SECURED ELECTRONIC VOTING MACHINE USING FINGERPRINT

Sagar Lahade, Akash Shinde, Yogita Ingle, Pooja Dhalpe, Prof. Ashwini Dhoke ,
Computer engineering department
Dr. D Y Patil Institute and engineering technology Pune India

Abstract:

The voting is most important part of the democracy countries. Voting is conducted for various purposes. It is the process of the collection of votes for the selection something among many. That shows peoples thinking. Traditional way of the voting system is centralized or decentralized we call it as polling booths where people votes are collected under supervisory authorities. Finally votes are counted by manually and results are displayed. This takes more time. To tackle this problem electronics machines are used in later system this system also error prone. In the system we proposing new technique which uses biometric polling. This can improve the efficiency, provide security, scalability and save time. After polling, system can automatically show the results and winner of the poll. Voting can be done on the manual machines. The main advantage of system, we already store the database of fingerprints and other details such as adhar card system. Valid users can only vote that is eligible these avoid best solution to avoid the false voting.

***Index Terms* – fingerprint, minutiae extraction, Biometrics, image processing**

1 .INTRODUCTION

Through the traditional voting system and other approaches they may be chance of the fake voting. This takes more work accordance with man power and counting of votes manually and takes more time for the voting results .We are proposing an voting system based on fingerprint which totally eliminates the fake voting. Fingerprint based secured voting system is a set of systematic and analytical process for pro viding the information regarding candidate voting results at the particular time. We have totally focused on minimum resources cost and fast result. It includes the preparation of voting statistical summaries and resources acquisition.

2 .PROBLEM STATEMENT

To suggest the government to use latest biometric technology for voting system. Now a days the entire polling was operated by the electronic machines. That is the time consuming task and chances of the false voting, so we develop the system which can improve the polling process and achieve secure results

3 .LITERATURE REVIEW

The minutiae extractor processes the fingerprint image to identify specific details known as minutiae points that are used to distinguish different users. Minutiae points represents location where friction and ridges end abruptly or where a ridge branches into two or more ridges. A typical good-quality finger-print image contains about 20-70 minutiae points; the actual number depends on the size of the sensor surface and how the user places his or her finger on the sensors. The system stores the minutiae information location and direction along with the user demographic information as a template in the enrollment database.

During the identification phase, the user touches the same sensor, generating a new fingerprint image called a query print. Minutia points are extracted from the query print, and the matcher module compares the query minutia set with the stored minutia templates in the enrollment database to find the number of common minutia points. Due to variations in finger placement and pressure applied on the sensor, the minutia points extracted from the template and query fingerprints must be aligned or registered, before matching.

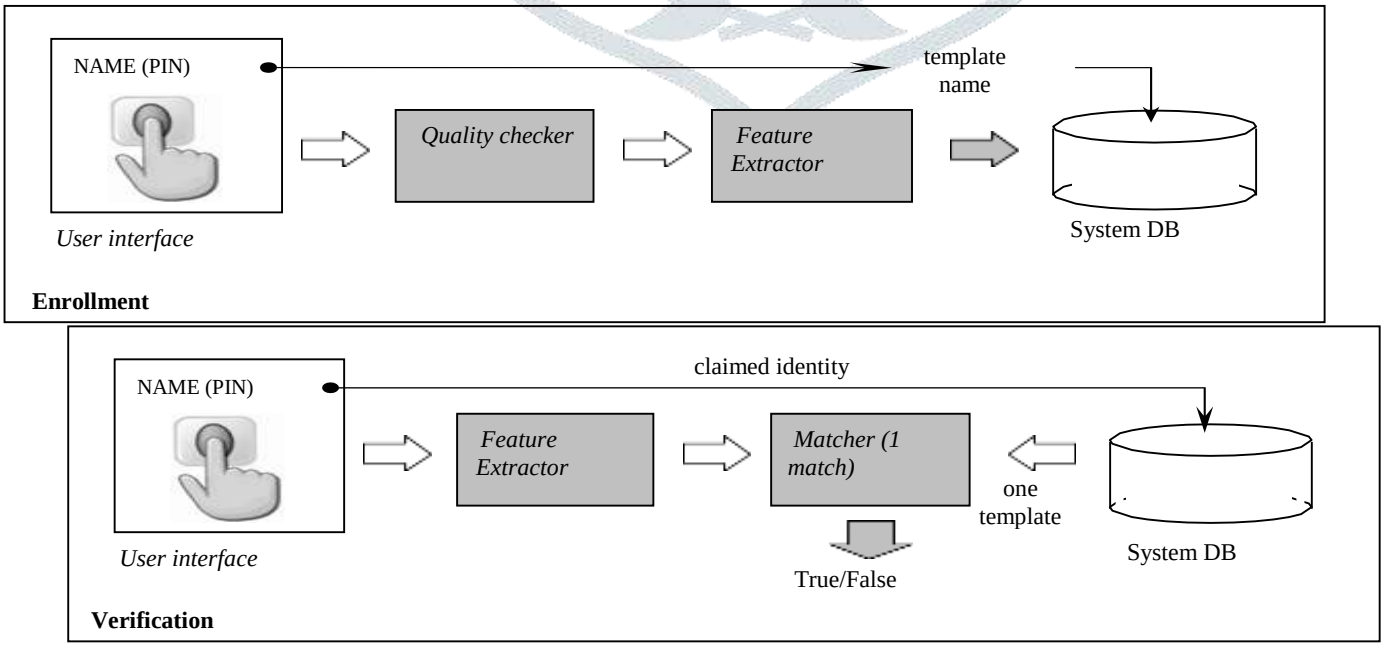
Fingerprints can be sensed using numerous technologies. The traditional ink and paper method, still used by many law enforcement agencies, involves applying ink to the finger surface, rolling the finger from one side of the nail to the other on a card, and finally scanning the card to generate a digital image. In the more popular live-scan method, a digital image is directly obtained by placing the finger on the surface of a fingerprint reader. Optical sensors based on the frustrated total internal reflection (FTIR) technique are commonly used to capture live scan fingerprints in forensic and government applications, while solid-state touch and sweep sensor silicon-based devices that measure the

