A secure mobile voting system using fingerprint

A SECURE MOBILE VOTING SYSTEM USING FINGERPRINT U. Rajkumar, H. Karunakaran, B. karthikeyan, M. venkatesh, com, Department of Information Technology, V. S. B Engineering College, Karur.

Abstract- The heart of the democracy is solely depending on the voting. The voting is the right for every citizen in the nation. The fingerprint shows the most promising future in real-world applications. Because of their uniqueness and consistency over time, fingerprints have been used for identification and authentication purpose.

However, there are some challenges in using fingerprint in real-world application. We are interested in designing and analyzing the Mobile voting system using fingerprint texture, which is the core in current modern approach for fingerprint analysis. As the mobile phone become a part of the human, it is very convenient to use. We are using the mobile phone for the purpose of voting. It helps the user to poll their vote in spite of any location and also in short period of time. Keywords— Biometric, Fingerprint, Minutiae, Mobile phone.

I. INTRODUCTION Elections allow the populace to choose their representatives and express their preferences for how they will be governed. Naturally, the integrity of the election process is fundamental to the integrity of democracy itself. The election system must be sufficiently robust to withstand a variety of fraudulent behaviors and must be sufficiently transparent and comprehensible that voters and candidates can accept the results of an election. Most of the countries in the world e-Voting system have been used.

Due to rapid growth of technology security problems are getting increased. So instead of developing e-voting systems, also there is a lot research work is being done to make these systems more secure. In some e-Voting systems, there is a password is issued to individuals to make the system more. Nowadays a lot of research work is going on developing more secure methods and one of them secure methods is usage of biometrics. Biometric based systems are those in which human physical characteristics like face shape, finger prints, etc. re being used for identification and authentication. Biometrics is the automated recognition of individuals based on their behavioral and biological characteristics. Biometric recognition means by measuring an individual’s suitable behavioral and biological characteristics in a recognition inquiry and comparing these data with the biometric reference data which had been stored during a learning procedure, the identity of a specific user is determined. A fingerprint is an impression of the friction ridges, from the surface of a fingertip.

Fingerprints have been used for personal identification for many decades, more recently becoming recognition is nowadays one of the most important and popular biometric technologies mainly because of the inherent ease in acquisition the numerous sources (ten fingers) available for collection, and the established use and collections by law enforcement agencies. Automatic fingerprint identification is one of the most reliable biometric technologies. This is because of the well known fingerprint persistence, distinctiveness, ease of acquisition and high matching accuracy rates.

Fingerprints are unique to each individual and they do not change over time. Even identical twins do not carry identical fingerprints. Scientific research in

areas such as biology, embryology, anatomy and histology has supported these findings. Fingerprint recognition method and ID system in biometric methods are frequently preferred because applications of them are easy and lowcost. Every human in the world has a unique Fingerprint so it is impossible to steal or lose so there is no need to remember fingerprints like if individual passwords or personal identification numbers (PINs) in card technology to keep systems secure.

Besides, every finger has distinctive characteristics because fingerprints of every finger of a person are different. That is why majority of secure systems are using fingerprint method alone or in combination with other biometric feature to make systems more secure in this rapidly advancing technology era. That is why in this Mobile Voting systems are identification of voter is based on fingerprints. A database is created containing the fingerprint of all the voters in the constituency. Illegal votes and repetition of votes is checked for in this system.

Hence if this system is employed the elections would be fair and free from rigging. Fingerprints are one of many forms of biometrics used to identify an individual and verify their identity. Extensive research has been done on fingerprints in humans. Two of the fundamentally important conclusions that have risen from research are: (i) a person’s fingerprint will not naturally change structure after about one year after birth and (ii) the fingerprints of individuals are unique. Even the fingerprints in twins are not the same. In practice two humans with the same fingerprint have never been found.

In this study, for the fingerprint authentication the minutiae or texture based matching is considered for higher recognition accuracy. This paper is organized as follows: The section II describes the issues of the present voting system, section III discusses the proposed mobile voting system, Section IV describes the gabor filter based fingerprint matching, Section V describes the conclusion. Privacy: (1) neither authorities nor anyone else can link any ballot to the voter who cast it and (2) no voter can prove that he voted in a particular way.

Verifiability: anyone can independently verify that all votes have been counted correctly. Collusion Resistance: no electoral entity (any server participating in the election) or group of entities, running the election can work in a conspiracy to introduce votes or to prevent voters from voting. If all entities conspire this property isn’t achieved. So, this characteristic should be measured in terms of the total number of entities that must conspire to guarantee a successful interference in the election.

Availability: (1) the system works properly as long as the poll stands and (2) any voter can have access to it from the beginning to the end of the poll. Resume Ability: the system allows any voter who had interrupted his/her voting process to resume it or restart it while the poll stands The existing elections were done in traditional way, using ballot, ink and tallying the votes afterward. But this system prevents the election from being accurate. Problems encounter the usual elections are as follows: • It requires human participation, in tallying the votes that makes the elections time consuming and prone to human error. The voter find the event boring resulting to a small number of voters. • Deceitful election mechanism. So, the proposed

mobile voting system has to be addressed these problems. II. ISSUES OF PRESENT VOTING SYSTEM There has been several studies on using computer technologies to improve elections. These studies caution against the risks of moving too quickly to adopt electronic voting system, because of the software engineering challenges, insider threats, network vulnerabilities, and the challenges of auditing.

