A Fingerprint Matching Technique using Minutiae based Algorithm for Voting System: A Survey

Talib Divan
Department of Computer Science and Engineering
G. H. Raisoni College of Engineering
Nagpur (M.S.), India
talibdivan@gmail.com

Veena Gulhane
Department of Computer Science and Engineering
G. H. Raisoni College of Engineering
Nagpur (M.S.), India
veena.gulhane@raisoni.net

***Abstract*— Voting is one of the important task in electing a government in any country. For voting purpose, there should be a biometric authentication which is secure & privacy protected. If the system designed is insecure then it may be prone to certain attacks in database. Some researchers has worked on different techniques based on fingerprint matching considering FRR rate, but not yet implemented in designing a voting system. This papers aims to review certain techniques based on fingerprint matching considering the issue handled. In this paper, a minutiae based algorithm is discussed briefly showing how a new identity is created, also a proposed architecture is explained. Minutiae based algorithm use two stage fingerprint matching technique, in which minutiae position from one fingerprint image & orientation from other is used to create combined fingerprint image. Proposed system aims implements a voting system using minutiae based algorithm with low FRR rate.**

Keywords*— *Fingerprint, FRR, Minutiae based algorithm, Template, Voting system.

I. INTRODUCTION

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 [1] is implemented in existing system with fingerprint authentication but it suffers from high error rate & also the system is not flexible. In existing system, the error rate is high i.e. FRR (False Rejection Rate) which degrades the performance of the system. Also there is no privacy in the system for the database protection which is prone to security attacks. Proposed system will implement privacy protected [9] authentication, in which an identity is created from two different fingerprints using minutiae-based fingerprint matching algorithm [2] [10]. In this algorithm, the two different fingerprint templates are used for creating a new identity which can be used for enrollment & authentication propose. By using the two 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 valuable vote at anywhere.

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 [6] 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 [2] 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 [6] in which core & ridge pattern is used. Descriptor based Hough algorithm [7] 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.

The related work about the previous research is explained in section II. Section III & IV describe the research design & proposed architecture of research work. Section V describes a impact of proposed work on existing works undertaken followed by the expected outcome in section VI. Section VII describes the conclusion.

978-1-4799-6085-9/15/$31.00©2015 IEEE

II. 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

A. Minutiae based algorithm [2]

In Minutiae based algorithm, minutiae of fingerprints of both fingers are used to produce 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.

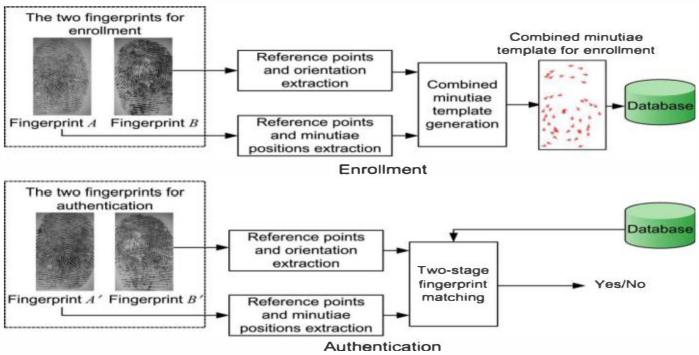

Fig. 1. Enrollment & Authentication phase in Minutiae based algorithm

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.

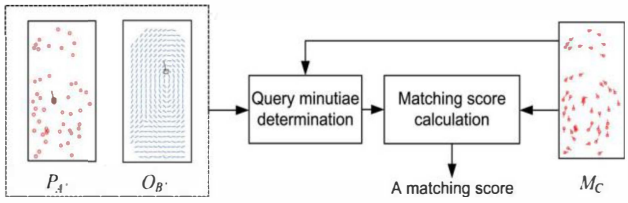

Fig. 2. Combined Minutiae template Generation

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 voting system.

B. Threshold Cryptography Technique [5]

In Threshold cryptographic technique, fingerprint image is divided into two or more shares using visual cryptographic technique followed by compression. Also one share of fingerprint is stored in server & remaining shares given to user. The template can only be reconstructed by superimposing shares. During the authentication phase the T-share are superimposed with the ID card shares available with the user & it gets authenticated. The major concern of this technique is reducing the error 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.

