Minutiae Based Fingerprint Matching for Identification and Verification

Deepika Sahu[1], Rashmi Shrivas[2]

[1]M.Tech, Mats University, School of Engineering and IT, Gullu Arang, Chhattisgarh, India

[2]Asst Professor, Mats University, School of Engineering and IT, Gullu Arang, Chhattisgarh, India

Abstract: ***Fingerprints play distinguishing role in biometrics. They give unique identification to the individual. They are permanent and non changing character pattern. The fingerprint recognition consists of retrieving specific fingerprints from database. The characteristics or features of a fingerprint are extracted and used in identification process. In this paper, a minutiae based algorithm is discussed briefly for voting system. Proposed system aims implements a voting system using minutiae based algorithm with low FRR Rate. It is done by comparing a fingerprint against another fingerprint. For this multiple features are used for better matching accuracy. This approach mainly uses sample fingerprint images for extraction of minutiae points and then performing fingerprint matching. Our paper involves image enhancement, feature extraction and minutiae matching. It finally results matched fingerprint after real minutiae calculation.***

Keywords: Fingerprint, FRR, Minutiae based algorithm, Voting System, Feature Extraction

1. Introduction

According to the biometric security, the identification of each person can be divided into ways: physical and behavioral. Fingerprint image is a unique physical parameter which will never change even for twins. Voice, iris, DNA and fingerprints are the biometric features which are very suitable for human recognition due to their uniqueness, universality, invariability and extraction facilities.

In the world of modernization, privacy is an important concept in any system. In any country for electing a government voting is conducted. But the existing systems still consist of manual approach which lags in time valuation. Presently voting systems consist of a control & balloting unit which are used for conducting a voting in a country. The control unit is kept at the Polling officer to allow for vote to every user & Ballot unit is used by voter for voting purpose. But it may possible that there may be illegal voting which is prone to security attacks. Because of which some people lose their valuable votes in selecting a government. Hence, if someone is not present in his location he can't vote.

For voting purpose a GSM based EVM [2] is implemented in existing system with fingerprint authentication but it suffers from high error rate & also the system is not bendable. In existing system, the error rate is high i.e. FRR (False Rejection Rate) which low down the performance of the system. Also there is no privacy in the system for the database protection which is susceptible to security attacks. Proposed system will implement privacy protected [6] authentication, in which an identity is created from matching different fingerprints using minutiae-based fingerprint matching algorithm [5] [4]. In this algorithm, the different fingerprint templates are used for creating a new identity which can be used for enrollment & authentication propose. By using the fingerprints matching technique, the FRR may reduce & performance of the system increases. Proposed system designs a voting system based on minutiae based algorithm using two stage fingerprint matching technique which is connected with the other voting devices through the internet. Hence, the proposed system is flexible, as anyone can cast their precious vote at anywhere.

2. Literature Review

There are many techniques presented previously based on fingerprint matching techniques. Most of the techniques undertaken in previous researches are based on the biometric authentication like fingerprint. Fuzzy vault system [8] is one of the most important mechanisms for secure biometric authentication based on fingerprint minutiae in which a secret key is produce selecting chaff points from minutiae template. Fingerprint matching using a Gabor filter [9] is another technique which uses fingerprint matching using a 16 Gabor filter from the template which results in designing a new method for comparing two ridge patterns map of image using adaptive filter method.

Minutiae based fingerprint matching algorithm [5] is useful in certain application for privacy protection. Previously, some work has been carried out to reduce the FRR (False Rejection Rate) by using certain techniques. Some of the techniques use the minutiae position of fingerprint images like Gabor filter technique [9] in which core & ridge pattern is used. Descriptor based Hough algorithm [3] is also proposed previously which uses a minutiae cylinder code to improve distinctiveness & Hough transform method to improve robustness & distortion of fingerprint image. Hence by referring certain techniques with respect to the FRR rate, the voting system can be designed using a Minutiae based algorithm.

