Survey On Finger Print Based Voting System Using Rfid

A.Nandhini[1] , V.Venkatesa Kumar [2], M.Newlin Rajkumar[3]
[1] Dept of CSE
[2, 3]Assistant Professor, Dept of CSE
[1, 2, 3] ANNUNIVERSITY REGIONAL CAMPUS COIMBATORE

Abstract- *The world is growing in all aspects of the basic needs of the most exenduces human needs with the support of technologies. In the developing country like India, the Election Commission faces major difficulties in finger print based voting system. The voting system focus on matching the fingerprint with the already stored fingerprint in RFID card. Now a day, finger print based voting system is more essential to avoid the fake votes and to reduce the need of the manual requirements. To identify the accuracy of the voting system and to review the existing standards available is the need of the hour. Thus suitable methodologies which will be optimized for efficient voting system in vital. Thus survey a standard comparison of different voting methodologies in existence and to identify the difficulties involved in the voting systems.*

Keywords- Fingerprint matching, RFID card, Fingerprint module.

I. INTRODUCTION

India has largest voting system in the world, There are many different types of voting systems. Among them the most general types of them are:

- Paper-Based Voting Systems
- Direct-Recording Electronic Voting Systems
- Public Network DRE Voting Systems
- Precinct Count Voting Systems
- Central Count Voting Systems

Paper-based Voting Systems (PVS): record, count, and produce a tabulation of the vote count from votes that are cast on paper cards or sheets. Some PVSs may allow voters to make selections by means of electronic input devices. Voter selections are, however, not independently recorded, stored or tabulated by such input devices.

Direct-recording Electronic (DRE) voting systems: record votes by means of a ballot display provided with mechanical or electronic optical components which could be activated by the voter. Such systems record voting data and ballot images in computer memory components. Also, data processing is achieved by the use of computer programs.

Public network DRE voting systems (PNDRE): Make use of electronic ballots and transmit vote data from the polling stations to other locations over a public network. The votes may be transmitted as individual ballots as they are cast, or periodically as batches of ballots, or as one single batch, at the end of voting.

Precinct counts voting systems (PCVS): put the ballots in a tabular form at a particular place, say, a polling station. They provide mechanisms that store vote counts electronically and transmit the results to a central location over public telecommunication networks.

Central count voting systems (CCVS): Tabulate ballots from multiple precincts at a central location. Voted ballots are safely stored temporarily at the polling station. These ballots are then transported or transmitted to a central counting location. CCVSs may, in some cases, produce printed reports on the vote count.

Electronic voting is the use of computers or computerized voting equipment to cast ballots in an election. Sometimes, this term is used more specifically to refer to voting that takes place over the Internet. Electronic systems can be used to register voters, tally ballots, and record votes. This paper is organized as follows. Section two presents different types of electronic voting schemes and their implementations. Section three describes electronic voting systems around the world. Section four explains the advantages and disadvantages of electronic voting over traditional paper voting. The last section will conclude the overall paper. I Electronic voting (also known as E-voting) is voting using electronic systems to aid casting and counting votes. Electronic voting technology can include punched cards, optical scan voting systems and specialized voting kiosks (including self-contained direct-recording electronic voting systems, or DRE).

An EVM consists of two units:

- Control Unit
- Balloting Unit

The Control Unit is with the Presiding Officer or a Polling Officer and the Balloting Unit is placed inside the voting compartment. Instead of issuing a ballot paper, the Polling Officer in-charge of the Control Unit will press the Ballot Button. The controller used in EVMs has its operating program etched permanently in silicon at the time of manufacturing by the manufacturer. No one can change the program once the controller is manufactured. The main drawback of this system is that, the voter's ID checking process is manual hence the possibilities of illegal voting by a wrong candidate.

II. RELATED WORK

A real time fingerprint recognition system based on novel fingerprint matching strategy[1]. In this paper they present a real time fingerprint recognition system based on a novel fingerprint minutiae matching algorithm. The system is developed to be applicable to today's embedded systems for fingerprint authentication, in which small area sensors are employed. The system is comprised of fingerprint enhancement and quality control, fingerprint feature extraction, fingerprint matching using a novel matching algorithm, and connection with the other identification system. Here they describe their way to design a more reliable and faster fingerprint recognition system which is based on today's embedded systems in which small area fingerprint sensors are used. Experiment on FVC database, show our system has a better performance than comparable. And for the image enhancement and matching techniques they use high efficiency, it can also give a real time identification result with high reliability.

