RESEARCH ARTICLE OPEN ACCESS

A SECURITY BASED VOTING SYSTEMUSING BIOMETRIC

M.Thangamani[1], S.Shunmathy[2], S.Backiyalakshmi[3], P.T.Aiswariya[4], K.Priyadharshini[5]
Computer Science and Engineering, Anna University, Chennai, India / Saranathan College of Engineering

ABSTRACT: The problem of voting is still critical in terms of safety and security. This paper is about the design and development of a voting system using fingerprint to provide a high performance with high security to the voting system. Fingerprint biometrics is widely used for identification. Biometrics identifiers cannot be misplaced and they represent any individual identity. The integration of biometric with electronic voting machine requires less manpower, save much time of voters and personal, ensure accuracy,transparency and fast result in election. In this paper a framework for electronic voting machine based on biometric verification is proposed and implemented. The proposed framework provides secured identification and authentication processes for the voters and candidates through the use of fingerprint biometric
Keyword: Fingerprint, Fingerprint sensor, minutiae, Database.

I. INTRODUCTION:

Now-a-days, democracy has become an important part of people's lives. The heart of democracy is voting. The voting must be trust one and vote must be recorded and tallied with accuracy and impartiality. This is achieved by using biometric system. An electronic voting system defines valid voting and gives an fast method of counting votes, which helps to yield a final result.

Moreover, electronic voting systems can improve voter identification process by using biometric recognition. Biometrics is becoming an essential personal identification solutions, since biometric identifiers cannot be misplaced and they represent an individual's identity. Biometric recognition refers to the use of iris, fingerprint, face, palm and speech characteristics, called biometric identifiers. Fingerprint matching is a important for this process. It is an extremely difficult problem, due to variations in different impressions of the same finger. Fingerprints are unique to each individual and they do not change over time.

Voting system starts from the 18th century and many proposals for voting system have been made till now. When designing an electronic voting system, it is essential to consider ways in which the voting tasks can be performed electronically without sacrificing voter privacy or introducing opportunities for fraud.

1.2 Requirement:

Abiometric system is a pattern recognition system that operates by extracting biometric data from an person, extracting a feature set from the extracted data, and comparing this feature set against the template set in the database. Depending on the application, a biometric system may operate in verification mode and identification mode. Fingerprint biometric is the most widely publicized biometrics for identification. This is largely due to its easy and cost effective integration in existing and upcoming technologies. The integration of biometric with electronic voting machine requires less manpower, save much time of voters and personnel ensure accuracy, transparency and fast results in election. In the framework for electronic voting machine based on biometric verification is proposed and implemented. The proposed framework ensures secured identification and authentication processes for the voters and candidates through the use of fingerprint biometrics. In this paper,using fingerprint followingfactors are achieved,

1. Security: No one can evaluate the result before announcement.
2. Eligibility: Only eligible voters are allow to vote.
3. Uniqueness: voters are allow to vote only once.
4. Accuracy: All the valid votes are automatically calculated by the system.
5. Time consumption: The time taken to count the vote is less than the existing system.

II. EXISTING SYSTEM

In India bar code scanning is performed with the help of India's national ID program called Aadhaar is the largest biometricdatabase of the world. It is a biometrics-based digital identity, instantly verifiable online at the point of service (PoS), at anytime, anywhere, in a paperless way. Currently it has 500 million people with 6 petabyte of data.

- It will reach 1.25 billion people in few years, 15 PB of data and over 200 trillion biometric

matches per day.It is designed to enable government agencies to deliver retail public service securely based on biometric data along with demographic data of a person.

- The data is transmitted in encrypted form over internet for authentication, aiming to free it from limitations of physical presence of a person at a given place. Thus is can be used for casting vote from anywhere, availing social security benefits from anywhere e.g. PDS ration form any shop etc.

Elections definesthe democracy of people. We speak about who is allowed to vote, how campaigns are conducted, and how they are financed, but no one gives priority to the understanding of the actual voting process. Electronic Voting Machines ("EVM").