3. Related Work

There are various algorithm designed based on fingerprint authentication focusing in reducing the FRR & FAR rate. Some of them show a result specifying the error rate i.e FRR ratio parameter. The different algorithms available for fingerprint matching are follows as

3.1 Minutiae Based Algorithms [5]

In Minutiae based algorithm, minutiae of fingerprints of both fingers are used to construct a new template. The new template is formed by the combination of two minutiae of fingers. The combined fingerprint image is constructed in two phase, in first phase fingerprint image is captured from both fingerprint .A reference point and orientation from first fingerprint and reference point & minutiae extraction is taken from both fingerprints to create a new combined fingerprint which is stored in database. By using the minutiae based algorithm, the complete minutiae feature of a both in new combined fingerprint will not be reconstructed when the database is robbed. By using different coding strategy it is found that the error rate is reduced i.e. FRR ratio gets reduced. Also the database is less prone to get information when it gets robbed.

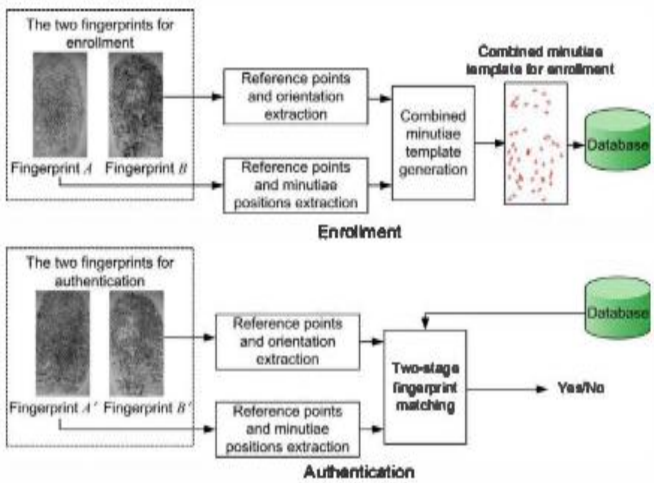
The two fingerprints for enrollment
Fingerprint A
Fingerprint B
Reference points and orientation extraction
Reference points and minutiae positions extraction
Combined minutiae template generation
Combined minutiae template for enrollment
Database
Enrollment
The two fingerprints for authentication
Fingerprint A'
Fingerprint B'
Reference points and orientation extraction
Reference points and minutiae positions extraction
Database
Two-stage fingerprint matching
Yes/No
Authentication

Figure 1: Phases of minutiae based algorithm

Figure 1 shows how the fingerprints A & B are stored in database considering the reference point & orientation of first fingerprint & reference point & minutiae position of second fingerprint which creates a new identity which stores in database during enrollment phase.

The combined minutiae template contains the minutiae position extracted from both fingerprint. During authentication phase when user input both fingerprints, depending upon the minutiae stored during enrollment phase it gets authenticated. The database stores the combined image of user which is privacy protected & secured. The two stage query matching is shown in figure 2.

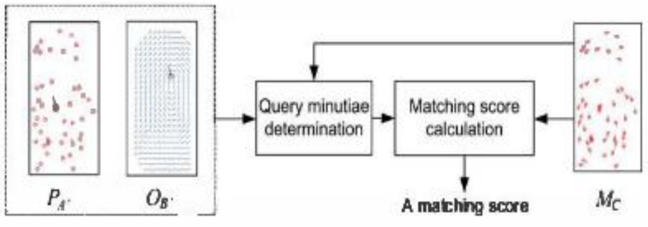

Figure 2: Combined Minutiae Generation

The combined minutiae template generation process is shown in figure 2 in which the minutiae points from first fingerprint & orientation from other fingerprint is used for query minutiae determination. Minutiae direction & position are aligned using different coding strategy for matching score calculation. Different coding techniques were used for matching the fingerprint & the best with low FRR is selected in the system. The advantages of this technique are low FRR rate & secure database prevention. The future research direction in combined minutiae based fingerprint matching algorithm will be using it in designing a votmg system.

