Real-Time Voting System Using Biometrics

Nitin Chavhan, Ajit Deshmukh, Simran Bhat, Shilpa Kukade, Manjushree Mahajan
Department of Computer Engineering, GHRCEM, Wagholi, Pune, India
nchavhan39@gmail.com, ajitdeshmukh111@gmail.com, 11simranbhat@gmail.com,
kukadeshilpaa7m95@gmail.com

Abstract - "Real Time Electronic Voting System" depends on the online administrations like where a voter can utilize his/her voting right online with no trouble. In this framework individuals who have citizenship of India and whose age is over 18 years old can make choice online without setting off to any surveying stall. The race commission of India has kept up a database server in which every one of the names of the voter with finish data is put away. The voter needs to fill an enlistment shape to enroll himself with the assistance of a USER ID and DYNAMIC PASSWORD. This data is checked by the database server which has effectively all the data about the voter. In the event that conditions aren't right then that passage will be disposed of and he would not have the capacity to vote. This framework will be useful for voters who live far from their home city and need to make their choice from anyplace in India. The principle preferred standpoint of In this machine voting is that the level of voting will increment. It diminishes the cost and time of voting process and consequently it will be more secure.

KEYWORDS: Online E-voting, Distance voting, Finger Scanner Module, Database server, Verification.

I.   INTRODUCTION

REALTIME Electronic Voting Machine is a machine that is utilized to store the votes set up of ticket papers and boxes were utilized as a part of customary voting framework. Voting's are of two sorts Distance voting and Presence voting. In remove voting voter make his or her choice from a place other than a surveying corner i.e. by means of mail or web voting. In nearness voting a voter can make his choice at a surveying station. To expand the effectiveness and security of voting methods, electronic voting frameworks were created. Securing the voted information is the primary test of electronic voting, thus planning a safe e-voting framework is vital. In this manner security is the core of modernized e-voting framework where race information is recorded, put away and handled as computerized data. There are diverse levels of e-voting security. Web based voting process confirmation should be possible with unique finger impression detecting at the season of voting. To make the framework more secure we are making utilization of the Aadhar Card Number which is one of a kind for every individual. This whole framework can be executed utilizing login which requires the Name of the competitor, Aadhar Card Number and the unique mark check. Substantial voters will have their name, unique mark and different subtle elements in the administration database server for each state region shrewd. This will subsequently guarantee with the assistance of one of a kind Aadhar card number and unique mark scanner just genuine

clients can make their choice. Web based voting framework contains.

- Voters' information in database.
- Voters name with Id.
- Voters fingerprint scan.
- Voters vote in the database.
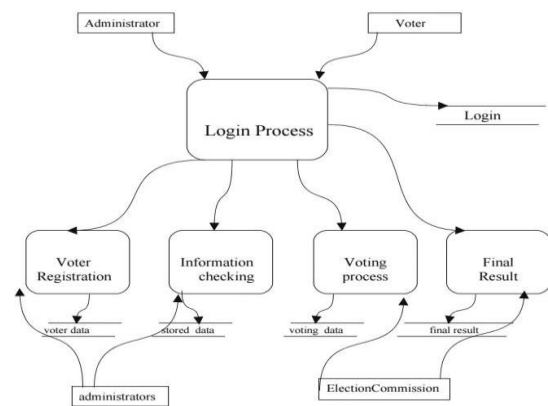
II.   E-VOTING PROCESS

A.   *How Does a Fingerprint Optical Scanner Work?*

A fingerprint scanner has two basic applications -- it needs to take an image of your finger perfectly, and it needs to determine whether the pattern of ridges and valleys in this image matches to that of pre-scanned images. Only specific characteristics, which are unique to every fingerprint, are filtered and saved as an encrypted biometric key or mathematical representation. No fingerprint image are ever saved, It can available series of numbers (binary code), which is used to verify. No one can duplicate your fingerprints because the algorithm cannot be reconverted to an image.

B.   *Advantages of Fingerprint Authentication*

There are several ways an electronic time clock system can verify that somebody is who they say they are. Most systems are looking for one or more of the following

· What you have ?
· What you know ?
· Who you are ?

