Design and analysis of an image based vote-recording system with cloud integration

[1]Vishal Balasubramanian, [2]Yupindra Kumar, [3]Yugan Raj, [4]Selvakumar VS

[1]Student, [2]Student, [3]Student, [4]Associate Professor
Department of Electronics & Communication,
Rajalakshmi Engineering College, Chennai, India

***Abstract*: Electronic voting machines (EVM) have been developed and widely used in many developed nations to improve the election process and to avoid rigging. However, in reality, they have failed to do so because it can be hacked from the inside. There have been several reports of EVM tampering from several nations. Keeping these problems in mind, we propose an image-based voting system, which is cheap, reliable, and tamper proof. This paper will discuss the present system and will provide the design and analysis of the proposed image-based voting system. For this, we use Raspberry Pi as the host, which is a credit card sized single computer or SoC and uses ARM1176JZF-S core. SoC, or System on a Chip, is a method of placing all required electronics for running a computer on a single chip. It needs an Operating system to start up. SD/MMC card will act as a bootable hard disk. A camera will be employed to detect the vote placed. Each voting machine is locked by finger print access module. As the voter fingerprint is matched with the database, he/she will be sent to a specific machine for voting. Each voting machine is linked with the central raspberry pi voting identification system. This system is highly secure and fool proof.**

***Index Terms*: Image Analysis, Image Processing, Electronic Voting, Microcontroller**

I. INTRODUCTION

With the evolution of information technology, the need for a better, faster, easier and a secure electronic voting is extremely important as the traditional election procedures cannot satisfy the demands of the rising voting population [1,2]. The main aim of any election organizing body is to increase the voter turnout and at the same time to conduct an unbiased and corruption free election process. For this, many researchers and scientists have been trying to introduce novel and fool proof approaches to secure electronic voting systems [3-7]. Technologies get in the way of accuracy by adding steps. Since no technology is perfect, each additional step results in a potential error. The after-effect of the unpleasant American presidential election held on 2 November 2004, the electronic voting machines came into existence. The votes were lost, subtracted and even doubled while using computerized machines because many machines have no paper audit trail. Therefore, a large number of votes will never be counted. In order to discuss the electronic voting machine, we need to know the difficulties faced in voting. An ideal voting system has four required characteristics. The goal of any voting machine is to establish the intent of each individual voter and to translate those intents into a tally. It is undesirable that the voting system fails to do this.

One of the main characteristic features of voting is security. The voting machine has to be designed such that it should not change a candidate's vote, stuff ballots, destroy votes, or otherwise affects the accuracy of the final tally. In order to facilitate voter's anonymity, the voting machines have to be designed with secret ballots employed in it. Secret ballots are fundamental for democracy. In the case of huge democracies, people expect the results to be declared before the end of day's election. Therefore, the voting machine has to provide the results quickly. Different technologies have done their best in these centuries. Paper ballots are dropped in sealed boxes, which in olden days are done by dropping stones and potshards in Greek vases. Mechanical voting booths, punch cards, and then optical scan machines replace hand-counted ballots. The new computerized voting machine provides more efficiency and internet voting is so convenient. Accuracy has been sacrificed in order to improve speed and scalability. There is a significant error rate in modern systems. Several voting systems have 5% error rate, which defines that one in twenty voters who vote in this system do not have their votes counted. Most of the systems that operates like this are assumed to have no error. If the errors are assumed to be uniformly distributed which means that they affect each candidate with equal probability, and then they will not affect the outcome except in very close races. Those systems are error prone. The touch screen systems, which are made of same software, makes them inaccurate in the worst possible way. 'Bugs' or errors which occur in a software are prone to many.