3.2 Threshold Cryptography Technique [10]

In Threshold cryptographic technique, fingerprint image is separated into two or more shares using visual cryptographic method followed by compression. Also one share of fingerprint is stored in server & remaining shares given to finger. The template can only be reconstructed by superimposing shares. During the authentication phase the T-are superimposed with the ID card shares available with the user it gets genuine. The major concern of this technique is reducing the rate. The advantage of the technique is the system is secured from the attack from server side. The disadvantage of this technique is there is no privacy of database. The server side attacks are removed by using this techniques. The figure 3 shows how the shares are match from the server & ID card which results in authentication.

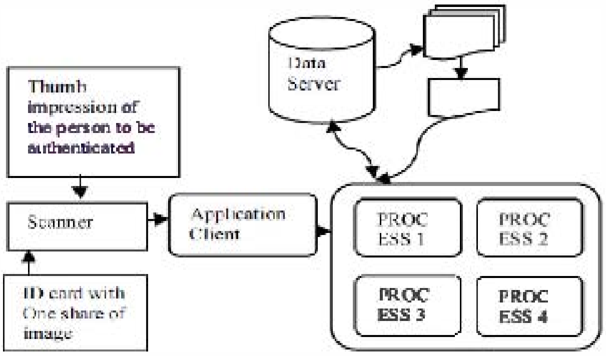
Thumb impression of the person to be authenticated
Data Server
Scanner
Application Client
ID card with One share of image
PROC ESS 1
PROC ESS 2
PROC ESS 3
PROC ESS 4

Figure 3: Threshold Cryptography Technique

3.3 Descriptor Based Hough Algorithm [3]

Latent are partial fingerprint which is smudgy & contain large distortions. Therefore, due to these it has significantly smaller number of minutiae points. Descriptor based Hough algorithms align fingerprints, also by taking into consideration both minutiae & orientation field information it measures similarity.

A Hough transform is used which improves robustness & distortion in fingerprint image. The process of matching in Descriptor Hough algorithm is shown in figure 4 in which manual marking is performed on fingerprint image to obtain the minutiae position & also automatic extraction on same image is performed. Both minutiae are aligned for calculating a score of fingerprint image. The benefit of this algorithm is that partial fingerprint can be identified.

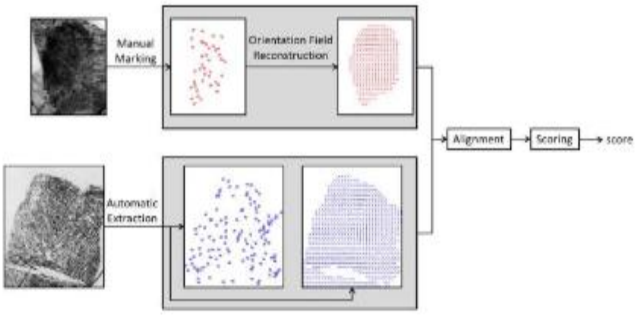

Figure 4: Latent fingerprint Matching

3.4 Image Based Matching Technique [12]

The image-based technique is generally used global features to match fingerprints without the need to extract any reliable minutiae-feature. This technique utilizes texture information, the ridge shape and local orientation for fingerprint verification. Image matching is done by computing the similarity between the template image and the input image. One of the main limitation of this technique is the lack of healthiness when tracking variations of scale and orientation.

3.5 Moodle [11]

Moodle is a software package used for creating courses and Internet Web sites. For registering in MoodIe, a fingerprint matching technique based on minutiae was used for login. It is bring into being that the fingerprint technique using a Moodle shows positive sign towards learning activities. By using the laptops & PC student can easily access certain learning courses.

The process of fingerprint matching process used in authentication in Moodle is shown in figure 5 in which different activities are involved. Firstly the fingerprint image are captured from both fingerprint image are used to create a new minutiae extracted image and has been process to enhancement process which include segmentation & normalization. The image is then given for binarization in which the quality of captured image is improved. If some image captured during the authentication is not clear then the binarization process improves it.