You need some sort of "token," such as an identity card with a magnetic strip to get past a "what you have" system, A "what you know" system requires you to enter a password.

A "who you are" the system can be required for physical evidences that you are who you say you are a specific fingerprint pattern on the available system.

"Who you are" have a number of advantages, They are follows

· Fingerprints cannot be easily faked than identity cards.
· Guessing a fingerprint pattern is impossible like you can think and guess a password of any system.
· You cannot misplace your finger, like you can misplace an id cards any ware.
· You can't forget your fingerprints like you can forget or change password of any system.

III.   RELATED WORK

Most of the computer scientists who have done work in e-electronic voting seem to agree that online e-voting does not meet the requirements for public elections and that the current widely-deployed voting systems need improvement. In India first election using electronic voting was held from April 20 to May 10, 2004. The Electronic Voting Machine comes in a reusable carry pack and can operate on a battery power source in remote areas. According to Election authorities, each EVM can record five votes' minute or nearly 3,000 votes in a polling day. Throughout history, election fraud has occurred in many electoral processes from which experience shows that the manual voting process is major source of such vices and violence in many democratic countries. A case in point is the Kenyan Electoral Commission (IEBC) that has on several occasions failed to update the Kenyan national voters' register in time before the voting date. The recent EVM have also implemented real time clock and date-time facility which authorize them to record the real time and date whenever a key is pushed. In recent years, a considerable number of countries has adopted E-voting for their official elections. These countries include America, Belgium, Japan and Brazil.

IV.   MTHODOLOGY

The knowledge based (password) and token based (key or card) security systems are prone to compromise because passwords can be forgotten or guessed and cards can be lost or stolen. Biometrics which refers to automatic identification of a person based on his or her distinguishing characteristics, is inherently more secure than knowledge based or token based identification.

Our fingerprint-based biometric e-voting system is essentially a pattern recognition system a person may be authenticate of his/her fingerprint. The enrolment module is responsible for registering individuals in the biometric system database (system DB). During the enrollment checking phase, the available fingerprint of an individual person is acquired by a fingerprint

scanner to produce raw digital representation.
The steps involved in fingerprint recognition are explained as follows
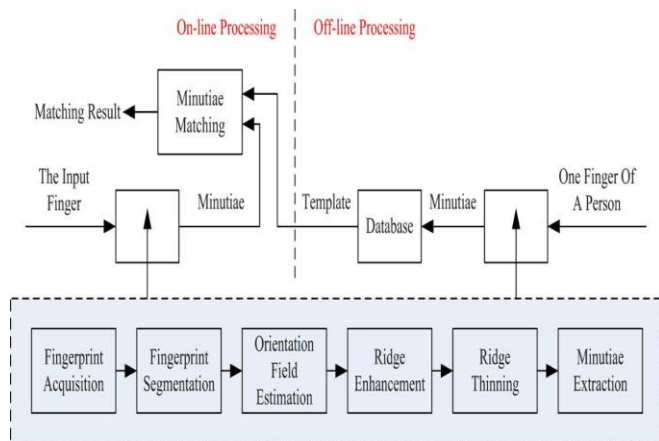
STEP 1: FINGERPRINT ACQUISITION

On the basis of collection procedure, fingerprint images can generally be classified into three categories, namely, rolled, plain and latent.

Rolled fingerprints are obtained from rolling the finger from one side to the other in order to capture all ridge details of the fingerprint.

Generating plain fingerprints images are acquired by pressing the fingertip on to a available flat surface. Latent fingerprints are usually storing from crime scenes, in which the print is lifted and object must be surfaces that were by mistake touched or handled.

A fingerprint image is classified based on the mode of acquisition as

   1.   Offline image

A fingerprint image assumption was performed by using "ink-technique" the finger can spread with black ink and pressed on paper card; the paper card was scanned by using a common paper card-scanner, producing the final digital image as per need.

2.   *Live scan image*

A digital image is directly obtained by placing the finger on the surface of a fingerprint reader. No ink is required in this method. The unique significant characteristics of fingerprint the readers can capturing the area their resolution.