EVM consists of two units, i) Control Unit, ii) Balloting Unit. The two units are joined by a five-meter cable. The Control Unit is with the Presiding Officer or a Polling Officer and the Balloting Unit is placed inside the voting compartment.The category "electronic voting" is potentially broad, referring to several distinct possible stages of electronic usage during the course of an election.

Security Problems – Many one can change the program installed in the EVM and tamper or fraud the results easily after the polling. By replacing a small part of the machine we change votepercentage of the particular candidate. These instructions can be sent wirelessly from a mobile phone.

Illegal Voting (Rigging) - The very commonly known problem, Rigging which is faced in every electoral procedure. One candidate, can put the votes for the people without his or her knowledge by illegally. This results in the loss of votes for the other candidates participating and also increases the number votes to the candidate who performs this action. This can be done externally at the time of voting.Traditional voting process can be divided into different phases:

1. *Identification*: In this phase, voter authenticates himself or herself by showing his or her voting card, this step is public and verified by the presiding officer. At the end of authentication process, presiding officer give a ballot paper to voter to cast his or her vote.
2. *Vote*: The vote takes place in a separate booth where voter cannot be seen by any person. The voter cast their vote by pressing the button in machine and it will be stored.
3. *Vote counting*: At the end of voting time, the presidingofficers collect the ballot box and submit it to the counting centre. After that with the help of members of the election committee nominated by election commission of India, the ballot boxes are opened and votes are counted and the results are then announced.
4. *Verification*: Various types of verification process are used, most procedure are public and verified by the representative of candidates of competing parties. Recount is also possible if there is anyfraud or error.

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 will be marked on the fore finger by using ink.
- Deceitful election mechanism.
- Constant spending funds for the elections staff every year.

III. PROPOSED SYSTEM

3.1fingerprint Recognition

Fingerprint recognition has been widely used in both forensic and civilian applications. Compared with other biometrics features, fingerprint-based biometrics is the most proven technique. In terms of applications, there are two kinds of fingerprint recognition systems: verification and identification**.**

*Fingerprint Verification:*Fingerprint verification is the method where we compare the fingerprint with an enrolled fingerprint, where our aim is to match both the fingerprint. This method is mainly used to verify person'sauthenticity. For verification a person needs to his or her fingerprint in to the fingerprint scanner. Then it is representation is saved in some compress format with the person's identity and his or her name. Then it is applied to the fingerprint verification system so that person's identity can be easily verified. Fingerprint verification is also called, one to one matching.

*Fingerprint Identification:*Fingerprint identification is mainly used to specify any person's identify by his or her fingerprint. Identification has been used for fingerprint matching. Here the system matches the fingerprint of unknown person against the other fingerprint present in the database. This process is also called one to many matching.

3.2 Minutiae Based Implementation

Fingerprint has been used as a method of personal identification for over a century. It is widely used in biometric authentication at present because of its uniqueness and performance. A fingerprint consists of ridges and valleys. There are

two basic features used in fingerprint recognition, i.e. ridge endings and ridge bifurcations. Other features are also used. According to features used in fingerprint recognition, automatic fingerprint recognition techniques are classified into
minutiae-based, image-based and ridge feature-based approaches. Ridge feature-based approach issued when minutiae are difficult to extract in very low quality fingerprint images, whereas other features of the fingerprint ridge pattern (e.g., local orientation andfrequency, ridge shape, texture information) may be extracted more reliably than minutiae, even though
their distinctiveness is generally lower.
A fingerprint is the pattern of ridges and valleys on the surface of a fingertip. The endpoints and crossing points of ridges are called minutiae.

