INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGY & CREATIVE ENGINEERING (ISSN:2045-8711)
VOL.1 NO.1 JANUARY 2011

A Novel design of Electronic Voting System Using Fingerprint

D. Ashok Kumar[#1], T. Ummal Sariba Begum[#2]

[#1]*Department of Computer Science, V .S.S. Government Arts College, Pulankurichi – 630 405, Sivagangai, Tamil Nadu, India*

[#2]*UGC Research Fellow, V.S.S. Government Arts College, Pulankurichi – 630 405, Sivagangai, Tamil Nadu, India*

Abstract— *The heart of democracy is voting. The heart of voting is trust that each vote is recorded and tallied with accuracy and impartiality. The accuracy and impartiality are tallied in high rate with biometric system. Among these biometric signs, fingerprint has been researched the longest period of time, and shows the most promising future in real-world applications. Because of their uniqueness and consistency over time, fingerprints have been used for identification over time. However, because of the complex distortions among the different impression of the same finger in real life, fingerprint recognition is still a challenging problem. Hence in this study, the authors are interested in designing and analysing the Electronic Voting System based on the fingerprint minutiae which is the core in current modern approach for fingerprint analysis. The new design is analysed by conducting pilot election among a class of students for selecting their representative. Various analysis predicted shows that the proposed electronic voting system resolves many issues of the current system with the help of biometric technology.*

Keywords— **Biometric, Fingerprint, Minutiae, Electronic Voting.**

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 behaviours and must be sufficiently transparent and comprehensible that voters and candidates can accept the results of an election. In context of Western democracies' current crisis, electronic voting has become a very popular topic of discussion in academic and technical circles.

Voting is a method for a group such as a meeting or an electorate to make a decision or express an opinion—often following discussions, debates, or election campaigns. It is often found in democracies and republics. Electronic voting (also known as e-voting) is a term encompassing several different types of voting, embracing both electronic means of casting a vote and electronic means of counting votes.

For many years, paper-based ballot is used as a way to vote during campus election day. This matter put an inefficient way of voting process as students have to queue up to register their name before they can vote. Furthermore, the traditional way of voting will take a long process and time. So, the novel electronic voting using minutiae will become the best solution for the matters; besides provide easier way of voting. Compared to existing voting system the Electronic voting has several advantages like: Electronic voting system is capable of saving considerable printing stationery and transport of large volumes of electoral material. It is easy to transport, store, and maintain. It completely rules out the chance of invalid votes. Its use results in reduction of polling time, resulting in fewer problems in electoral preparations, law and order, candidate's expenditure, etc. and easy and accurate counting without mischief at the counting centre. It is also eco friendly [8].

Biometrics is the automated recognition of individuals based on their behavioural and biological characteristics. Biometric recognition means by measuring an individual's suitable behavioural 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 distinctiveness, persistence, 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 [28].

Because biometric identifiers cannot be easily misplaced, forged, or shared, they are considered more reliable for person recognition than traditional token or knowledge based methods. The objectives of biometric recognition are user convenience (e.g., money withdrawal without ATM card or PIN), better security (e.g., difficult to forge access), and higher efficiency (e.g., lower overhead for computer password maintenance). The tremendous success of fingerprint based recognition technology in law enforcement applications, decreasing cost of fingerprint sensing devices, increasing availability of inexpensive computing power, and growing identity fraud/theft have all ushered in an era of fingerprint-based person recognition applications in commercial, civilian, and financial domains. So the Electronic voting system has to be improved based on the current technologies viz., biometric system.

There are some previous works which uses fingerprint for the purpose of voter identification or authentication. As the fingerprint of every individual is unique, it helps in maximizing the accuracy. 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.

Fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. 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 [7]. In this study, for the fingerprint authentication the minutiae based matching is considered for higher recognition accuracy. Also, the matching accuracy of fingerprint based authentication systems has been shown to be very high. Fingerprint – based authentication systems continue to dominate the biometrics market by accounting for almost 52% of authentication systems based on biometric traits [2].

This paper is organized as follows: The section II describes the issues of the present voting system, section III discusses the fundamentals of finger print authentication system Section III describes the proposed novel application for Electronic Voting Systems, Section IV describes the Experimental Results of a pilot election conducted among a class of students to chose their representative and Section V concludes and states the future work plans.