Step 2: Fingerprint Segmentation

An automatic fingerprint recognition system is the important step in segmentation of fingerprint images. A captured fingerprint image are two types, which are called the foreground and the background. The foreground is the component that originated from the contact of a fingertip with the sensor. The noisy area at the borders of the image is called the background. The task of the fingerprint segmentation algorithm is to decide which part of the image belongs to the foreground and which part to the background. A fingerprint segmentation goal was discard the background, reduce the minimum number of false features, and thus improve maximum matching accuracy of system.

Step 3: Orientation Field Estimation

By considering a fingerprint as a texture pattern can be utilize the both fingerprint orientation and frequency information to segment latent. Most of the approaches proposed in the literature for singularity detection operate on the fingerprint orientation image. The orientation of the image represents the property of the available fingerprint images and also defines the invariant coordinates for available ridges. By viewing a fingerprint image as an oriented texture, a number of methods have been proposed to estimate the orientation field of fingerprint images.

Step 4: Ridge Enhancement

Uniqueness of the fingerprint is exclusively depended on the local ridge and relationships. The two most prominent ridge characteristics called minutiae are
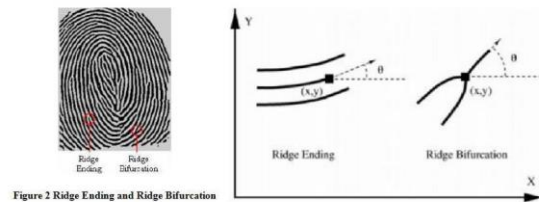
1. *Ridge ending*
    A ridge ending is defined as the point where a ridge ends abruptly.

2. *Ridge bifurcation*

A ridge bifurcation is defined as the point where a ridge forks or diverges into branch ridges.

Figure 2 Ridge Ending and Ridge Bifurcation

Step 5: Ridge Thinning

The final image can be enhancement step typically involving to performing prior to extraction is thinning. Morphological operation of thinning that erodes successively the foreground pixels until and one pixel is wide. A standard thinning algorithm is employed, which performs the thinning operation using two sub-iterations. The examining of an pixel each pixel sub-iteration begins by examining the neighborhood of each and every pixel in the binary image, and based on set of the pixels-deletion criteria, it checks whether the pixel can be deleted or not. These sub-iterations continue until no more pixels can be deleted. The important application of thinning algorithm it can responsible for preserving the fingerprint image and connectivity of the ridge structures while forming a skeleton zed version of the binary image. This skeleton image is then used in the subsequent extraction of minutiae.

Step 6: Minutiae Extraction

Almost maximum number of fingerprint features, minutia point features. The minutiae features can be representation of reducing the problem of complex fingerprint recognition and point to the pattern matching problem. Finally, a simple image scan allows the detection of pixels that correspond to minutiae through the pixel-wise Computation of crossing number. There are maximum number of minutiae extraction methods available . We can classify these methods broadly into two types .Those that work on binarized fingerprint images. Those that work directly on gray -scale fingerprint images.

Step 7: Minutiae Matching

Minutiae are extracted from the two fingerprints and stored as sets of points in the two-dimensional plane. The alignment can be find between template and input minutiae sets of that results in the available minutiae pairings. This is the most popular and widely used in commercial applications, because of its good performance and low computation time, especially for good quality images.

V.   PROPOSED WORK

A.   *Design Considerations*

The proposed system is focused on improving the existing

system by making voting available to all registered voter who cannot be present in home city during election period.

First voter need to register and give valid reason for his/her absence in city during election time. The authorized officials will then have to create a new record in database for that voter. Voter must give all required personal details to register for this system. Special record to be entered in database will be voters fingerprint. Id passwords are not required as voter will only need his/her Unique ID/Voter ID and fingerprint later to login. This system will bring increase in overall percentage of voting which will help to choose best leader. Following diagram show process of voting
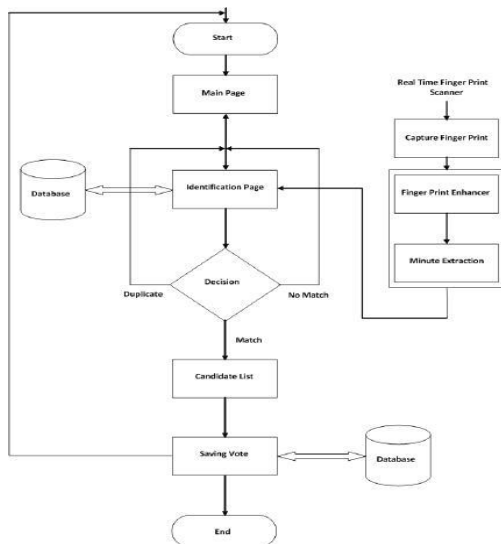
VI.   CONCLUSION AND FUTURE WORK