Computer programs malfunctions in a surprising and subtle ways. This is true for all software, including the software in computerized voting machines. It is known that software can be hacked which means one can deliberately introduce an error that modifies the result in favour of his preferred candidate. A far- reaching effect can be observed if a malicious change or an error occur in a software. A problem with a manual machine affects only the machine. However, the results of the entire election would be screwed up if there were a problem in the software which in turn affects the thousands of machines. Some have argued in favour of touch-screen voting systems, citing the millions of dollars that are handled every day by ATMs and other computerized financial systems [8-11]. That argument ignores another vital characteristic of voting system – anonymity. Another incident with the paper based electoral system is the chemical treatment of ballot papers. The papers can be treated in such a way that, the ink of the actual stamp can disappear in some time and the mark, which had been put earlier, appears prior to the counting process. This was a huge problem during the Indira Gandhi election case in 1971.

To address all these issues and to establish a reliable and a secure voting system, we in this paper propose an image based electronic voting machine. The main aim of this project is to secure and simplify the process of voting for people [12-14]. This system considers several other features such as anonymity, security and transferability [15,16].

II. MATERIALS AND METHODS

The image-based voting pad consists of a microcontroller, preferably Raspberry Pi 3 model B, a pi camera, voting pad, a 16*2 LCD display and a speaker. The model consists of the control unit and the voting pad. Raspberry Pi 3 Model B is the latest version of the Raspberry Pi computer. It is the fastest when compared to previous products. We can connect several sensors like finger print sensor, IR sensor etc. Just add a keyboard, mouse, display, power supply, micro SD card with installed Linux Distribution and you will have a fully-fledged computer that can run applications from word processors and spreadsheets to games. As the Raspberry Pi 3 supports HD video, you can even create a media center with it. The Raspberry Pi 3 Model B is the first Raspberry Pi to be open-source from the get-go, expect it to be the de facto embedded Linux board in all the forums. In this project, we are going to connect pi camera to the Raspberry Pi 3.

The camera used here is connected to the raspberry pi 3. It captures the live video and sends the data to processor. In the processor, the video will be processed and will be sent to the display unit. The Raspberry Pi Camera v2 is the new official camera board released by the Raspberry Pi Foundation. The Raspberry Pi Camera Module v2 is a high quality 8-megapixel Sony IMX219 image sensor custom designed add-on board for Raspberry Pi, featuring a fixed focus lens. The Raspberry Pi Zero now comes complete with a camera port. Using the new Raspberry pi camera adapter, we have used a Raspberry Pi camera to our Raspberry Pi 3. It is capable of 3280*2464-pixel static images, and supports 1080p30, 720p60 and 480p90 video. It attaches to Pi by way of one of the small sockets on the board upper surface and uses the dedicated CSI interface, designed especially for interfacing to cameras. The weight of the camera is just over 3 grams. It is connected to the Raspberry Pi board via a short ribbon cable, Camera v2 is supported in the latest version of Raspbian.

An overview of this project is that, a voter comes to the voting desk and places his palm on the desk in which the respective party name is printed. The image-processing camera will focus on the hand. If the palm is placed correctly, the vote will be counted. If not an error message along with an alert sound will be given. The layout of a standard voting machine is given in Figure 1.

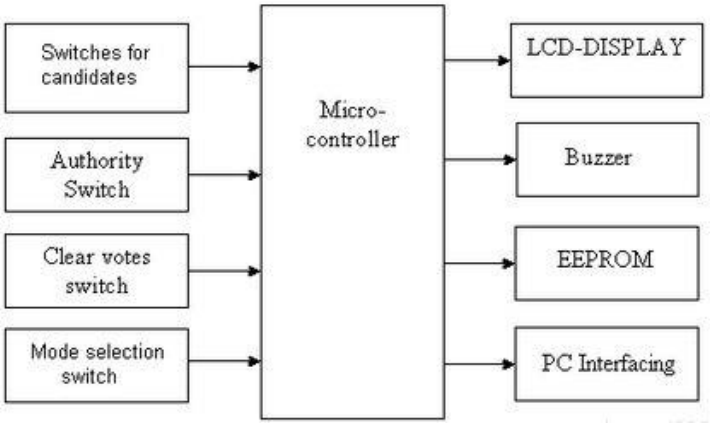

Figure 1. Block diagram of a standard voting machine

The voting machine consists of two parts – voting pad and control unit. The diagrammatic representation of voting pad is given in Figure 2. It consists of several palm-sized boxes arranged horizontally. To the voting pad is connected a colour camera that focuses on the pad only and not on the person. In this way, we have solved the issue of anonymity. Above the placing pads lie the information about the candidate and the party.