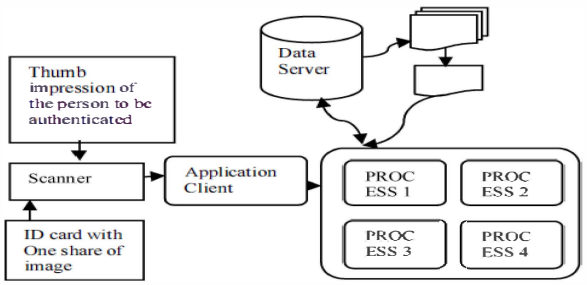

Fig. 3. Threshold Cryptography technique

C. Moodle [3]

Moodle is a software package used for creating courses and Internet-based Web sites. For registering in Moodle, a fingerprint matching technique based on minutiae was used for login. It is found 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 4 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.

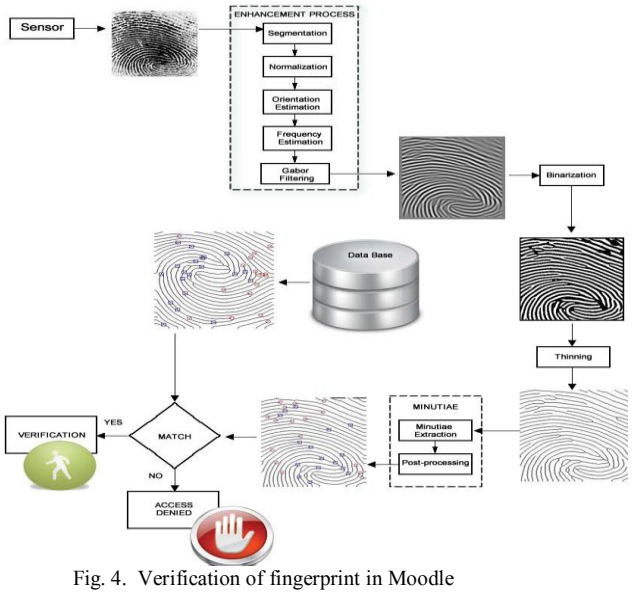

Fig. 4. Verification of fingerprint in Moodle

D. *Descriptor based Hough algorithm [7]*

Latent are partial fingerprint which is smudgy & contain large distortions. Hence, due to these it has significantly smaller number of minutiae points. Descriptor based Hough algorithms align fingerprints, also by considering both minutiae & orientation field information it measures similarity. Minutiae cylinder code in this technique improves distinctiveness. A Hough transform is used which improves robustness & distortion in fingerprint image.

The process of matching in Descriptor Hough algorithm is shown in figure 5 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 advantage of this algorithm is that partial fingerprint can be identified.

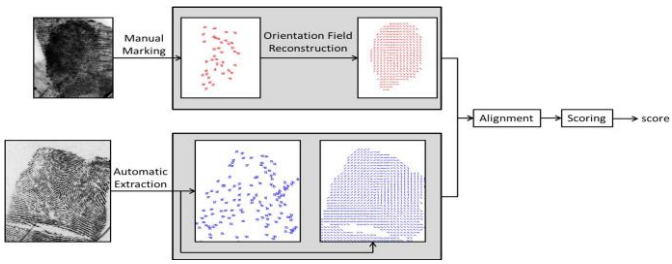

Fig. 5. Latent fingerprint matching

E. *Fingerprint-Based Fuzzy Vault [8]*

Fuzzy vault is considered as most comprehensive mechanisms for secure authentication and cryptographic key protection. Fingerprint based fuzzy vault is used matching the fingerprint image which stores only a transformed version of the template. Fingerprint-based fuzzy vault is the alignment of the query with the transformed template stored in the vault. Ffuzzy vault technique uses multiple biometric sources for improving the performance of system.

Figure 6 shows the operation for fuzzy minutiae based matching technique in which encoding & decoding during authentication & enrolment process is done. During enrolment phase the minutiae position from fingerprint template is captured in which chaff points are added to improve the security of the system.