The fingerprint combined image is then passed through the thinning process before the minutiae position gets selected. After which the pre-processing is done then minutiae position gets selected from the image. Depending upon the fingerprint image used during the enrollment process, the information used during the authentication phase. As minutiae based algorithm has low FRR rate, the image captured during the enrollment phase gets authenticated if one or more position of minutiae match.

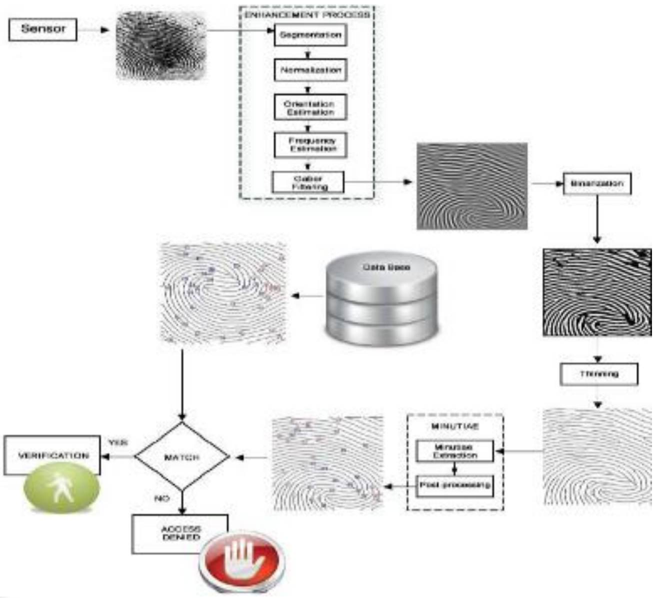

Figure 5: Verification of fingerprint in moodle

4. Comparative Analysis

Comparative analysis of techniques are discussed in table 1. Different techniques are compared according to the parameter undertaken and restrained.

Table 1: M

Technique	*Objective*	*Parameter*	*Out put*	*Limitation*
Matching Technique [13]	To design a voting system with matching technique	FRR ratio	FRR ratio >1.5 %	The system lag with high FAR & FRR ratio
Minutiae Based Algorithm[5]	To design an algorithm with privacy & security purpose	FRR ratio	Error rate i.e. FRR >0.4%	The algorithm is not design for EV&I
Threshold Cryptography Technique [10]	To develop a technique by dividing it into small share	FRR ratio	Error rate i.e. FRR >0.3%	Compression is required for reconstruction of fingerprint image
Fingerprint matching using Gabor filter	To develop a technique to increase genuine acceptance rate	GAR	GAR is 91%	More number of Gabor filter is used

From the analysis in the table 1. From the analysis in the table 1, it is found that minutiae based algorithm is best suitable for designing a fingerprint based voting system which has low error rate (FRR is low). Most of the techniques discussed above are not yet used for designing in any Voting system in previous researches. So, in proposed system a minutiae based fingerprint matching is being implementing for Voting system. The comparative analysis is made according to the FRR ratio, most of the techniques uses different coding techniques for reducing false rejection rate. Existing Voting system suffers from high FRR rate & insecurity.

5. Proposed Work

The proposed architecture is shown in figure 6 in which the Fingerprint Identification and Variation for Voting System consist of fingerprint sensors which are used for enrollment & Identification of user. The sensor output is given to PC for processing template of fingerprint. In the enrollment phase, the system captures fingerprints. Then some preprocessing are applied then minutiae position from fingerprint images is extracted to produce the template.

Minutiae position & direction are aligned in the template & stored in database. During Verification phase the template image stored in database are matched with the user image & user is authenticated. Minutiae based algorithm is used to improve the efficiency of system.