II. ISSUES OF PRESENT VOTING SYSTEM

There has been several studies on using computer technologies to improve elections [5, 38, 21, 22, and 29].

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 electronic voting system should have [30]:

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.

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.

- Constant spending funds for the elections staff every year.

So, the proposed electronic voting system has to be addressed these problems.

III FUNDAMENTALS OF FINGERPRINT AUTHENTICATION SYSTEM

The types of information that can be collected from a fingerprints friction ridge impression can be categorized as Level 1, Level 2, or Level 3 features as shown in fig 1. Level 2 features or **minutiae** refer to the various ways that the ridges can be discontinuous. These are essentially Galton characteristics, namely ridge endings and ridge bifurcations. 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. Minutiae are the most prominent features, generally stable and robust to fingerprint impression conditions. The distribution of minutiae in a fingerprint is considered unique and most of the automated matchers use this property to uniquely identify fingerprints. Uniqueness of fingerprint based on minutiae points has been quantified by Galton [7]. Statistical analysis has shown that Level 2 features have sufficient discriminating power to establish the individuality of fingerprints [34].

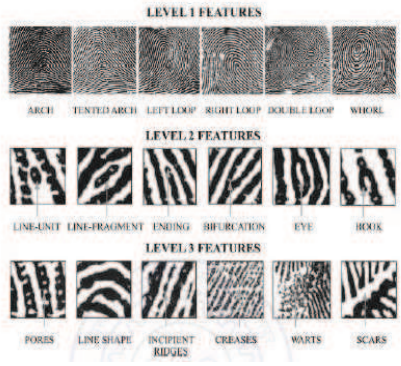

Fig 1 Fingerprint features at Level 1, Level 2, and Level 3 [36, 23]

The Fig 2 shows the clear view of minutiae. A minutia is characterized by its location and orientation.

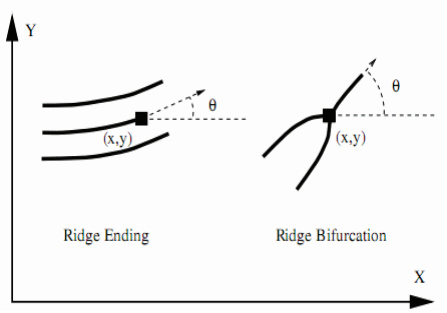

Fig 2 Characteristic Attributes of a Minutiae

In a recently published World Biometric Market Outlook (2005-2008), analysts predict that the average annual growth rate of the global biometric market is more than 28%, by 2007 [11]. The technologies that would be included in this are fingerprint technology by 60%, facial & iris by 13%, keystroke by 0.5% and digital signature scans by 2.5% Basically there are two types of fingerprint Recognition System:

(1) AFAS (Automatic Fingerprint Authentication System)
(2) AFIS (Automatic Fingerprint Identification / Verification System)

1) AFAS (Automatic Fingerprint Authentication System) Components of AFIS are: [40] [10][42]

1. Physical Fingerprint required as input.
2. Input is processed by using various image processing tools and databases and Classification of Fingerprints. The basic fundamental steps of these systems (see Fig (3) are image acquisition, pre-processing segmentation, enhancement etc), feature extraction, matching along with classification through databases. Authentication or verification systems authenticate the person's identity by comparing the own biometric template(s) stored in database (One-to-One comparison). An identification system recognize an individual by searching the entire templates in database for match (One-to-Many Comparison) [31] [17].

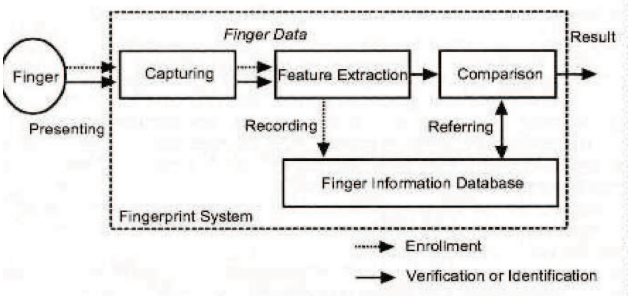

Fig 3 Typical Structure for Fingerprint System [16]

2) AFIS (Automatic Fingerprint Identification/ Verification System)

A fingerprint recognition system operates either in verification mode or in identification mode. The various stages in a fingerprint verification system are shown in Fig 4.

