Secured Polling for Avoidance of Recasting and Proxy Casting

R.Charumathy, R.Kavitha, N.Rashmi
Department of Computer Science and Engineering, Sri Muthukumaran Institute of Technology, Chennai, India.

Abstract – The voters cast their vote to select right candidate, where they simply put their vote in voting box and at the end of the voting day the votes are going to be count manually. This process was much time consuming as well as was erroneous. To overcome this drawback Electronic Voting Machine (EVM) was introduced. In EVM, Voter cast their vote by pressing the voting button which was on EVM. The Major advantage of EVM system is, the votes are counted automatically instead of manually. But the drawback of EVM machine was, the votes may get manipulated and was not secure. So to overcome all these drawbacks, research on biometric based voting system is going on. This Paper focuses on survey of different voting system using Fingerprint biometric through different algorithms and methods. Also authors combined both steganographic and cryptographic techniques to demystify authentication security requirements of an online e-voting system using both secret key and voters biometric fingerprint template as the cover. The proposed model is an improvement on method by embedding Voter's Unique Identification Number and System generated and SHA256hashed secret key created during registration on Voters Fingerprint template as unique.

Index Terms – Polling, Recasting, Vote, Steganographic.

1. INTRODUCTION

BIOMETRICS, led by the fast development of imaging technologies and pattern recognition algorithms, has been utilized in complicated fields ,from physical logical access control to justice/law enforcement and from time and attendance to health care biometrics . Now, the requirements of biometric systems only focus on a high recognition rate and robustness, but have also extended to compact, online, user-friendly, and flexible for complicated cross-disciplinary application .For instance, hand-held fingerprint capturing devices and iris capturing devices are widely used for outdoor applications. Fingerprint sensors being integrated with laptops, fingerprint sensors being embedded in locks, and iris sensors being integrated with the steel safe provide better user experience and higher security than conventional solutions. However, one of the best biometric technologies, palm print recognition, which exhibits excellent recognition performance for the rich feature and is highly reliable under multi spectrum light. Line-scan technique would be an ideal solution for a palm print acquisition system. Using the line-scan technique, palmprint-capturing devices could save a great amount of space for a comfortable user interface and flexible structure without sacrificing image quality Ina line-scan sensor (also called the linear image sensor, the 1-D image sensor), pixels are placed in a linear array, which is different from area sensors.Because of this layout of the pixel array, the imaging structure can be simplified, and space can be saved. In addition, user interactions and applications were also limited by the size and the structure of the systems. For example, most palmprint acquisition systems are large,and can only be used as desktop or standalone devices.

2. RELATED WORK

There exists a number of related works in literature where the science of cryptography, steganography and combination of both are applied secure electronic voting systems for the delivery of credible electronic democratic governance. The requirement, design and implementation of a generic e-voting system were proposed . The security consideration of the model was based on RSA cryptosystem for end to end ballot security and firewalls in form of proxy server. The security consideration of the model was limited tolarge key size of RSA which requires large amount of computing time and large storage size on both mobile andelectronic voting devices. Authors in developed asecurity scheme that provides an extra layer of security against hacking called Stegacrypt. Stegacrypt is the hybridization of encryption and steganography. This is done by modifying the palettes of the carrier image and embedding one message bit of an encrypted file into each pixel in a Graphic Interchange Format (GIF) image. The problem of statistical weakness by using an insertion rate that is less than4% of the least significant bit was overcome in this work as the visual quality of the carrier image is retained as compared to other steganography tools.

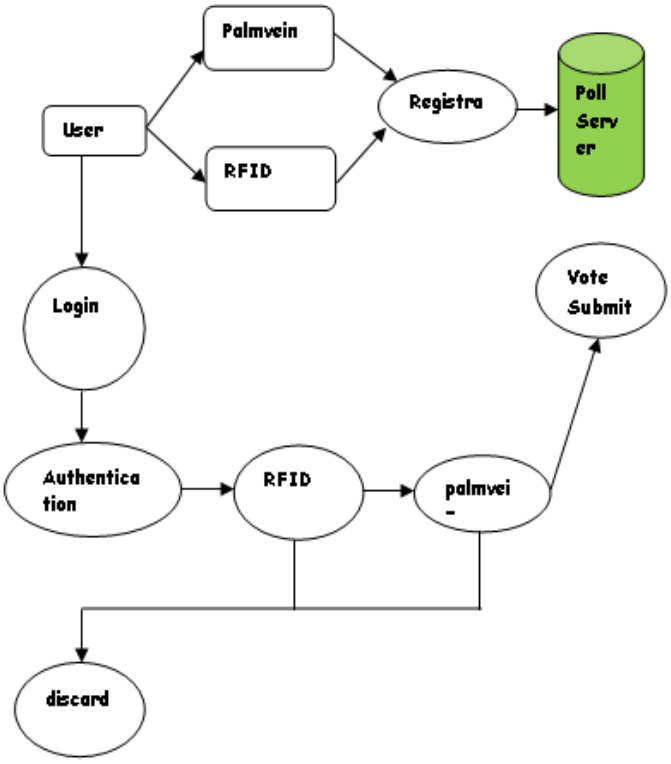
The stability of the stegacryptagainst attacks was tested by using stegalyzer, the result shows that stegacrypt is able to withstand various forms of attack on stego-image embedded by the software.Line-scan technique would be an ideal solution for a palm print acquisition system. Using the line-scan technique, palmprint-capturing devices could save a great amount of space for a comfortable user interface and flexible structure without sacrificing image quality and system performance.