National ID card, electronic commerce, and access to computer networks are some scenarios where reliable identification is a must[2]. Existing authentication systems relying on knowledge-based approaches like passwords or token-based such as magnetic cards and passports contain serious security risks due to the vulnerability to engineering-social attacks and the easiness of sharing or compromising passwords and PINs. Biometrics such as fingerprint, face, eye retina, and voice offer a more reliable means of authentication. However, due to large biometric database and complicated biometric measures, it is difficult to design both an accurate and fast biometric recognition.

A correlation-based fingerprint verification system is presented[3]. Unlike the traditional minutiae-based systems, this system directly uses the richer grayscale information of the fingerprints. The correlation-based fingerprint verification system first selects appropriate templates in the primary fingerprint, uses template matching to locate them in the secondary print, and compares the template positions of both fingerprints. Unlike minutiae-based systems, the correlation-based fingerprint verification system is capable of dealing with bad-quality images from which no minutiae can be extracted reliably and with fingerprints that suffer from non-uniform shape distortions. Experiments have shown that the performance of this system at the moment is comparable to the performance of many other fingerprint verification systems.

Most fingerprint recognition techniques are based on minutiae matching and have been well studied[4]. However, this technology still suffers from problems associated with the handling of poor quality impressions. One problem besetting fingerprint matching is distortion. Distortion changes both geometric position and orientation, and leads to difficulties in establishing a match among multiple impressions acquired from the same finger tip. Marking all the minutiae accurately as well as rejecting false minutiae is another issue still under research. Our work combines many methods to build a minutia extractor and a minutia matcher. The combination of multiple methods comes from a wide investigation into research papers. Also, some novel changes like segmentation using morphological operations, improved thinning, false minutiae removal methods, minutia marking with special considering the triple branch counting, minutia unification by decomposing a branch into three terminations, and matching in the unified x-y coordinate system after a two-step transformation are used in the work.

A fingerprint image enhancement method, a refined Gabor filter, is presented [5]. This enhancement method can connect the ridge breaks, ensures the maximal gray values located at the ridge center and has the ability to compensate for the nonlinear deformations. It includes ridge orientation estimation, a Gabor filter processing and a refined Gabor filter processing. The first Gabor filter reduces the noise, provides more accurate distance between the two ridges for the next filter and gets a rough ridge orientation map while the refined Gabor filter with the adjustment parameters significantly enhances the ridge, connects the ridge breaks and ensures the maximal gray values of the image being located at the ridge center. In addition, the algorithm has the ability to compensate for the nonlinear deformations. Furthermore, this method does not result in any spurious ridge structure, which avoids undesired side effects of the subsequent processing and provides a reliable fingerprint image processing for the Fingerprint Recognition System. In a word, a refined Gabor filter is applied in fingerprint image processing, then a good quality fingerprint image is achieved, and the performance of Fingerprint Recognition System has been improved.

Biometrics now days consider as a very vital component used as personal identification, considering that the biometric identifiers impossible to be shared between people or lost and the individual's identity can be represented by them [6]. Biometric identification indicates to the use of eye, fingerprint, faces of the human being as well as speech characteristics. One of the most important parts of biometric process is the use of fingerprint. It is a very complicated issue, because of variations in unique impressions even in the same finger. There is one problem with the fingerprint which is different fingerprint impression seems to be similar, while the fingerprint impression belong to same person look different. That's why the fingerprint matching is a big deal. Fingerprint recognition is a term called from the electronic method of identifying or verifying fingerprints images belong to humans. As mentioned earlier fingerprints are considered most important forms of biometrics that have been used in order to check the individual's identity.

There are two modes used in fingerprint recognition systems the first one is the verification mode while the second mode called an identification mode. In other word the fingerprint can be designed to operate either in identification mode or verification mode. The verifies process in the verification mode done by making a comparison between the input fingerprint of the person with his own template which is saved in the database of the system. While on the other hand the identification mode the system search the fingerprint template has been stored in the database which is belong to the users in order to identify an individual. There are some techniques used in the fingerprint identification system to make the search process faster. These techniques called fingerprint classification and indexing technique.