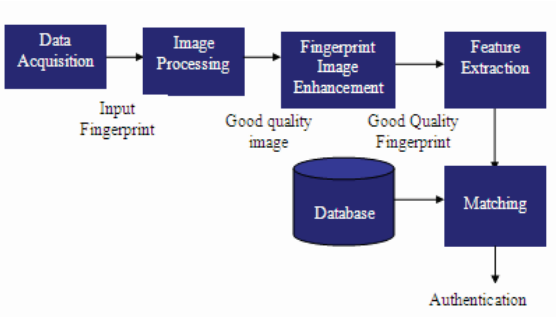

Fig 4 Architecture of Fingerprint Verification System

The first stage is the data acquisition stage in which a fingerprint image is obtained from an individual by using a sensor. The next stage is the pre-processing stage in which the input fingerprint is processed with some standard image processing algorithms for noise removal and smoothening. The pre-processed fingerprint image is then enhanced using specifically designed enhancement algorithms which exploit the periodic and directional nature of the ridges. The enhanced image is then used to extract salient features in the feature extraction stage. Finally, the extracted features are used for matching in the matching stage.

Data Acquisition: Traditionally, in law enforcement applications fingerprints were acquired off-line by transferring the inked impression on a paper. Nowadays, the automated fingerprint verification systems use live-scan digital images of fingerprints acquired from a fingerprint sensor. These sensors are based on optical, capacitance, ultrasonic, thermal and other imaging technologies. The techniques followed in these sensors are discussed in [2].

Image Pre-processing: The preprocessing steps try to compensate for the variation in lighting, contrast and other inconsistencies which are introduced by the sensor during the acquisition process. The paper [1] discusses the pre- processing steps generally used, which are Gaussian Blur, Sliding-window Contrast Adjustment, Histogram based Intensity Level and etc.,

Fingerprint Image Enhancement: The Performance of fingerprint feature extraction and matching algorithms relies heavily on the quality of the input fingerprint images. Due to various factors such as skin conditions (e.g., we, dry, cuts, scars and bruises). Non-uniform finger pressure, noise introduced by sensor and inherently poor-quality fingers (e.g., manual workers, elderly people), a significant percentage of fingerprint images is of poor quality. In fact, a single fingerprint image may contain regions of good, medium, and poor quality. Thus an enhancement algorithm which can improve the quality of ridge structure is necessary. A survey on different enhancement techniques can be found in [2]. The paper [9] describes the popular enhancement algorithm by Sharat et al. [33], which used contextual filtering in Fourier domain. In paper [24], the enhancement technique like histogram, Fourier and Gabor are compared and best technique gabor is found.

There has been lot of interesting work done in enhancing fingerprints. Sherlock [35] proposed enhancing the features in a fingerprint image by directional Fourier filtering. This frequency domain filtering is computationally less expensive than the spatial convolution of the image with filters. The filtered image is usually binarized or thinned for feature extraction. But there has been an effort to extract features from grey scale images, Maio and Maltoni [16] proposed an algorithm to extract features from gray scale images. The feature extraction algorithm has usually been employed on thinned images. Jain [11] and Ratha [27] developed algorithms for thinned images, their approach has involved local neighbourhood based processing on the images.

Many authors have identified the need to perform post processing on fingerprint images to remove the false minutiae, Ratha et al., where the minutiae are validated based upon heuristics like distance. Since the fingerprint based system rely on matching between the query fingerprint and the database fingerprint, classification of the database results in the query only searching in a particular class. Many attempts [16] [20] have been made to classify the fingerprints based upon core as well as delta points; these have been point based approach. The matching forms the heart of any fingerprint; the query fingerprint of even a client is usually a transformed version of the database fingerprint. This involved registration of the images before obtaining the match. There have been several prior approaches that addressed this. Ranade and Rosenfield [26] proposed an iterative approach for obtaining point correspondences.

The fingerprint enhancement techniques proposed by Chen et al. [27], is based on the convolution of the image with Gabor filters which has the local ridge orientation and ridge frequency. The algorithm includes normalization, ridge orientation estimation, ridge frequency estimation and filtering.

The paper [24] evaluates the performance of three types of image enhancement techniques and their impact in minutiae detection. In this work we have taken the account of hough transformation and

analyzed the results with previous referred transformations.