3. SYSTEM ARCHITECTURE

The radio frequency identification card is used instead of manual voter's ID and results are announced as per

schedules.Both Radio Frequency Identification card & palm vein is used for User Authentication and register purpose.Then the registered vote automatically updated in website through IOT.This process is fully done by a microcontroller. Results are announced immediately.Radiofrequency identification (RFID) uses electromagnetic fields to automatically identify and track tags attached to the objects.The tags contain electronically stored information.

The image resolution on the motion direction is definedby the rollers and the gear ratio.Given a gear ratio, *Rg*, and the diameter of rollers, *DR*, when the hand moves $MR = \pi DR$, the roller rotates one round. Thenthe axis of the encoder rotates *Rg*rounds. If the encoder sendsout*Pe*pulses per round, the encoder sends out $P = (Pe/Rg)$pulses for *Rg*rounds. It means that when the hand moves*MR*mm, the encoder sends out *P* pulses. For a filter ratio*Rf*, the sensor only captures



(P/Rf)lines, then the resolution*SM*(in metric) can be computed by dividing the number of

captured lines (P/Rf) by the distance *MR*, as follows:

$SM = PRfMR$

$= PMR \cdot Rf$

.Here, the unit of the *SM* is lines per mm. One inch is

25.4mm. Thus, the resolution *SL* (in dpi) can be defined as

$SL = 25.4 \times SM = 25.4 \times PMR \cdot Rf$

$= 25.4 \times Pe$

$\pi \cdot DR \cdot Rg \cdot Rf.$

In our prototype device, the photoelectric encoder is industry standard at 500 pulses per round (*Pe*= 500). The rollers'diameter is 10 mm. The gear ratio *Rg*is2:1.. The filter ratio *Rf* is 2 : 1. Under this condition, the vertical resolution (along the rolling direction) is 101.1 dpi, which is close to the resolution along the width direction of the CIS module (100 dpi).

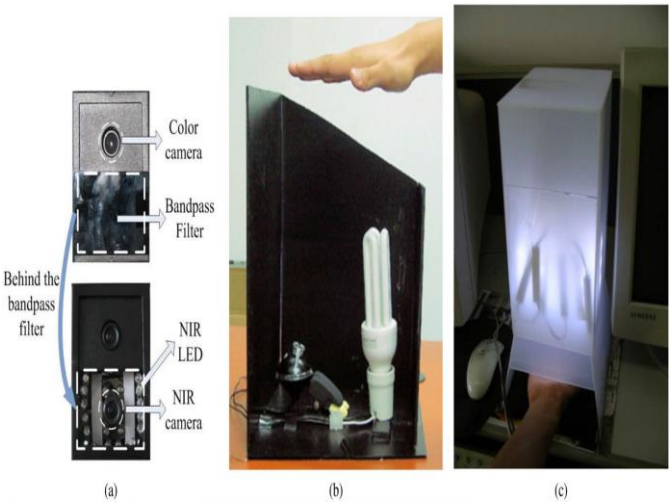
4. ADVANTAGES

With this electronic voting system the identity of the voters can be secure. Theproxy casting and recasting can be avoided Thevotes are calculated simultaneously and the results can be announced immediately. The voters can cast their vote from any booth

5. BLOCK DESCRIPTION

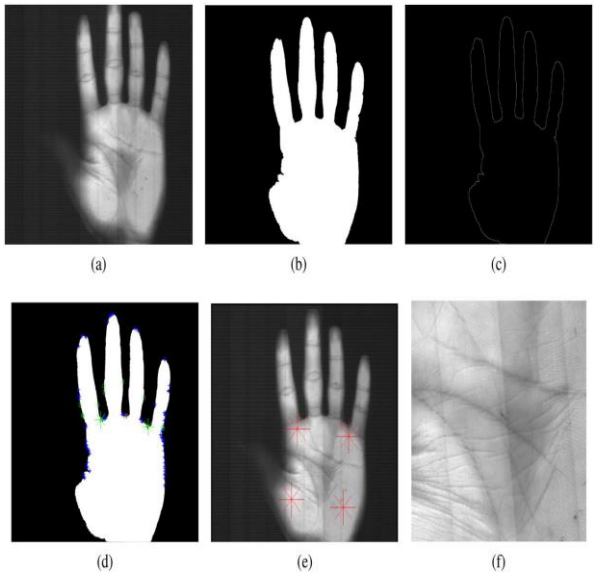
PALM VEIN

A region of interest (ROI) is a portion of an image that you want to filter or perform some other operation on. You define an ROI by creating a binary mask, which is a binary image that is the same size as the image you want to process.