Researchers in the electronic voting field have already reached a consensus pack of following core properties that an mobile voting system should have: Accuracy: (1) it is not possible for a vote to be altered, (2) it is not possible for a validated vote to be eliminated from the final tally, and (3) it is not possible for an invalid vote to be counted in the final tally. Democracy: (1) it permits only eligible voters to vote and, (2) it ensures that eligible voters vote only once. III.

MOBILE VOTING SYSTEM The main core of this study is to design an Mobile voting system based on fingerprint minutiae is discussed in this section by two phases: i) Enrolment Process and ii) Voting Process. A. ENROLMENT PROCESS The Fig. 1 shows the enrolment process clearly. The Process involved in using fingerprint scanner for election is very simple. First, the chosen finger for example, the thumb is captured and extracted. The fingerprint template is then enrolled and store in a local repository, a database. Along with this we are going to store the other details like user name, location, age, etc,..

This primary process is done during the registration process. After that, the chosen finger can be live scan. The fingerprint template is then processed

and extracted. It will subsequently match the scanned fingerprint against the stored template. Upon verification, they will have the access to vote for their desired candidates. Mismatched fingerprint certainly would indicate denial form the access. of any location . We intend to ease the people with the help of technology development. This is the innovation we made so that the people can vote from their work and no person is allowed to vote for the second time, as it is ne of the drawbacks of the present voting machine. The each casted vote by the users are stored in the server according to the respective nominee. After the completion of voting process, on the counting day, the authorized person can know the status of the nominees by checking the server. Figure 1. Enrollment process B. VOTING PROCESS In Fig. 2 the voting process is explained. The first process is capture the input image using the mobile phone scanner, the captured image is then sent to the database using the mobile phone scanner, then it is matched with the database using Gabor filter.

And also we are using the location criteria to minimize the possibilities of number of templates for the fingerprint matching, by allocating it to the appropriate server. After this, it is compared with the template which is stored in the database. If the matching result is true, the person is allowed to vote. Otherwise he is rejected and given the error message. The person who is authenticated may vote for their beloved one by giving his fingerprint to the fingerprint scanner of the mobile phone, then by selecting their corresponding nominee. As, we are using the mobile phone the user can cast their vote in spite Figure 2.

Voting process. IV. GABOR FILTER BASED . FINGERPRINT MATCHING We have followed the method of Gabor Filter based fingerprint matching proposed by the Salil Prabhakar in his PhD Thesis [3]. It is a generic]. scheme for representing fingerprint texture that relies on extracting one point of reference of the fingerprint image. A predetermined region of interest around the reference point is tessellated into cells. Each cell is then examined for the information in one or more different orientations. mation An ordered detail of the features, thus extracted from each cell are used for the fingerprint he representation [4].

Four main steps in extraction]. algorithm are explained below: defined around the reference point and divided in efined four bands and each band is further divided into sixteen non-overlapping sectors. Therefore, a overlapping total number of 64 sectors are created, as shown re in Figure. 4. The region of interest is collection of . 4. all sectors. The innermost band (circle) is not used for feature extraction because the sectors in the region near the reference point contain very he few pixels. Therefore, the feature extraction in this region is not very reliable.

A circular tessellation is chosen since a rotation of the fingerprint will correspond to the rotation of the tessellation [3]. A. REFERENCE POINT LOCATION e The reference point of fingerprint is the point of maximum curvature of concave ridges as shown cave in Figure. 3 [3]. In order to locate these points,]. we have followed the method propos proposed by Nilsson K. and Bigun J. [4]. According to this]. method, these points have special symmetry properties, which make them easy to identify [3 [3]. These points

have strong response to complex filters, designed to detect rotational symmetries.

The Nilsson method has an advantage, that even if two fingerprints are rotated and translate translated relative to each other, it can estimate both translation and rotation parameters quickly [4 d [4]. Figure. 4 Tessellated Region C. NORMALIZATION Before applying Gabor filter to the fingerprint image, the gray level intensities of all pixels in each sector in the region of interest must be normalized to a constant mean and variance [3 [3]. Normalization is performed to remove the effects of sensor noise and gray level background due to finger pressure differences.

The norma normalized image is shown in Figure. 5. Figure. 3 Reference Point Location Figure. 5 Normalized Fingerprint Image . 5 B. TESSELLATION Tessellation is a pattern of identical shapes that must fit together without any gap, and shapes should not overlap [3]. In this method, a circle is]. D. GABOR FILTER A Gabor filter is a linear filter used in image processing for edge detection. Gabor filter works as bandpass filter for the local spatial frequency distribution, achieving an optimal resolution in both spatial and frequency domains [5].