Feature Extraction: In this section I describe various levels of feature in fingerprint**.** The levels of features which is to be extracted are Minutiae, Pores, Ridge Contour Extraction.

Minutiae Extraction The next step after enhancement of the image is the extraction of minutiae. The enhanced image is binarized first in this step. The skeleton of the image is then formed. The minutiae points are then extracted by the following method. The binary image is thinned as a result of which a ridge is only one pixel wide. The minutiae points are thus those which have a pixel value of one (ridge ending) as their neighbour or more than two ones (ridge bifurcations) in their neighbourhood. This ends the process of extraction of minutiae points.

Let (x, y) denote a pixel on a thinned ridge, and N0, N1,…, N7 denote its eight neighbours. A pixel (x, y) is a

Ridge ending if $(\sum_{i=0}^{7} Ni) = 1$

Ridge bifurcation if $(\sum_{i=0}^{7} Ni) > 2$

Pores extraction: Pores are extremely fine details which are lost after the enhancement stage. Kryszczuk et al. [15] and [3] have proposed skeletonization based approach for pore extraction. Jain et al. [13] have proposed a pore extraction technique directly from gray scale image. . A recent study [9] by the International Biometric Group has proposed a new approach for pore extraction which utilizes orientation information of pores along with the location information.

Ridge Contour Extraction: Ridge contours can be extracted by using classical edge detection algorithms. Jain et al [13] have proposed an algorithm to extract the ridge contours which used a simple filter to detect ridge contours.

Fingerprint Matching: A variety of automatic fingerprint matching algorithms have been proposed in the pattern recognition literature. A useful literature survey on fingerprint recognition can be found in [2].

One family uses correlation based matching [4]. [6] and [19]. Correlation matching is less tolerant to rotational and translational variances of the fingerprint and of extra noise in the image. Another family uses Minutiae-based matching [37], [10], [14]. Minutiae matching are certainly the most well known and widely used method for fingerprint matching. In general minutiae matching are considered by most to have, higher recognition accuracy. The last family uses Ridge feature based matching [12]. Jain et al [12] proposed a local texture analysis where the fingerprint area of interest is tessellated with respect to the core point and finger code obtained. The paper [32] proposed a fingerprint matching which is more robust at shift and rotation of the fingerprints while it is of high accuracy. A Survey on Ridge feature based matching techniques is proposed in paper [1].

Minutiae based Matching

Let T and Q be the feature vectors, representing minutiae points, form the template and query fingerprint, respectively. Each element of these feature vectors is a minutiae point, which may be described by different attributes such as location, orientation, type, quality of the neighbourhood region, etc. The most common representation of a minutiae is the triplet x, y, θ where x, y is the minutiae location and θ is the minutiae angle. Let the number of minutiae in T and Q be m and n, respectively.

$T=m_1, m_{2,}\ldots, m_m, \quad m_i = x_i, y_i, \theta_i, \quad i=1\ldots m$

$Q=m'_1, m'_{2,\ldots,}m'_{ni} \quad m'_j = x'_j, y'_j, \theta'_j, \quad j=1\ldots n$

(9)

A minutiae m_i in T and m_j' in Q are considered matching, if following conditions are satisfied:

$$sd(m'_j, m_i) = \sqrt{((x'_j-x_i)^2+(y'_j-y_i)^2)} \le r_o$$

$$dd(m'_j, m_i) = \min(|\theta'_j - \theta_i|, 360 - |\theta'_j - \theta_i|) \le \theta_o$$

(10)

Here, r_0 and θ_0 are the parameters of the tolerance window which is required to compensate for errors in feature extraction and distortions caused due to skin plasticity.

The number of "matching" minutiae points can be maximized, if a proper alignment (registration parameters) between query and template fingerprints can be found. Correctly aligning two fingerprints requires finding a complex geometrical transformation function (map ()), that maps the two minutiae set (Q and T) the desirable characteristics of map () functions are: it should be tolerant distortion; it should recover rotation, translation and scale parameters correctly.

For the fingerprint enhancement technique, we compare the four types of fingerprint enhancement technique viz., Histogram, Fourier filter, Hough Transform and Gabor filter and find the best enhancement based on the following measures

III. A NOVEL ELECTRONIC VOTING SYSTEM

The main core of this study is to design an electronic voting system based on fingerprint minutiae is discussed in this section by two phases: i) Enrolment Process and ii) Voting Process.

i) Enrolment Process

The Fig 6 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. 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.