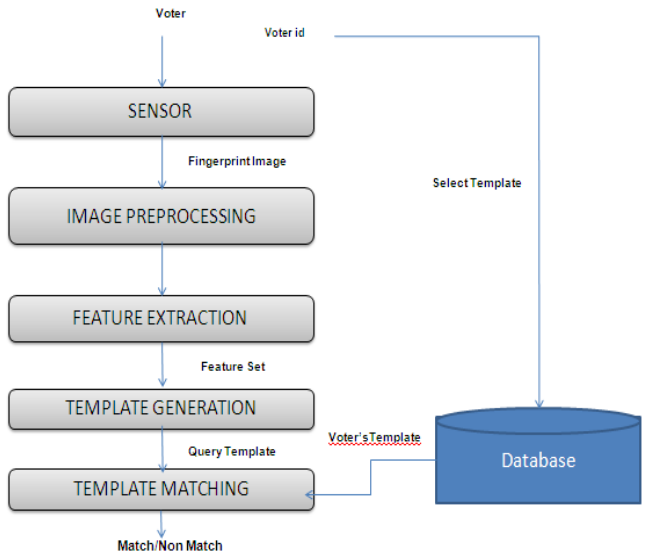

Figure 6 : Proposed Fingerprint Identification & Verification

6. Expected Outcome

Expected outcome of proposed system will be designing a Fingerprint Verifications and Identification for voting System with a secured authenticating technique with low error rate. The system will be secure, as fingerprint is used for creating new identity which can't be recovered if database stolen. Also, from the analysis of different techniques a minutiae algorithm is best for designing such applications.

References

[1] Sheng Li and Alex C. Kot "Fingerprint Combination for Privacy Protection," IEEE Transactions on Information Forensics and Security, February 2013

[2] Sreenath.M, Sukumar.P, Naganarasaiah Goud.K, P.Sivakalyani & V.Phani Kumar, "GSM based electronic voting machine using touch screen," 10SR Journal of Electronics and Communication Engineering, June 2014

[3] Paulino & Jianjang Feng, "Latent Fingerprint Matching Using Descriptor-Based Hough Transform," IEEE Transactions on Information Forensics and Security, March 2013.

[4] Xi Cheng, Sergey Tulyakov and Venu Govindaraju, "Minutiae-based Matching State Model for Combinations in Fingerprint Matching System," IEEE Conference on Computer Vision and Pattern Recognition Workshops, 2013.

[5] Sheng Li and Alex C. Kot "Fingerprint Combination for Privacy Protection," IEEE Transactions on Information Forensics and Security, February 2013.

[6] Sheng Li and Alex C. Kot, "A Novel System for Fingerprint Privacy Protection," 7th International Conference on Information Assurance and Security, 2011.

[7] Koichi Ito, Ayumi Morita, Takafumi Aoki, Tatsuo Higuchi, Hiroshi Nakajima, and Koji Kobayashi," A Fingerprint Recognition Algorithm Using Phase-Based Image Matching for Low-Quality Fingerprints", 0-7803-9134-9/5/20.00/@2005 IEEE

[8] Karthik Nandakumar, Anil K. Jain & Sharath Pankanti, "Fingerprint Based Fuzzy Vault: Implementation and Performance, "IEEE Transactions on Information Forensics and Security, December 2007.

[9] Muhammad Umer Munir and Dr. Muhammad Younas Javed, "Fingerprint Matching using Gabor Filters," National Conference on Emerging Technologies, 2004.

[10] Rajeswari Mukeshi & V.J.Subashini, "Fingerprint Based Authentication System Using Threshold Visual Cryptographic Technique," IEEE-International Conference On Advances In Engineering, Science And Management, March 2012

[11] Rosario Gil, Mohamed Tawfik, Alberto Pesquera Martin & Sergio Martin, "Fingerprint Verification System in Tests in Moodie," IEEE Journal of Latin-american Learning Technologies, February 2013.

[12] Jin Fei Lim, Renee Ka Yin Chin "Enhancing Fingerprint Recognition Using Minutiae-Based and Image-Based Matching Techniques"2013 First International Conference on Artificial Intelligence, Modelling & Simulation