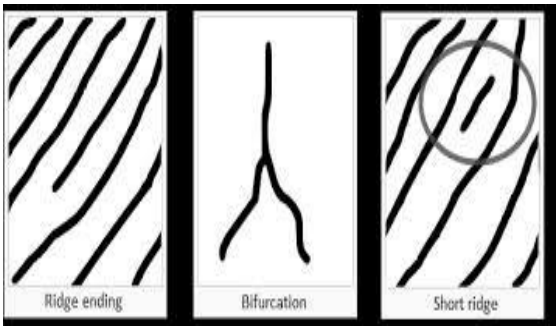


Figure1:Ridge ending and Bifurcation

3.2.1 Advantages Fingerprint Authentication

Fingerprint solutions offer many advantages which address the human factors of authentication.

- One of a kind identifier - Fingerprints from each one of our ten fingers is distinctive, different from one another and from those of other persons. Even identical twins have distinctive fingerprints.
- Greater convenience - Users no longer have to remember multiple, long and complex, frequently changing passwords or carry multiple keys.
- Relatively equal security level for all users in a system - One account is not easier to break into than any other (such as an easily guessed password or through social engineering).
- Ensures the user is present at the point and time of recognition and later cannot deny having accessed the system.
- Cannot be shared, lost, stolen, copied, distributed or forgotten unlike passwords, PINs, and smart cards. Fingerprints strongly link an identity to a physical human being making it difficult for attackers to forge.
- Long history of successful use in identification tasks. Fingerprints have been used in forensics for well over a century and there is a substantial body of scientific studies and real world data supporting the distinctiveness and permanence of fingerprints.

3.2.1fingerprint Matching Technique

The minutiae ending and bifurcation are shown in the Figure 1. A ridge ending is defined as the ridge point where a ridge ends abruptly. A bifurcation is defined as the ridge point where a ridge bifurcates into two ridges. It is accepted that the minutiae pattern of each finger is unique and does not change during life period. When human fingerprint experts determine if two fingerprints are from the same finger, the matching degree between two minutiae pattern is one of the most important factors. The way of human fingerprint experts and compactness of templates, the minutiae-based matching method is the most widely studied matching method. The algorithms which are compared in this paper belong to the minutiae-based matching method.

Image-based approaches use the entire gray scale fingerprint images as a template to match against input fingerprint images. This approach needs a large size of storage space and fingerprint images are illegal to be stored in some nations.

Minutiae-based approach attempts to get the similarity degree between two minutiae sets. However, minutiae-based methods may make the computation more easyand need to search for the best correspondence of minutiae pairs or ridge pairs or use core or delta minutiae point to estimate the alignment. The problem of lost minutiae or false minutiae always occurs during the minutiae detection process. Hence, the corresponding pairs may not be found under this condition.
Minutiae Based Matching is a technique in which minutiae are extracted from a fingerprint and stored as sets of points in a two-dimensional plane and then minutiae of the fingerprint to be recognized are extracted and matched with the stored points. Minutiae matches the alignment between the template and the input minutiae sets that result in the maximum number of minutiae pairings. Automatic fingerprint identification is one of the most reliable biometric technologies. This is because of the well-known fingerprint distinctiveness, persistence, ease of acquisition and high matching accuracy rates.

3.2.2 Feature Extraction

In this section, we discuss how to extract the features used by the matching algorithm. We give a brief description of the ridge and minutiae extraction.

3.2.2.1ridge And Minutiae Extraction

Given a gray-scale fingerprint image, a series of steps, computing the orientation image, frequency image computation, directional filtering,binarization and thinning, are used to produce a binaryimage. From the binary image, minutiae are detected and ridges are extracted by tracing. Each minutia has four features: x coordinate, y coordinate, direction and type (termination or bifurcation). Ridges are represented as lists of points. To simplify the representation of ridges, ridges associated with a bifurcation are treated as three ridges and a closed ridge is broken at a randomly selected point. Singular points are extracted using an improved version of the Point care index method. Each singular point has four features: x coordinate, y coordinate, direction (only defined for core), and type (core or delta).