III. METHODOLOGY

There are various method to check these verification processes of voter's for voting system, but all the process is only done by human. The fingerprint sensor is used to scan the finger print and RFID card to store the details about voter's. The RFID scanner to read the card data. In this paper they are doing to develop the voting system monitoring and fake votes avoidance using fingerprint matching. They are using GSM technology, matching technology.

S.NO	CONCEPT	PROBLEM STATEMENT	SOLUTION	METHODOLOGY/ COMPONENTS	PROS AND CONS
1	Online fingerprint identification with a fast and distortion tolerant hashing method.	Database misses match, high cost, Large database needed.	Using biometric voting to stop the fake votes and give more secure for voting.	Arduino Microcontroller, Creating voting page, Matching finger print.	Pros: highly secure to cast their votes. Cons:high cost,large database need.
2	A fingerprint verification system using the minutiae extraction technique	Poor quality impressions, Database misses match, high cost	Using minute extraction technique to verify the fingerprint.	Minutiae matching, Raspberry pie, Arduino microcontroller, Fingerprint sensor.	Pros:more secure. Cons: new database needed to cast their votes.
3	Paper-based electronic voting system	One user can vote many times, Do not have any database about a user.	Using ballot paper to Cast their vote.	Ballot papers and boxes	Pros:low cost,do not need large database. Cons:not secured.
4	Document ballot voting system	Marked by hands on a ballot paper, Counting of votes done electronically.	Using ballot paper to cast their vote and counting the votes electronically.	Ballot paper and boxes, Electronic machine.	Pros: Cost is low, Unity, reliability, isolation, Cons: not secured.
5	Smart Electronic Voting Machine System	No database has created.	Using smart voting system programmed to record voting data and then tabulates the voting data	Micro-Controller, Electronic voting machine, voter database.	Pros: Security. Reliability. Cons:not secured.

IV. CONCLUSION

In a voting system faces the lot of problems such as a manual checking process, hence the possibilities of illegal voting by a wrong candidate. And also, possibility of multiple votes by same person. Security Problems One can change the program installed in the EVM and tamper the results after the polling votes in favor of a chosen candidate. It can easily hacked by hackers. Most of the electronic voting machines used in the country do not have any mechanism by which the voter can verify their identity before casting the vote due to which fake voters can cast numerous fake votes. Thus the fingerprint, print based voting system. The system is the best solution and support for voting systems.

REFERENCES

[1] D. Mao, D. Maltoni, A. K. Jain, and S. Prabhakar (2003). Handbook of Fingerprint Recognition. Springer Verlag.
[2] Jain, K, Ross, A, Prabhakar, S (2004). An Introduction to Biometric Recognition. New York, USA.
[3] Farah Azirar, (2011). Fingerprint Recognition. Bachelor Thesis. School of Electronics and Physical Sciences, Department of Electronic Engineering, University of Surrey.
[4] Jawad Nagi, (2009). Design of an Efficient High-speed fingerprint Recognition System. Final Year Project Proposal. College of Engineering, Universiti Tenaga Nasional.
[5] Meng, T. Y. (2008). Electronic Voting Systems: Security Implications of the Administrative Workflow. University of the Aegean, Samosl Greece.
[6] Phil Brimblecombe, (2005). Face Detection Using Gabor filter, Bachelor Thesis. School of Electronics and Physical Sciences, Department of Electronic Engineering. University of Surrey.
[7] A. Ross, S. Das, and A. K. Jain (2010). A deformable model for fingerprint matching, Pattern Recognition. University of Michigan.
[8] Xiao Yun Jing and David Zhang (2009). A fingerprint Recognition Approach Based on minutiae DCT Feature Extraction. Nanjing University of Science.
[9] Phil Brimblecombe, (2005). Fingerprint identification Using Neural Networks, Bachelor Thesis. School of Electronics and Physical Sciences, Department of Electronic Engineering. University of Surrey.
[10] Mayuree Lertwatechakul & Siriporn Thammawaja (2009). Design a Secure Electronic Voting System formal and s Election. 94(2), 455-466.
[11] Brunsilius, J., et al. (2009). A Biometric-Secure e-Voting System for Election Processes. Digest of Technical Papers.
[12] L. L., & Davie, B. D. (2011). Computer Networks, Fifth Edition: A Systems Approach (The Morgan Kaufmann Series in Networking). Morgan Kaufmann; 5 edition.