The chaff point are selected randomly from the fingerprint image and few points are selected which is used for storing in database. The graph in figure 6 indicates how the secret key is extracted from the polynomial equation & gets authenticated.

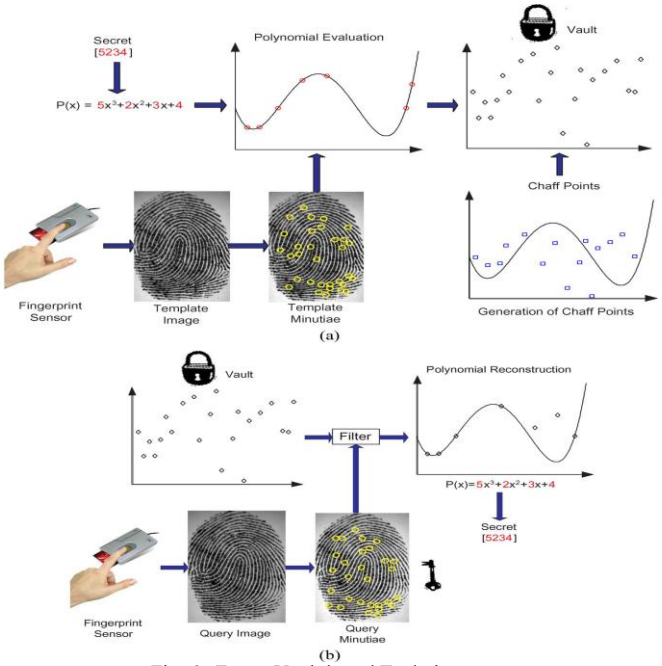

Fig. 6. Fuzzy Vault based Technique

The techniques discussed in related works are based on the fingerprint matching & certain techniques are presented considering the advantage & disadvantage. So, comparative analysis of these techniques considering the FRR & FAR parameter is done & found that the minutiae based algorithm [2] is found to be more effective in designing a voting system application. The FRR rate is less in minutiae based algorithm & there is privacy & security in database. Also, only Minutiae based algorithm uses two fingerprint matching which is new concept in designing voting system. Existing system does not used two stage fingerprint matching technique.

III. COMPARATIVE ANALYSIS

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

TABLE I. Comparative Analysis of Techniques.

Technique	Objective	Parameter	Output	Limitations
Matching Technique [1]	To design a voting system with matching technique.	FRR ratio	FRR ratio is >1.5%	The system lags with high FAR & FRR ratio.
Minutiae Based Algorithm [2]	To design an algorithm with privacy & security purpose.	FRR ratio	Error rate i.e FRR is 0.4%	The algorithm is not designed for voting application.
Threshold Cryptography Technique [5]	To develop a technique by dividing it into small shares	FRR ratio .	Error rate i.e FRR is 0.3%	Compression is required for reconstruction of fingerprint image.
Fingerprint Matching using Gabor Filter[6]	To develop technique to increase genuine acceptance rate.	GAR	GAR is91%	More number of gabor filter used.

IV. RESEARCH DESIGN

The research contribution is to design a voting system using minutiae based algorithm. Following are the research objective in designing a voting system,

1. Voting system has to be designed using minutiae based algorithm with low FRR.
2. The system is flexible.

V. PROPOSED ARCHITECTURE

The proposed architecture is shown in figure 7 in which the voting system consist of two fingerprint sensors which are used for enrollment & authentication of user. The sensor output is given to PC for processing template of fingerprint.

In the enrollment phase, the system captures two fingerprints from two different fingers. The minutiae position from both fingerprint images is extracted to produce the template. Minutiae position & direction are aligned in the template & stored in database.

During authentication 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. The html page consisting of various party logos has to be designed & votes are stored in MySQL database. As the system is flexible, a GPRS Module is used which communicate with server. The proposed system is flexible as anyone can cast their valuable vote. In designing a proposed system SQL database will be used for storing the information of users & result of votes.

The hardware requirement in designing the proposed system are Fingerprint sensor(R-305) ,Microcontroller(AVR), GPRS Module(SIM 300) & LCD(16X2).The software used in this project are Embedded C & MATLAB.