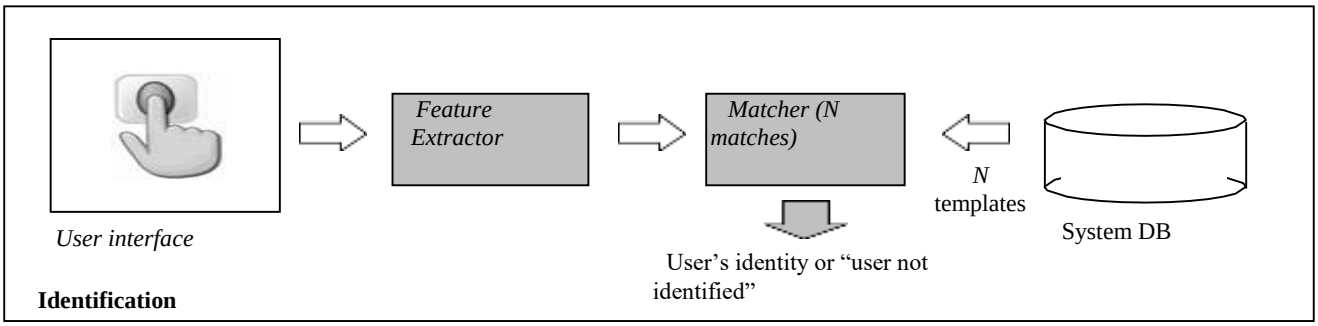
differences in Feature extraction. Features extracted from a fingerprint image are generally categorized into three levels. Level 1 features capture macro details such as friction ridge flow, pattern type, and singular points. Level 2 features refer to minutiae such as ridge bifurcations and endings Level 3 features include all dimensional attributes of the ridge such as ridge path deviation, width, shape, pores edge contour, and other details, including incipient ridges, creases, and scars. Level 1 features can be used to categorize fingerprints into major pattern types such as arch, loop, or whorl; level 2 and level 3 features can be used to establish a finger- prints individuality or uniqueness. Higher-level features can usually be extracted only if the fingerprint image resolution is high. For example, level 3 feature extraction requires images with more than 500-ppi resolution. The flow chart of a typical minutiae feature extraction algorithm.

First, the algorithm estimates the friction ridge orientation and frequency from the image. Matching A fingerprint matching module computes a match score between two fin- fingerprints, which should be high for fingerprints from the same finger and low for those from different fingers. Fingerprint matching is a difficult pattern-recognition problem due to large intra class variations (variations in fingerprint of same finger) and large interclass similarity (similarity between finger- print images from different fingers). Intra class variations are caused by finger pressure and translation, and contact area with respect to the sensor and condition of the finger such as skin dryness and cuts. Meanwhile, interclass similarity can be large because there are only three types of major fingerprint patterns (arch, loop, and whorl).Most fingerprint-matching algorithms adopt one of four approaches : image correlation, phase matching, skeleton matching, and minutiae matching. Minutiae- based representation is commonly used. A *fingerprint-based biometric system* is essentially a pattern recognition system that recognizes a person by determining the authenticity of her fingerprint. Depending on the application context, a fingerprint-based biometric system may be called either a *verification* system or an *identification* system:

- A verification system authenticates a person's identity by comparing the captured fingerprints with her own biometric template(s) pre-stored in the system. It conducts one-to-one comparison to determine whether the identity claimed by the individual is true.
- An identification system recognizes an individual by searching the entire template database for a match. It conducts one-to-many comparisons to establish the identity of the individual.