3.2.2.2the Proposed Representation: Minutiae Direction Map

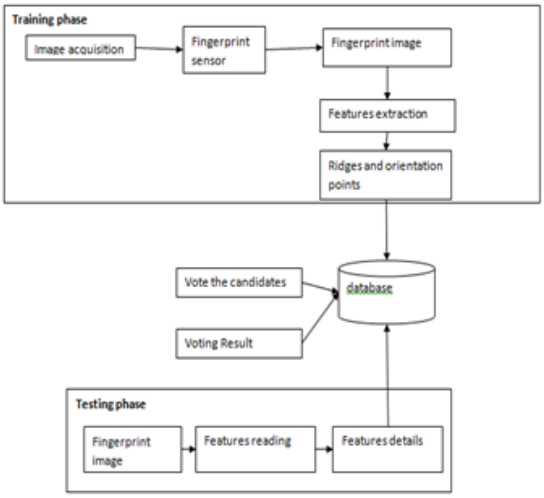
Phase correlation cannot be used to align two point sets directly. We present a new representation called Minutiae Direction Map (MDM) which is generated by converting minutiae point sets into a 2D image space. Alignment parameters are determined using phase correlation between two MDMs.

Let M=$((x_1,y_1,\propto_1),\ldots..(x_N,y_N \propto_N))$ denote the set of N minutiae in a fingerprint image. The image size is CxR and $(x_i,y_i \propto_i)$ are the three features (special position and orientation) associated with the ith minutiae in set M. define the MDM of set M as μ^M(m,n),m€[0,C-1], n€[0,R-1]. It contain the angle of minutiae direction at the position of minutiae points and 0 otherwise, which is written as

$$\mu^M(m,n)=\begin{cases} cos \propto_i + j\, sin \propto_i, & m = x_i, n = y_i \\ 0 & otherwise \end{cases}$$

3.2.2.3 Working Of Minutiae Extraction

The minutiae extractions consist of series of action. Among all the fingerprint features minutiae point features with corresponding orientation maps are unique enough for making distinctions. The minutiae feature representation reduces the complex fingerprint recognition problem to a point pattern matching problem. An accurate extraction and representation of the fingerprint feature is very important in automatic fingerprint recognition systems. Minutiae detection algorithm need to locate efficiently and accurately the minutiae points. There are various minutiae extraction algorithm available, they can be categorized into four groups. The first type of groups extracts minutiae points directly from the gray scale image. A second type of methods extracts minutiae from binary image. Third type of methods extracts minutiae using machine learning methods. The last type of methods extracts minutiae from binary skeletons. In paper we have concentrated on binary image.



3.2.2.4 Minutiae Points

Fingerprint ridges are not continuous, straight ridges. Instead, they are broken, forked, interrupted or changed directionally. The points at which ridges end, fork, and change are called minutia points which provide distinctive, identifying information.

There are five characteristics of minutia points in fingerprints:

1. Type

There are several types of minutia points. The most common are ridge endings and ridge bifurcations.

Ridge Ending – occurs when a ridge ends abruptly.

Ridge Bifurcation – the point at which a ridge divides into branches.

Dot or Island – a ridge that is so short it appears as a dot.

Enclosure – a ridge that divides into two and then reunites to create an enclosed area of ridge-less skin.

Short Ridge – an extremely short ridge, but not so short that it appears as a Dot or an Island.

Core Point-The core point, located at the approximate center of the finger impression, is used as a starting reference point for reading and classifying the print.

2. Orientation

The point on the ridge on which a minutia resides is called the orientation of the minutia point.

3. Spatial Frequency

Spatial frequency refers to how far apart the ridges are in relation to the minutia point.

4. Curvature

The curvature refers to the rate of change of ridge orientation.