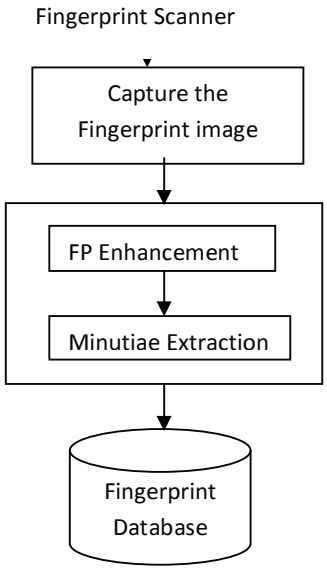

Fig 6 Enrollment Process

ii) A Novel Design for E-Voting Process

In the Fig 7, the first process is capture the input image, the captured image is then enhanced by using the best enhancement technique Gabor. The next step after enhancement is the extraction of minutiae. After extracting minutiae, it is compared with the template which is stored in the database based on minutiae based matching as proposed in the previous chapter. If the matching result is true, the person is allowed to vote. Otherwise he is rejected and give the beep sound. The person who is authenticated may vote for their beloved one by giving his fingerprint to the fingerprint scanner of corresponding nominee. This is the innovation we made so that no person is allowed to press voting button as it is one of the drawbacks of the present voting machine. After the completion of voting, one can know the status of the nominees by clicking the count button.

IV. EXPERIMENTAL RESULTS

In this work, we have conducted the Pilot Election using a Personal Computer with four fingerprint scanners for selecting class representative. For that, we have created the database which consists of the fingerprint of the Computer Science department students with the number of 80 (45 males and 35 females). The database is created based on the digital personal scanner. 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 from the access.

During the voting, the voter first places his thumb on the touch sensitive region. If the fingerprint matches he is allowed to vote. In case the print is not stored before, a single beep is given, so the person cannot vote OR if the same person votes again, the system should give a double beep, so that the security can be alerted. The system is programmed to recognize a fingerprint twice, but to give a beep for more than once.

There are three nominees for the selection of representative and each student is asked to vote for the candidates they wish by checking their identity through fingerprint and allowing them to vote by giving thumb impression against the fingerprint scanner of candidate.

The Table 6 shows the pilot election results.

TABLE 6: PILOT ELECTION RESULT

S. No	Name of the Candidate	Count of the Votes Polled
1	M. Jeyaraj	20
2	S. Ashik	15
3	P. Kokila	10
4	P. Krishna	35
Total		80

From the results of Table 6 it is declared that Mr. Krishna has been elected as Representative of the Class of Students.

V. CONCLUSIONS AND FUTURE DIRECTION

For over a century, fingerprints have been one of the most highly used methods for human recognition; automated biometric systems have only been available in recent years. This work is successfully implemented and evaluated four different models and PC based electronic voting system under Matlab 7.5. The arrived results were significant and more comparable. It proves the fact that the fingerprint image enhancement step will certainly improve the verification performance of the fingerprint based recognition system.

The best enhancement technique Gabor is used to enhance the fingerprints for electronic voting and the report of the pilot study for students' election shown the better accuracy. By the use of this PC based voting system, the student's representative is elected in a proper way with high security. Because fingerprints have a generally broad acceptance with the general public , law enforcement and the forensic science community, they will continue to be used with many governments' legacy systems and will be utilized in new systems for evolving applications that require a reliable biometric.

In this work, we counted the spurious minutiae and did not address impact of image enhancement algorithm with spurious minutiae removal algorithms and also we are designed only a PC based electronic voting system. In future, we will design a device with Biometric Technology which can be used as if Indian Electronic Voting Machine.