The block diagrams of a fingerprint-based verification system and an identification system are depicted in Figure 1; user enrollment, which is common to both tasks is also graphically illustrated. The enrollment module is responsible for registering individuals in the biometric system database (system DB). During the enrollment phase, the fingerprint of an individual is acquired by a fingerprint scanner to produce a raw digital representation. A quality check is generally performed to ensure that the acquired sample can be reliably processed by successive stages.





Block diagrams of enrollment, verification, and identification tasks.

Recent developments in fingerprint scanners have focused on reducing both their cost and size. Although lower cost and size are essential to enable a wide deployment of the technology in civilian applications, some of these developments have been made at the expense of fingerprint image quality (e.g., dpi resolution, etc.). It is very likely that while the market will continue to drive down scanner prices, it will also require higher-quality products at the same time. Manufacturers will continue to innovate low-cost small-size scanner designs, but they will also take care that their products deliver high quality-images of large areas of the finger. Robust extraction of fingerprint feature remains a challenging problem, especially in poor quality fingerprints.

Development of fingerprint-specific image processing techniques is necessary in order to solve some of the outstanding problems. For example, explicitly measuring (and restoring or masking) noise such as creases, cuts, dryness, smudginess, and the like will be helpful in reducing feature extraction errors. Algorithms that can extract discriminative non-minutiae-based features in fingerprint images and integrate them with the available features and matching strategies will improve fingerprint matching accuracy. New (perhaps, model-based) methods for computation (or restoration) of the orientation image in very low-quality images is also desirable to reduce feature extraction errors. Most of the fingerprint matching approaches introduced in the last four decades are minutiae-based, but recently correlation-based techniques are receiving renewed interest. New texture-based methods have been proposed and the integration of approaches relying on different features seems to be the most promising way to significantly improve the accuracy of fingerprint recognition systems.

4. MATHEMATICAL MODEL

$$S = \{_D = \{v1' v2' \cdots vn\}, C = \{c1' c2' \cdots cn\}, f' fc' p' R' o' V' G' s\}$$

Where, S is the start of the system and it is the set if the processes for e-voting

$$D = \{v1' v2 \cdots vn\} \quad (1)$$

D is the database of the

$$f = fc(f) \quad (2)$$

f is the fingerprint in equation to 2 we scan the fingerprint fc

Then we extract feature from the image and preprocess

$$s = \{_{es' rs}\} \quad (3)$$

s = segmentation of image

es = edge based segmentation.