5. Position

The position of the minutia point refers to its location, either in an absolute sense or relative to fixed points like the delta and core points

3.3sensor (Scanner Device)

The tool enables developers to perform basic fingerprint biometric operations: capturing a fingerprint from a Digital Persona fingerprint reader, extracting the distinctive features from the captured fingerprint sample, and storing the resulting data in a template for later comparison of a submitted fingerprint with an existing fingerprint template.

3.3.1 Fingerprint Authentication On A Remote Computer.

This SDK includes transparent support for fingerprint authentication through Windows Terminal Services (including Remote Desktop Connection) and through a Citrix connection to Metaframe Presentation Server using a client from the Citrix Presentation Server Client package. Through Remote Desktop or a Citrix session, you can use a local fingerprint reader to log on to, and use other installed features of, a remote machine running your fingerprint-enabled application.

The following types of Citrix clients are supported:

- Program Neighborhood
- Program Neighborhood Agent
- Web Client

To take advantage of this feature, your fingerprint-enabled application must run on the Terminal Services or Citrix server, not on the client.

3.3.2developing Citrix-Aware Application

This SDK includes support for fingerprint authentication through Windows Terminal Services (including Remote Desktop Connection) and through a Citrix connection to Metaframe Presentation Server using a client from the Citrix Presentation Server Client package.

The following types of Citrix clients are supported for fingerprint authentication:

- Program Neighborhood
- Program Neighborhood Agent
- Web Client

In order to utilize this support, your application (or the end-user) will need to copy a file to the client computer and register it. The name of the file is DPICACnt.dll, and it is located in the "Misc\Citrix Support" folder in the product package.

To deploy the DigitalPersona library for Citrix support:

1. Locate the DPICACnt.dll file in the "Misc\Citrix Support" folder within the product package.
2. Copy the file to the folder on the client computer where the Citrix client components are located (i.e. for the Program Neighborhood client it might be the "Program Files\Citrix\ICA Client" folder).
3. Using the regsvr32.exe program, register the DPICACnt.dll library.

If you have several Citrix clients installed on a computer, deploy the DPICACnt.dll library to the Citrix client folder for each client. If your application will also be working with Pro Workstation 4.2.0 and later or Pro Kiosk 4.2.0 and later, you will need to inform the end-user's administrator that they will need to enable two Group Policy Objects (GPOs), "Use DigitalPersona Pro Server for authentication" and "Allow Fingerprint Data Redirection"

3.3.3setting The False Accept Rate

This appendix is for developers who want to specify a false accept rate (FAR) other than the default used by the DigitalPersona Fingerprint Recognition Engine.

3.3.3.1 False Accept Rate(Far)

The false accept rate (FAR), also known as the security level, is the proportion of fingerprint verification operations by authorized users that incorrectly returns a comparison decision of match. The FAR is typically stated as the ratio of the expected number of false accept errors divided by the total number of verification attempts, or the probability that a biometric system will falsely accept an unauthorized user. For example, a probability of 0.001 (or 0.1%) means that out of 1,000 verification operations by authorized users, a system is expected to return 1 incorrect match decision. Increasing the probability to, say, 0.0001 (or 0.01%) changes this ratio from 1 in 1,000 to 1 in 10,000.Increasing or decreasing the FAR has the opposite effect on the false reject rate (FRR), that is, decreasing the rate of false accepts increases the rate of false rejects and vice versa. Therefore, a high security level may beappropriate for an access system to a secured area, but may not be acceptable for a system where convenienceor easy access is more significant than security.

3.3.3.2representation Of Probability

The DigitalPersona Fingerprint Recognition Engine supports the representation for the FAR probability that fully conforms to the BIOAPI 1.1, BIOAPI 2.0, and UPOS standard specifications. In this representation, the probability is represented as a positive 32-bit integer, or zero. (Negative values are reserved for special uses.). The definition PROBABILITY_ONE provides a convenient way of using this representation. PROBABILITY_ONE has the value 0x7FFFFFFF (where the prefix 0x denotesbBase 16 notation), which is 2147483647 in decimalnotation. If the probability (P) is encoded by the value (INT_N), thenProbability P should always be in the range from 0 to 1. Some common representations of probability are listedin column one of Table 2. The value in the third row represents the current default value used by theDigitalPersona Fingerprint Recognition Engine, which offers a mid-range security level. The value in the secondrow represents a typical high FAR/low security level, and the value in the fourth row represents a typical lowFAR/high security level.