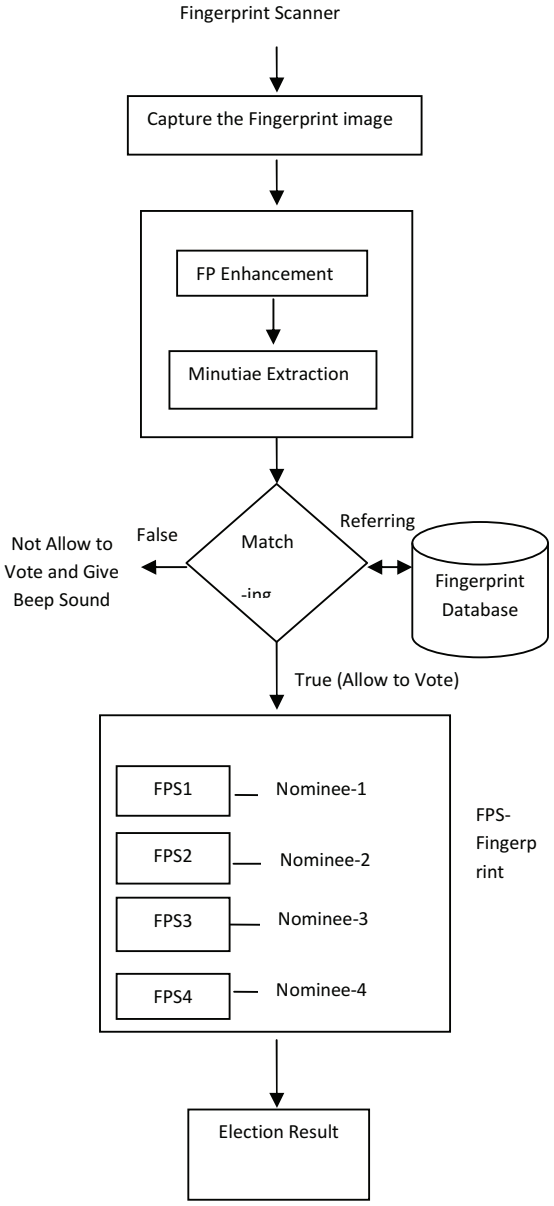

Fig.7 A Novel Design for E-Voting Process

ACKNOWLEDGMENT

This work is a part of a Research Project and authors are thankful to UGC for funding the Project (File No. F-38-258/2009 (SR) Dt: 19.12.2009).The authors would like to thank the anonymous reviewers for their thorough reviews, and constructive suggestions which significantly enhance the presentation of the paper.

REFERENCES

Abishek Rawat,, A Hierarchical Fingerprint Matching System, Indian Institute of Technology, Kanpur, July 2009

Anil K. Jain and David maltoni. , Handbook of Fingerprint Recognition, Springer-verlag New York, Inc., Secaucus, NJ, USA, 2003

Ashbaugh D. R., Quantitative-Qualitative Friction Ridge Analysis: An Introduction to basic and advanced Ridgeology. CRC Press, 1999

Bahuguna R., Fingerprint Verification using Hologram matched filterings, Biometric Consortium Eighth Meeting, San Jose, CA, 1996

California Internet Voting Task Force. A Report on the Feasibility of Internet Voting, Jan.2000. http://www.ss.ca.gov/executive/ivote/

Coetzee L. and Botha E.C., Fingerprint Recognition in low quality images, Pattern Recognition , Vol.26, No.10, pages. 1441-1460, 1993

Francis Galton. Fingerprints, Macmillan, London, 1892

Frank Vahid and Tony Givargis, Embedded System: Design A unified Hardware/Software Introduction, John Wiley & Sons, Inc, 2002.

International Biometric Group. Analysis of Level 3 features at High Resolutions. http://level3tk.sourcforge.net/, 2008

Jain A. K., Hong L. , Bolle R., Online Fingerprint Verification, IEEE Trans Patt Anal Mach Intell, Vol 19, No. 4., Pages 302-314, 1997

Jain A., Hong, L., Pankanti, S., and Bolle, R. An identity authentication system using fingerprints. In Proceedings of the IEEE ,vol. 85, pp. 1365–1388.Sep 1997

Jain A.K, Prabhakar S., Hong L. , Pankanti S., Filter bank based fingerprint matching, IEEE Trans. Image Processing, 9(5): Pages 846–859, 2000.

Jain A.K., Chen Y. and Demirkus M., Pores and Ridges: High Resolution Fingerprint Matching using Level 3 features, PMAI, 29(1):15-27, January 2007

Jie Y., Yifang Y., Renjie Z. and Qifa S., Fingerprint minutiae matching algorithm for real time system, Pattern Recognition , pp. 143–146 , 2006

Kryszczuk K., Drygajlo A. and Morier P., Extraction of Level 2 and Level 3 features for Fragmentary Fingerprints. In proc. Second COST Action 275 Workshop, pages 83-303, 1996.