rs = region based segmentation

f = feature extraction

$$F(_C) = \int_0^{\infty}(_s + f + DN) \quad (4)$$

After preprocessing system recognize with database fingerprint for verify voter

O = otp

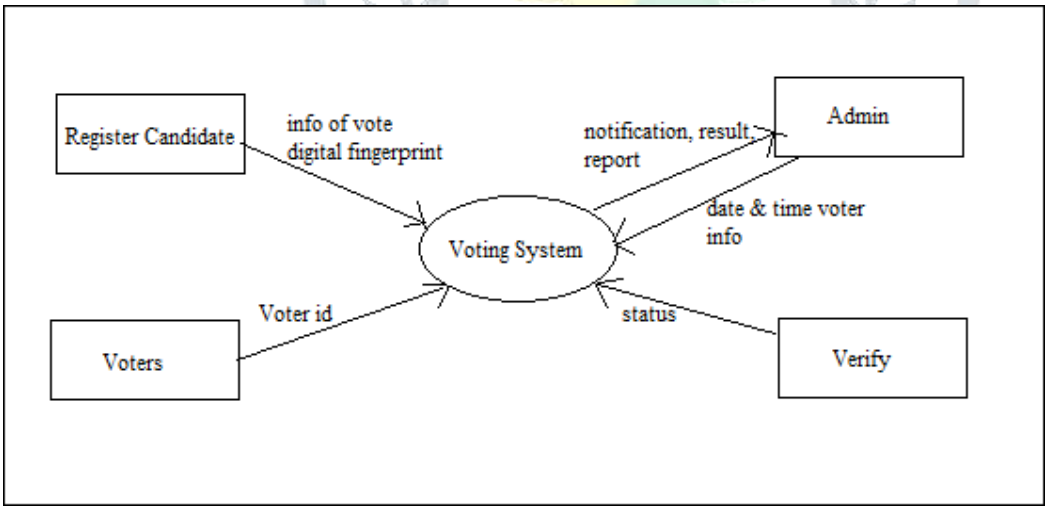
V= Vote the candidate

$$V = vote(_C) \quad (5)$$

$$G = \sum_{i=0}^{n}(_V) \quad (6)$$

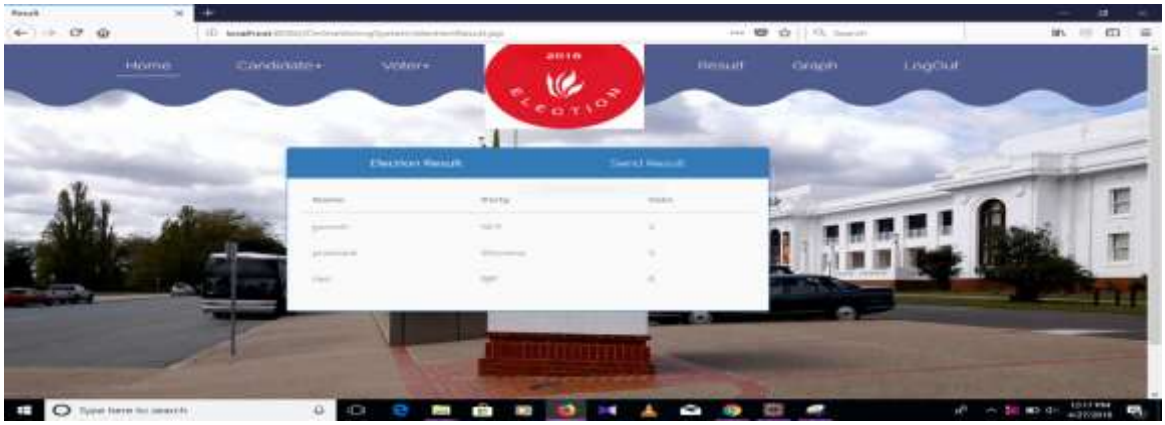
G is the final results generated by calculating votes

5. SYSTEM OVERVIEW



Above figure shows the overall dataflow of project. First we have to register candidates who are standing for election. We have to upload there details along with their fingerprint also. All these activities will done with access of admin. .After registration of candidates next step is to upload all the detail of voters who will be going to vote. After voting process has finished then admin will take further controls.it will check, verify fingerprints and count the total number of votes and system generates the results within seconds.

6. RESULT AND DESCUSSION



Above figure shows an sample results generated by the system. It will shows the total number of votes gained each candidate. It include name of winner .it will also shows the election voting graph as we as number of voting graph.

7. ADVANTAGES

The advantage of this system it will suggesting use latest fingerprint technology for voting system which reduces human cost, resources cost, and time for election. This system avoiding fake votes. It has powerful identifications of voters.

8. APPLICATIONS

- This system can be useful in election process conducted at local level such as GS selection at college level, team leader selection at organization.
- It would be useful at simple election process in organization such as bank, college, university, nongovernment organization.
- It can be used as global level such as parliament level election with some enhancement in features and adopt policy by government.
- The fingerprint based voting system can be used in each local level.

9. CONCLUSION

We have implemented project ”secured electronic voting machine using fingerprints ”suggested secured and efficient voting machine which is saving lot of time and resources required for voting transaction rather than existing traditional EVM machines. We have learned and implemented various key features such as image extraction process, fingerprint mechanism and counting accuracy and minutiae extraction algorithm we come to know that this algorithm has good time and space complexity than any other algorithm.

10. REFERENCES

1.Ballard, D.H.: Generalizing the Hough Transform to Detect Arbitrary Shapes. Pattern Recognition, vol. 3, no. 2 (1981) 110□122.

2. Bazen, A.M., Gerez, S.H.: Systematic Methods for the Computation of the Directional Fields and Singular Points of Fingerprints. IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 24, no. 7 (2002) 905□919.

3. Bazen, A.M., Verwaaijen, G.T.B., Gerez, S.H., Veelenturf, L.P.J., van der Zwaag, B.J.: A Correlation-Based Fingerprint Verification System. Proc. Workshop on Circuits Systems and Signal Processing (ProRISC 2000) (2000) 205□213

4 .Criminal Justice Information Services: Electronic Fingerprint Transmission Specification. Int. Report. CJIS-RS-0010 (V7), (1999), available at: http://www.fbi.gov/hq/cjisd/iafis/ efts70/cover.htm.

5 .Donahue, M.L, Rokhlin, S.I.: On the use of Level Curves in Image Analysis. CVGIP: Image Understanding, vol. 57, no. 2 (1993) 185□203.

6 .Golfarelli, M., Maio, D., Maltoni, D.: On the Error-Reject Tradeoff in Biometric Verification Systems. IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 19, no.7, (1997) 786□796.