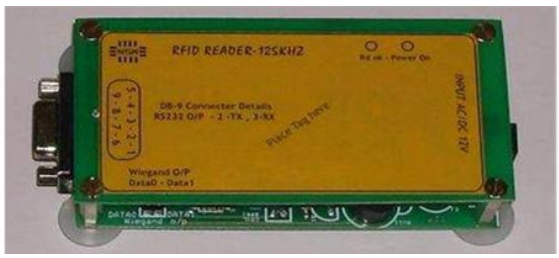
When evaluating an image acquisition system for a biometric system, the most important criterion is the recognitionperformance of the overall system. The requirements for acquisition systems are quite different, when the systems are beingused with different feature extraction, and matching methods. In this section, to compare the recognition performance of theproposed LPS and the area palmprint systems, we present a verification experiment on a large database collected by the proposed system.

In this verification experiment, the proposed palmprint acquisition system is combined with a set of ROI extraction, feature extraction, and matching methods to build a complete palmprint verification system. This set of ROI extraction, feature extraction, and matching methods is identicalto three area palmprintsystems.Inaddition,the scale of the database is comparable with the three area palmprint databases In the mask image, the pixels that define the ROI are set to 1 and all other pixels set to 0.Line-scan technique would be an ideal solution for a palm print acquisition system. Using the line-scan technique, palmprint-capturing devices could save a great amount of space for a comfortable user interface and flexible structure without sacrificing image quality and system performance.



6. RADIO FREQUENCE IDENTIFICATION

We use microcontroller to communicate the palm vein and RFID authentication so the people can independently cast the vote.There will be no duplication or proxy of vote will be casted, election commission can validate these authentication method and allow the user to cast the vote.



7. TOUCH PANEL VOTING SYSTEM

The Server will store the entire voter's information in their database and verify them if required.The Server has to establish the connection to communicate with the Users.

The Server will update the each new voter's updating in its database. The Server will authenticate each voter by RFID and palm vein before they access the Application.So that the Server will store the RFID and palm vein of every voter in the server .so that the user can access the application.

8. CONCLUSION AND FUTURE SCOPE

The system is design based on latest technology is smart voting system using fingerprint recognition. Smart voting system is useful for voter because voter can cast vote from any city to their constituency. Smart voting system may become rapid, boosted and efficient way to administration election. It also simplify counting of votes and requires minimum number of officers. Result are quickly transferred to centralized database.

FUTURE SCOPE

In future, the performance of our technique will be quantitatively assessed using Image quality metrics and compared with similar models of secure e-voting systems. Also, a multi-platform authentication parameter will be adopted to enable integration with other electronic systems like tablets and mobile-phones. Consequently the following open issues can be addressed:

a. Exploring a complex multimedia objects such as video and audio for confidentiality in the election process: Video and Audio cover media can provide better payload capacity for improved secure electronic democratic decision making using the concept of crypto-watermarking.

b. Incorporating an audio/visual device to support persons with impaired sight. Future work could incorporate design considerations for disable electorate to exercise their democratic preference.

c. Enhancing the system to solve other security issues like non-repudiation and non-coercibility. The addressed fundamental e-voting security requirements could be further complemented with post-electoral ballot verification and aversion of vote coercion as well as vote selling prior to voting.

d. Implementing the secure e- voting system based on template-free system to eliminate the threat of compromising the fingerprint template database: Future research could also investigate a template free system for improved model performance.

REFERENCES

[1] Mohammed Khasawneh, Mohammad Malkawi, Omar Al-Jarrah2, Laith Barakat2, Thaier S. Hayajneh3, and Munzer S. Ebaid4, "A Biometric-Secure e-Voting System for Election Processes", the 5th International Symposium on Mechatronics and its Applications (ISMA08),Amman, Jordan, May 27-29, 2008

[2] HanadyHussien , HussienAboelnaga , "Design of a Secured E-voting System",Electronic and Communication Department. AAST Cairo,Egypt

[3] DonovanGentles,Dr. Suresh Sankaranarayanan, "Biometric Secured Mobile Voting".

[4] SrivatsanSridharan . "Implementation of Authenticated and Secure Online Voting System", International Institute of Information Technology – Bangalore,IEEE – 31661.
[5] S.Lavanya, "Trusted Secure Electronic Voting Machine", M.E. Computer Science and Engineering, Pauls Engineering College.
[6] 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.
[7] Barbara Ondrisek, "E-Voting system security optimization", 42nd Hawaii International Conference on System Sciences – 2009.
[8] LazarosKyrillidis, Sheila Cobourne, Keith Mayes, Song DongandKonstantinosMarkantonakis, "Distributed e-Voting using the Smart Card Web Server", 7th International Conference on Risks and Security of Internet and Systems (CRiSIS),2012.
[9] Haijun Pan, Edwin Hou, Nirwan Ansari, "E-NOTE: An E-voting System That Ensures Voter Confidentiality and Voting Accuracy", Communication and Information Systems Security Symposium, IEEE ICC 2012.
[10] Foster D, Stapleton L, Huirong Fu ,"Secure Remote Electronic Voting", Proceeding, IEEE International Conference on Electro/information Technology, 710 May 2006, pp: 591- 596.