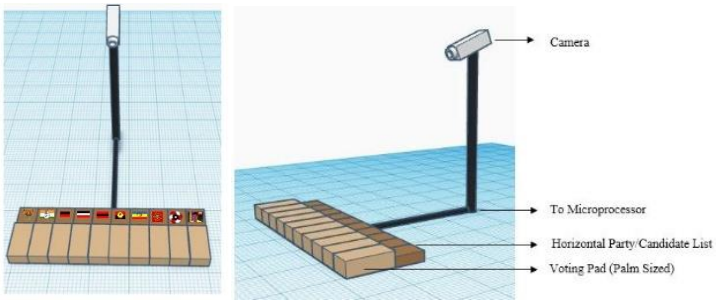

Figure 2. Representation of Voting Pad

The control unit consists of a reset button. Once a voter has placed his vote, the camera stops the filming cycle and the message is sent to the control unit. The controller will then release the camera so that the next voter can place his vote. A simple yet powerful program is written in assembly language and is burnt onto the microcontroller to accept votes and to keep counting the total votes polled. Every voter gets approval from the polling officer. If the polling officer issues approval with his control switch, then only

the voter can poll his vote. This issuance of approval is indicated by a long buzzer beep. Vote count is stored in EEPROM and an LCD display is provided to display the total number of votes polled and individual contestant-wise votes polled.

The flow diagram of the entire process is given below in Figure 3 and the connection are given in Figure 4.

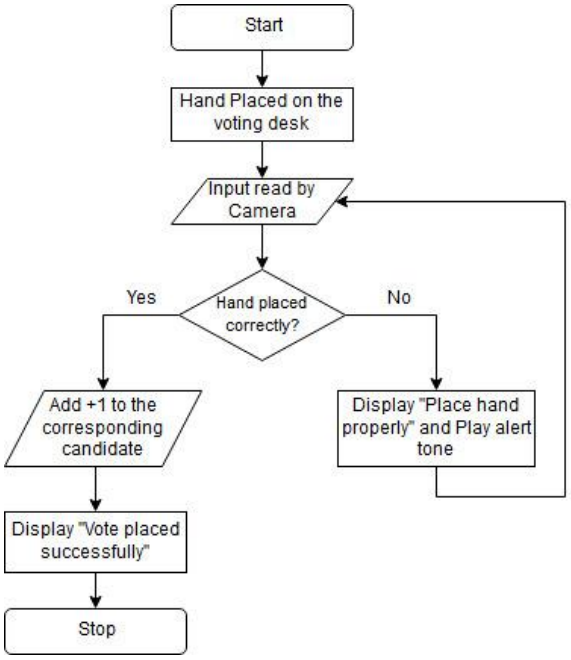

Figure 3. Flowchart of image-based voting pad system

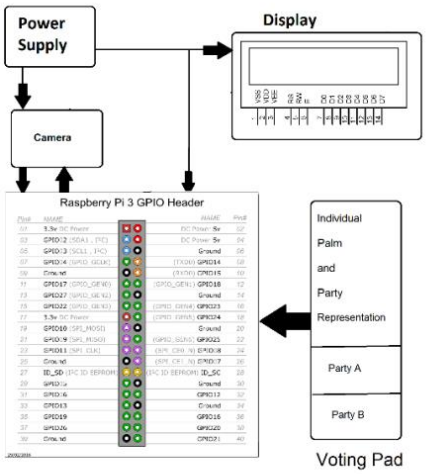

Figure 4. Layout of Proposed Voting System

The software part of the proposed system is a little complicated. It consists of two parts. The local memory and the central server memory. As and when a vote is placed, the count is transmitted to the cloud-based central server located at the headquarters. This increases the reliability of the system. During the counting day, the votes obtained in the central server is cross verified with those stored in the local memory of the voting unit. It can be clearly understood by the below diagram of how a cloud-based server works. Here, the voting unit is considered as the User Interaction Interface.