A 2D Gabor filter is a Gaussian kernel function multiplied by a sinusoidal plane wave. For extracting useful features from an image, a set of Gabor filters with different frequencies and orientations are required [3]. The result of 8 differently oriented Gabor filter is shown in Figure. 6. E. MATCHING Fingerprint matching is based on finding the Euclidean distance between the corresponding FingerCodes. The translation invariance in the FingerCode is

established by identifying the reference point. The approximate rotation invariance is achieved by cyclically rotating the features in the FingerCode itself.

A single-step cyclic rotation of the features in the FingerCode corresponds to a feature vector which would be obtained if the image was rotated by 22. 5 . The nature of the circular tessellation is such that the feature is invariant to only small perturbations that are less than 11. 25 . Therefore, we generate another feature vector for each fingerprint at the time of user enrollment which corresponds to a rotation of 11. 25. The original image is rotated by an angle of 11. 25 and its FingerCode is generated [6]. For each fingerprint in the database, we store two templates, each having 8 different orientations.

So, when the fingerprint is loaded into the Matlab, we perform 8 rotations on both the templates. Then, these two stored templates correspond to all the rotations of the fingerprint image in multiples of 11. 25 . This takes care of the fingerprint rotation while matching the input FingerCode with the stored templates. The final matching distance score is taken as the minimum of the 16 scores obtained by matching the input FingerCode with each of the 16 templates. This minimum score corresponds to the best alignment of the two fingerprints being matched.

Figure . 6 Gabor Filter Oriented at Eight different angles The even symmetric two-dimensional Gabor filter has the following mathematical form, In Eq (1) , is the frequency of the sinusoidal plane wave along the direction ? from the x-axis, and and are the space constants of the Gaussian envelope along x and y axes, respectively. In the proposed MVS, we set the filter frequency f

to the average ridge frequency (1/K), where K is the average inter-ridge distance. The average inter-ridge distance is approximately 10 pixels in a 500 dpi fingerprint image.

If f is too large, spurious ridges are created in the filtered image, whereas if f is too small, nearby ridges are merged into one [6]. If and (standard deviations of the Gaussian envelope) values are too large, the filter is more robust to noise, but is more likely in smoothing the image to the extent that the ridge and valley details in the fingerprint are lost. If x and y values are too small, the filter is not effective in removing the noise. The values for and were empirically determined and each is set to 4. 0 (about half the average interridge distance). Figure 7. Feature Vectors of different users F.

RESULT OF THE MATCHING ALGORITHM Two similar looking fingerprints are shown in Figure. 7, however they are taken from two different voters. Therefore, the two different, but similar fingerprints can be differentiated using their FingerCodes. A threshold for minimum distance between FingerCodes of two different voters was empirically found and was set at near 800. If two fingerprints have this minimum distance value less than 800, this implies that both fingerprints belong to the same voter, otherwise not. The minimum distance for the two fingerprints shown in Figure 7. is 1712. 34, On the other hand, Figure 8. hows two images of the same user which appear quite different. The Figure8. also shows their corresponding FingerCodes and matching distance. FingerCodes are matched successfully with the minimum distance of 320. 3. as templates, the identification time would be relatively insensitive to size of database. An extracted FingerCode template of a user consists of around 6. 0 Kb which is comparatively very

less than the image size of 150 Kb. As the users are using the mobile phone for the voting, there is no need to carry any of the proofs with the them and also there is no possibility for the fraudulence.

We are intending to bring the current technology to the people, in order to make the voting system as easy as they do their other activities. Our project would provide the security for each individuals vote, with the help of the technology. VI. REFERENCES [1]. A Novel design of Electronic Voting System Using Fingerprint by DA Kumar, T. Ummal Sariba Begum in International Journal Of Innovative Technology & Creative Engineering (Issn: 2045-8711) Vol. 1 No. 1 January 2011. [2]. Electronic Voting System Using Fingerprint Matching with Gabor Filter Sobia Baig, Ummer Ishtiaq, Ayesha Kanwal, Usman Ishtiaq, and M.

Hassan Javed. [3]. " Fingerprint Classification and Matching Using a Filter bank", Salil Prabhakar, PhD thesis, Michigan State University, Computer Science & Engineering 2001 pp. 102 -115, 160162. [4]. " Localization of corresponding points in fingerprints by complex filtering," Nilsson K. and Bigun J. , vol. 24, Pattern Recognition Letters, 2003, pp. 2135–2144. Figure 8. Feature Vectors of same user V. CONCLUSION We have developed Mobile Voting System using Fingerprint Recognition. This system has provided an efficient way to cast votes, free of fraud.

We have used Gabor Filter based fingerprint identification and matching with high accuracy. If orientation normalized FingerCode of all enrolled fingerprints are stored [5]. Next Generation A Secure E-Voting System Based On Biometric Fingerprint Method Kashif Hussain Memon1, Dileep Kumar2

and Syed Muhammad Usman in 2011 International Conference on Information and Intelligent Computing IPCSIT vol. 18 (2011) © (2011) IACSIT Press, Singapore. [6]. “ On Face Recognition using Gabor Filters , Al-Amin Bhuiyan, and Chang Hong Liu World Academy of Science Engineering and Technology Issue 28 Apr 2007 artcal # 10, pp. 3.