The resultant value of INT_N is represented in column two, in decimal notation.

INT_N = P * PROBABILITY_ONE

P=(INT_N)/(PROBABILITY_ONE)

Probability P should always be in the range from 0 to 1. Some common representations of probability are listed in column one of Table 2. The value in the third row represents the current default value used by theDigitalPersona Fingerprint Recognition Engine, which offers a mid-range security level. The value in the secondrow represents a high FAR/low security level, and the value in the fourth row represents a typical low FAR/high security level.The resultant value of INT_N is represented in column two, in decimal notation.

Table 2. Common values of probability and resultant INT_N values

Probability (P)	**Value of INT_N in decimal notation**
0.001 = 0.1% = 1/1000	2147483
0.0001 = 0.01% = 1/10000	214748
0.00001 = 0.001% = 1/100000	21475
0.000001 = 0.0001% = 1/1000000	2147

3.4 Database

In our project we are using both local and centralized database. The data will be fetched from the local database. But the updation will be taken in both database. From the fingerprint we are taking major points like ridges,bifurcation and valleys from that we are ploting points using a direct mapping method only the points are stored in the database in binary format but scanner takes fingerprint as a template.

IV. CONCULSION

In this paper, we have presented a fingerprint-based management system. The developed system is part of a fingerprint recognition/authentication system based on minutiae points. The system extract the local characteristic of a fingerprint which is minutiae points in template based. Templates are matched during both registration and verification processes. For improved quality control during the registration or verification process, a matching score was used to determine whether correct user or not .The matching score was specified so that only sets of minutiae data that exceed the score will be accepted and data below the score will be rejected. Therefore,Fingerprint Recognition using Minutia Score Matching method was used for matching.

In this system, a framework for electronic voting machine based on biometric verification is proposed and implemented. The proposed framework ensures secured identification and authentication processes for the voters and candidates through the use of fingerprint biometrics. In the project wehave try to reduce the search time by using the local database instead of using one centralized database.

REFERENCE

[1] Sobia Baig, Ummer Ishtiaq, Lahore "Electronic Voting System Using Fingerprint Matching with Gabor Filter"

[2] Mark A. Herschberg, 1997 "Secure Electronic Voting Over the World Wide Web".

[3] M. Byrne, K. Greene, and S. Everett, "Usability of Voting Systems: Baseline Data for Paper, Punch Cards, and Lever Machines," ACM International Conference on Human Factors in Computing Systems, pp. 171–180, 2007.

[4] SussaneCaarls, "E-voting Handbook: Key Steps in the Implementation of E-enabled Elections", Council of Europe, 2010.

[5] Santin, R. Costa and C. Maziero, "A Three-Ballot- Based Secure Electronic Voting System", IEEE Transaction on Security & Privacy, Vol. 6(3), pp. 14- 21, 2008.

[6] Kumar, " Electronic voting machine- A review", IEEE International Conference on Pattern Recognition, Informatics and

Medical Engineering (PRIME), pp. 44-48, 2012.

[7] Jain and D. Maltoni, "Handbook of Fingerprint Recognition," Springer-Verlag, New York, USA, 2003.

[8] O. Iloanusi and C. Osuagwu, "Framework for a dynamic Fingerprint Indexing Biometric-based Voting System", African Journal of Computing & ICTs, pp. 55- 63, Vol. 5(4), 2012.

[9] Altun and M. Bilgin, "Web baesd secure e-voting system with fingerprint authentication", Scintific Research and Essays, pp. 2494-2500, Vol. 6(12), 2011.