Maio D. and Maltoni D. , Direct gray scale minutia detection in fingerprints. Transactions on PAMI, 19(1), 1997.

Maltoni D., Dmaio, Jain A.K., Prabhakar S. , "Hand book of Fingerprint Recognition", Springer, 2003.

Mariam BT. Samawi , Web Based Campus Election using Thumb Recognition, Mara University of Technology Faculty of Information Technology and Quantitative Science, May 2006

Marsh R.A., Petty G. S., Optical Fingerprint Correlator, US Patent 5050220, 1991

Meltemp Ballan & F. Ayhan Sakarya & Brian L.Evans, "A Fingerprint Classification Technique Using Directional Images".

Mercuri R.. Electronic Vote Tabulation Checks and balances. PhD thesis, University of Pennsylvania, Philadelphia, PA, Oct.2000

National Science Foundation. Report on the National Workshop on Internet Voting: Issues and Research Agenda, Mar.2001.

Nieuwendijk H.Y.D, Fingerprints. http://www.xs4all.nl/~dacty/minu.htm, October 2006

Rajnikannan M., Ashok Kumar D., Muthuraj, Estimating the Impact of Fingerprint Image Enhancement Algorithms for Better Minutia Detection, International Journal of Computer Application, No.1 Article 7, 2010

Raju Sonavane, Dr. B.S. Sawant., Noisy Fingerprint Image Enhancement Technique for Image Analysis: A Structure Similarity Measure Approach, SNS International Journal of Computer Science and Network Security, Vol. 7, No. 9, September 2007

Ranade A. and Rosenfeld A, Point pattern matching by relaxation. Pattern Recognition, 12(2):269–275, 1993.

Ratha, N., Chen, S., and Jain, A. Adaptive flow orientation based feature extraction in fingerprint images. Pattern Recognition 28, 11, 1657–1672., 1995

Ridges and Furrows – history and science of fingerprint identification technology and legal issues. http://ridgeand.furrows.homestead.com/fingerprint.html

Rubin A.D. Security considerations for remote electronic voting. Communications of the ACM, 45(12):39-44,Dec.2002.

Rui Joaquim, André Zúquete, Paulo Ferreira Revs- A Robust Electronic Voting Voting System *Instituto Superior Técnico*

Salil Prabhakar, "Fingerprint classification and matching using filterbank", Ph. D. Thesis, 2001.

Shaharam Mohammadi, Ali Frajzadeh A . Matching Algorithm of Minutiae for Real Time Fingerprint Identification System , World Academy of Science, Engineering and Technology 60 ,2009

Sharat Chikkerur, Alexander N. Cartwright and Venu Govindaraju., Fingerprint Enhancment using STFT analysis., Pattern Recognition., 40(1):198-211, 2007

Sharath Pankanti, Salil Prabhakar and Anil K. Jain., On the Individuality of Fingerprints, IEEE Trans. Pattern Anal. Mach. Intell, 24(8):1010-1025, 2002

Sherlock, D. B. G., Monro, D. M., and Millard, K. Fingerprint enhancement by directional Fourier filtering. In IEEE Proc. Vis. Image Signal Processing , vol 141, pp. 87–94., 1994

The Thin Blue Line. http://policensw.com/info/fingerprints/finger06.html, October 2006

Tico M., Kuosmanen P., Fingerprint Matching using an Orientation based minutia descriptor, IEEE Trans. On Patt. Analy and Mach Intell, Vol. 25, No. 8, Pages 1009-1014, 2003

Voting: What Is; What Could Be, July 2001. http://www.vote.caltech.edu/Reports/

WUZHILI, "Fingerprint recognition," Student project, Hong Kong Baptist University, April 2002.

Xia X. and O'Gorman, L. Innovations in fingerprint capture devices. Journal of Pattern Recognition, Pergamon Press, Vol. 36, No. 2, pp. 361-370, 2002

Xuejun Tan Bhanu, Yingqiang Lin B. , Fingerprint classification based on learned features, Center for Res. In Intelligent Syst., Univ. of California, Riverside, CA, USA; Aug 2005.

Zhou Wang ,Alan Conrad Bovik'sJain,A., "Image Quality Assessment :from error visibility to structure imilarity IEEE transaction On image processing" Vol.13 No4, April 2004