Paper voting based Election are never perfect, even in the world of paper ballots put into the boxes and lever machines read the outputs of dials. Today, volunteers are faced with electronic voting machines manufactured and maintained by private firms that have software that hasn't been rigorously tested and source code that is not available to experts of all political persuasions.

In this e-voting system will manage the Voter's information like voters Aadhar card and voting card details, by which voter can login and use his voting rights. The system will incorporate with all features of voting system. The system will have lesser cost, faster tabulation of results, improved accessibility, greater accuracy, and lower risk of human and mechanical errors.

Voter's detail will be stored in database after registration. Biometric voting system increases percentage of voting. It decreases the cost and time of voting process.

Future enhancements focused to provide online e-voting

with some authentication parameters like facial recognition. In case of usage offline e-voting authentication processes like, Finger Vein and iris matching and detection can be done.

REFERENCES

i.   Jean Bacon,Fellow, DavidEyers, Thomas F. J.-M. Pasquier, Jatinder Singh, Ioannis Papagiannis and Peter Pietzuch, "Biometrics using Electronic Voting System with Embedded Security", IEEE Transactions on Networkand Service Management, VOL. 11, NO. 1, MARCH 2014.

ii.   Reem Abdelkader and Moustafa Youssef, "UVote A Ubiquitous E-Voting System", 2012 Third FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing.

iii.   Claudia Garcya-Zamora, Francisco RodriguezHenriquez, Daniel Ortiz-Arroyo, "SELES An e-Voting System for Medium Scale Online Elections," enc, pp.50-57, Sixth Mexican International Conference on Computer Science (ENC'05), 2005.

iv.   Hsing-Chung Chen and Rini Deviani, "A Secure E-Voting System Based on RSA Time-Lock PuzzleMechanism", 2012 Seventh International Conference on Broadband, Wireless Computing, Communication and Applications.

v.   Balkrushna Bhagwatrao Kharmate, Shahebaz Shakil Shaikh, Prashant Ravindra Kangane, Tushar Anant Lad, Prof. Ashvini Y. Bhamare, "A Survey on Smart E-Voting System Based On Fingerprint Recognition", International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297 2007 Certified Organization) Vol. 3, Issue 9, September 2015.

vi.   Sanjay Kumar, Manpreet Singh, "DESIGN A SECURE ELECTRONIC   VOTING   SYSTEM   USING   FINGERPRINT TECHNIQUE", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 4, No 1, July 2013.

vii.   Alaguvel.R, Gnanavel.G2, Jagadhambal.K , "Biometrics using Electronic Voting System with Embedded Security", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 3, March 2013.

viii.   M.O Yinyeh, K.A. Gbolagade, "Overview of Biometric Electronic Voting System in Ghana", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, July 2013.

ix.   Firas Hazzaa, Seifedine Kadry, New System of E-voting Using Fingerprint, International Journal of Emerging Technology and Advanced Engineering", Vol 2, pp 355-363, 2012.

x.   Muhammad Imran Razzak, Rubiyah Yusof and Marzuki Khalid, "Multimodal face and finger veins biometric authentication", Scientific Research and Essays Vol. 5(17), pp. 2529-2534, 4 September, 2010.

xi.   Mrs. S.M.Shinde, Mrs. Priti Subramanium, "BIOMETRIC GSM VOTING SYSTEM", International Journal of Technical Research and Applications, Volume 1, Issue 4 (sept-oct 2013), PP.103-107.

xii.   Shanu Agrawal, Pradeep Majhi, Vipin Yadav, "Fingerprint Recognition Based Electronic Voting Machine", International Journal of Engineering and Technical Research ISSN 2321-0869, Special Issue.