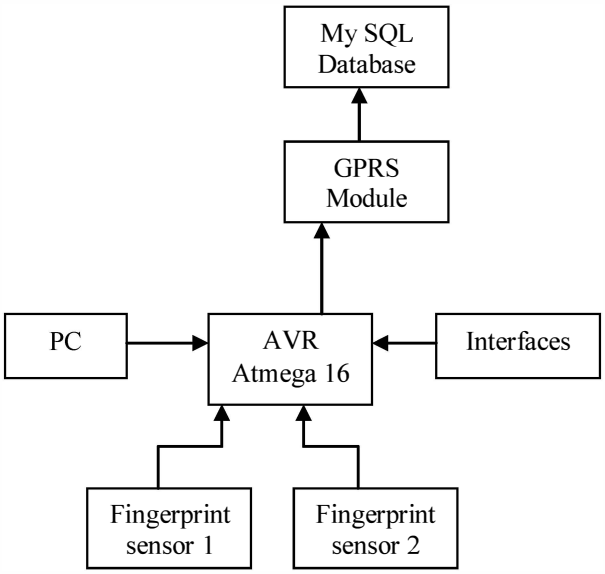

Fig. 7. System Architecture

The minutiae based matching process which can be used for designing a voting system is shown in figure 8 in which a fingerprint image is given for diagnostic process which undergoes binarization of the new combined image. In binarization the image are allowed to operate on bi-level i.e white & black. Black pixel represent ridge & white pixel represent valley in fingerprint. The fingerprint image is then extracted for the minutiae position to generate the template which can be used for authentication & enrollment process.

The fingerprint image after the extraction are stored in the template database which can be used during the authentication for matching & enrollment for storing.The stored fingerprint template are secured as it is made through two stage fingerprint process and less prone to server side attacks.

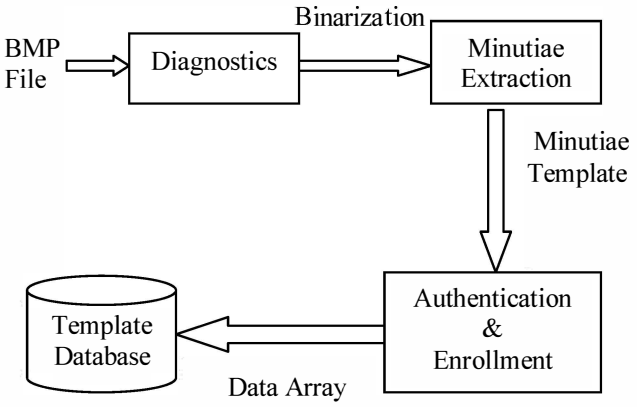

Fig. 8. Fingerprint template storing in Template Database

VI. Impact of Proposed System

Proposed system is being designed using a technique having low FRR i.e. minutiae based algorithm. As no voting system has been implemented previously using such technique so proposed designs a new method of identification which will be secure & privacy protected. Also through the literature survey, the minutiae based algorithm is considered as best among other techniques for implementing a voting system. Most of techniques has high FRR rate like fuzzy vault produce high error rate. Hence, voting system with fingerprint authentication using a minutiae based algorithm will create a impact on other techniques with its security, privacy & low FRR rate.

VII. Expected Outcome

Expected outcome of proposed system will be designing a voting system with a secured authenticating technique with low error rate. The system will be secure, as two 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 a system with low FRR ratio.

VIII. Conclusion

Thus, here a minutiae based algorithm is discussed considering fingerprint matching process. Also different techniques are analyzed considering the FRR ratio of technique. It is found that the Minutiae based algorithm is best suitable in designing a proposed architecture by considering its FRR rate. Hence, a proposed system will implement a voting system with privacy & security.

Acknowledgment

The research work presented in this paper is in development phase carrying out by Talib Divan student of 4th Semester in Embedded System & Computing branch of Computer Science & Engineering Department.

References

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

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

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

[4] Diponkar Paul & Sobuj Kumar Ray,"A Preview on Microcontroller Based Electronic Voting Machine," International Journal of Information and Electronics Engineering, March 2013.

[5] 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 .

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

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

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

[10] 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.