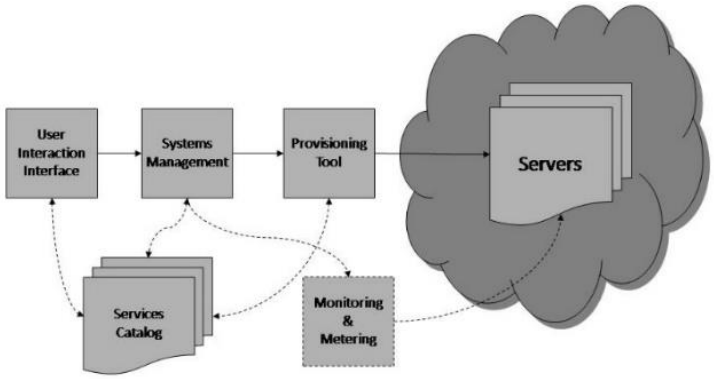

Figure 5. Cloud-based Server Systems

III. RESULTS

The main aim of the work, that was to provide speed, accuracy and reliability have been obtained successfully using our proposed solution. The image analysis can be seen below in Figure 6.

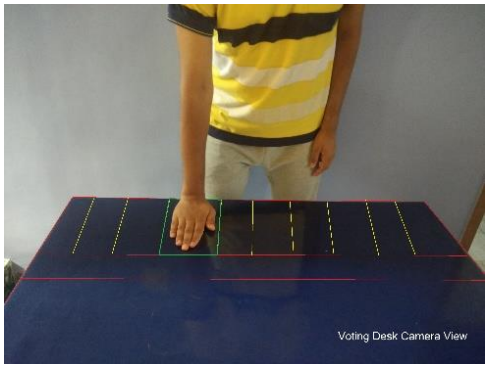

Figure 6. Voting Desk Camera View

As you can see from the above figure, the location of the arm is detected using image analysis. The corresponding Cartesian coordinates are obtained to know the location of the palm. From the obtained data, the candidate is recognized and the vote count of the candidate is increased. As the camera does not focus on the person, the identity of the person remains anonymous. In addition, this type of voting is secure and reliable as it uses the property of image interpretation and coordinate geometry.

IV. CONCLUSION

It would be easy to program a dishonest EVM or EVM component so that the manipulation is only performed after voting has been going on for a long time, or if the total number of votes is in the hundreds. That way, simple mock polls will show the proper results, but all the final election results will be manipulated. Until now, the EVMs have not been subjected to rigorous, independent, public scrutiny. Claims that the EVMs are "perfect" and "infallible" are not based on verifiable arguments. If the Election Commission disagrees with our claims, we look forward to a proper scientific debate based on credible, published evidence. The votes registered are offline and everything is stored locally as well as transmitted to the central server where it is stored in the cloud. Hence, there is very little or no chance for the system to be tampered. Therefore, the image-based voting system turns out to be cheap, reliable and tamper proof.

V. ACKNOWLEDGMENT

We would like to thank Dr.M.Palanivelan, Professor, Department of Electronics and Communication Engineering, Rajalakshmi Engineering College, Chennai, for his valuable inputs and constant encouragement.

