Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition. New York: Springer-Verlag, 2003.

[3] F. Pernus, S. Kovacic and L. Gyergyek, "Minutiae-Based Fingerprint Recognition," Proc. Fifth Int'l Conf. Pattern Recognition, 'pp. 1380-13%2,1980.

[4] Nikodeiiiusz-Szekely, V. Szekely, Image Recognition Problems of Fingerprint Identification, Microprocessors and Microsystems, Vol. 17, No.4, 215-218, 1993.

[5] Greenberg, S., Aladjem, M., Kogan, D. &Dimitrov, I.(2000) Fingerprint Image Enhancement using Filtering Techniques. 15thInternational Conference on patter n Recognition, Barcelona, vol. III, pp. 326–329.

[6] Ross and A. Othman, "Mixing fingerprints for template security and privacy," in Proc. 19th Eur. Signal Proc. Conf. (EUSIPCO), Barcelona, Spain, Aug. 29–Sep. 2, 2011.

[7] Ross and A. Othman, "Visual cryptography for biometric privacy," IEEE Trans. Inf. Forensics Security, vol. 6, no. 1, pp. 70–81,Mar. 2011.

[8] S. Li and A. C. Kot, "A novel system for fingerprint privacy protection," in Proc. 7th Int. Conf. Inform. Assurance and Security (IAS), Dec. 5–8, 2011, pp. 262–266.

Lukesh N. Jain,
Post-Graduate Student
Electronics & Telecommunications Engineering,
K. J. Somaiya College of Engineering, Mumbai.

Dr. R. G. Karandikar,
Dean (Academics)
Electronics & Telecommunications Engineering,
K. J. Somaiya College of Engineering, Mumbai.