REFERENCES

[1] T. Kohno, A. Stubblefield, A. D. Rubin and D. S. Wallach, "Analysis of an electronic voting system", IEEE Symposium on Security and Privacy, 2004. Proceedings. 2004, Berkeley, CA, USA, 2004, pp. 27-40. doi: 10.1109/SECPRI.2004.1301313

[2] D. A. Kumar and T. U. S. Begum, "Electronic voting machine — A review", International Conference on Pattern Recognition, Informatics and Medical Engineering (PRIME-2012), Salem, Tamilnadu, 2012, pp. 41-48. doi: 10.1109/ICPRIME.2012.6208285

[3] D. Balzarotti et al., "An Experience in Testing the Security of Real-World Electronic Voting Systems", in IEEE Transactions on Software Engineering, vol. 36, no. 4, pp. 453-473, July-Aug. 2010. doi: 10.1109/TSE.2009.53
[4] Anandaraj S, Anish R and Devakumar P.V, "Secured electronic voting machine using biometric", 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, 2015, pp. 1-5. doi: 10.1109/ICIIECS.2015.7192976
[5] D. Karima, T. Victor and R. Faycal, "An improved electronic voting machine using a microcontroller and a smart card", 2014 9th International Design and Test Symposium (IDT), Algiers, 2014, pp. 219-224. doi: 10.1109/IDT.2014.7038617
[6] M. R. Clarkson, S. Chong and A. C. Myers, "Civitas: Toward a Secure Voting System", 2008 IEEE Symposium on Security and Privacy (sp 2008), Oakland, CA, 2008, pp. 354-368. doi: 10.1109/SP.2008.32
[7] S. Lavanya, "Trusted secure electronic voting machine", International Conference on Nanoscience, Engineering and Technology (ICONSET 2011), Chennai, 2011, pp. 505-507. doi: 10.1109/ICONSET.2011.6168014
[8] R. Kusters, T. Truderung and A. Vogt, "Clash Attacks on the Verifiability of E-Voting Systems", 2012 IEEE Symposium on Security and Privacy, San Francisco, CA, 2012, pp. 395-409. doi: 10.1109/SP.2012.32
[9] K. Ranganathan, "Trustworthy pervasive computing: the hard security problems", IEEE Annual Conference on Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second, Orlando, FL, USA, 2004, pp. 117-121. doi: 10.1109/PERCOMW.2004.1276916
[10] A. F. N. Al-Shammari, A. Villafiorita and K. Weldemariam, "Understanding the Development Trends of Electronic Voting Systems", 2012 Seventh International Conference on Availability, Reliability and Security, Prague, 2012, pp. 186-195. doi: 10.1109/ARES.2012.76
[11] Young Ho Kwon and N. da Vitoria Lobo, "Face detection using templates", Proceedings of 12th International Conference on Pattern Recognition, Jerusalem, Israel, 1994, pp. 764-767 vol.1. doi: 10.1109/ICPR.1994.576435
[12] H. Koshimizu, M. Tominaga, T. Fujiwara and K. Murakami, "On KANSEI facial image processing for computerized facial caricaturing system PICASSO", IEEE SMC'99 Conference Proceedings. 1999 IEEE International Conference on Systems, Man, and Cybernetics (Cat. No.99CH37028), Tokyo, Japan, 1999, pp. 294-299 vol.6. doi: 10.1109/ICSMC.1999.816567
[13] V. S. N. Prasad and B. Yegnanarayana, "Finding axes of symmetry from potential fields", in IEEE Transactions on Image Processing, vol. 13, no. 12, pp. 1559-1566, Dec. 2004. doi: 10.1109/TIP.2004.837564
[14] L. O. Jimenez, A. Morales-Morell and A. Creus, "Classification of hyperdimensional data based on feature and decision fusion approaches using projection pursuit, majority voting, and neural networks", in IEEE Transactions on Geoscience and Remote Sensing, vol. 37, no. 3, pp. 1360-1366, May 1999. doi: 10.1109/36.763300
[15] Jiaya Jia and Chi-Keung Tang, "Image repairing: robust image synthesis by adaptive ND tensor voting", 2003 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2003. Proceedings, Madison, WI, USA, 2003, pp. I-I. doi: 10.1109/CVPR.2003.1211414
[16] D. Chaum, "Secret-ballot receipts: True voter-verifiable elections", in IEEE Security & Privacy, vol. 2, no. 1, pp. 38-47, Jan.-Feb. 2004. doi: 10.1109/MSECP.2004.1264852