INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 2)
Available online at: www.ijariit.com

Multi-factor authentication for secure electronic balloting credentials

Anita Titus
anitatitus72@gmail.com
Agni College of Technology, Chennai, Tamil Nadu

Nithiya Princy Rajam. B
nithiya1096@gmail.com
Agni College of Technology, Chennai, Tamil Nadu

Swetha. M
chinniswethamacha18@gmail.com
Agni College of Technology, Chennai, Tamil Nadu

Ramya. S
ramyasaravanan16797@gmail.com
Agni College of Technology, Chennai, Tamil Nadu

ABSTRACT

In recent times there has been a decline in the confidence of common people over the Electronic Voting Machines (EVMs). Today's automated vote casting methods have faced immense controversy to being vulnerable to hacking and questions have been raised about their transparency and security. This paper is lodged in style and develop a tamper-resistant electronic legal system that aims to alleviate the problems with existing machines. Here, multiple bedded verification method is administrated on an associate eligible citizen by means of fingerprint recognition primarily to demonstrate his identity. Subsequently, the person would cast the vote by pressing a button corresponding to a particular candidate which would be recorded in the system providing the vote caster a visual confirmation. Then steganography technique is used to hide secret messages into ordinary digital media without drawing suspicion. This system not only prevents multiple vote casts but also eliminates the discrepancies that commonly arise with a person claiming not to have voted, whereas his or her name is present in the list of vote casters. The experimental results show that the proposed method outperforms previous EVMs by electronically transmitting their results back to the Election Commission from the control unit, through a simple and unconditionally secure protocol.

Keywords: *EVM, Fingerprint recognition, Secured protocol.*

1. INTRODUCTION

In India, Electronic Voting Machines are being used in General and State Elections. The EVMs reduce the time both in casting a vote and declaring the results compared to the old paper ballot system. The voting machines in India use a two-piece system with a balloting unit presenting the voter with a button for each choice connected by a cable to an electronic ballot box. The two units in current EVMs are (1) Control Unit (2) Balloting Unit. These units are joined together by a five-meter cable. The Control Unit is with the Presiding Officer or a Polling Officer and the Balloting Unit is placed inside the voting compartment. The officer-in-charge of the Control Unit will press the Ballot Button which will enable the voter to cast his vote by pressing the button on the Balloting Unit against the candidate and symbol of his choice. 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.

a. Benefits

It will be easier to move the EVMs compared to ballot boxes as EVMs are lighter, portable and come with polypropylene carrying cases. The vote-counting is extremely quick and therefore the result can be declared within 2 to 3 hours. In India, where illiteracy is still a factor, illiterate folks realize EVMs easier to use than ballot paper system.

Bogus voting can be greatly reduced by the use of EVMs. Further, the maximum number of votes that can be cast in a single EVM is 3840. The votes recorded until the stage when the EVM went out of order remains safe in the memory of the Control Unit and it is not necessary to start the poll from the beginning. The Control Unit can store the result in its memory for more than 10 years. The battery is required only to activate the EVMs at the time of polling and counting. As soon as the polling is over, the battery can be

switched off and this will be required to be switched on only at the time of counting. Even when the battery has removed the memory in the microchip remains intact. Invalid votes can be avoided by use of EVMs. Since EVMs work on a 6-volt battery, there is fully no risk of any elector obtaining an electric shock.

b. Limitations

First, fake votes can be cast with the help of related officials themselves. These are termed fake votes once one person casts multiple votes for a specific candidate which is considered unauthenticated. Secondly, the Fake machines, where the machines are programmed in such a way that when a legitimate elector casts his/her vote to their specific candidate, the vote is being cast for another specific person alone. This happens whether or not that voter prefers to vote for that candidate.

2. LITERATURE SURVEY

R. Murali Prasad et al [2016], has proposed a technique in which the details of the voter can be verified from the AADHAR card database, which is newly developed information database that has all the information concerning the people. By using this database, the voter's information will be stored on the personal computer. At the time of elections, the finger prints of the voter can be accessed by using finger sensing module. Here in Aadhar based EVM, the information is used from the primarily based server containing Aadhar details, Raspberry-pi for online technology and Arduino is employed for interfacing Raspberry-pi. The elector is allowed into election booth with Aadhar card ID. Here the voter first gives his Aadhar card for QR reading/Keypad operator. The elector is allowed into the ballot box room when the QR reading/UID authentication is finished with success by the operator. The elector has to scan the person's thumb biometric and also check if the thumb data that are scanned is matched with the pre-loaded server information, then the elector is permitted to vote. Otherwise, the Authentication will fail and the voter will not be able to cast the vote. The overall data of casted votes are distributed to the server net technology in order to provide security and easy counting of casted votes so that the results are often declared among all the constituencies quickly.

Haijun Pan et al [2015], proposed an E-voting procedure which utilizes the multi-part ballot mode providing voters an enhanced way to cast and audit their own votes with great anonymity. In the proposed scheme, the **M**ulti-part ballot based **N**ame and v**O**te separa**T**ed **E**-voting system (M-NOTE), has a watchdog device. This is used to record and monitor the entire online voting transactions. Only the voting authorities have access to the data stored in the watchdog device. The ballot distribution transactions will be recorded in the watchdog device to avoid any multiple or duplicated ballots. Thus, this achieved the goal of keeping candidates confidential and voters anonymous, as well as reducing the risk of leaking both candidates' and voters' identities during the ballot distribution phase. In addition, M-NOTE can prevent the possible clash attack in which either malicious authority or hackers could partially manipulate voting results by tampering voters' original ballots. Meanwhile, the performance analysis shows that M-NOTE provides a better security level, as the possibility of ballot reconstruction and voting result manipulation has been reduced closer to zero.

Talib Divan et al [2016], proposed papers based on fingerprint matching, considering the issues which occur at the time of handling. The major technique which they implemented is minutiae based algorithm. This Minutiae based algorithm includes two-stage fingerprint matching technique, one is the minutiae positioning which is done from one fingerprint image & orientation from other is used to create combined fingerprint image. The minutiae-based matching process is used for designing a voting system in which a fingerprint image is given for diagnostic process which undergoes binarization of the new combined image. In binarization, the images are allowed to operate on bi-level i.e white & black. Black pixel represents ridge & white pixel represent valley in the fingerprint. The fingerprint image is then extracted for the minutiae position to generate the template which can be used for authentication & enrolment process. The fingerprint images after extraction are stored in the template database which can be used during the authentication for matching & enrolment for storing. The stored fingerprint template is secured as it is made through two-stage fingerprint process and less prone to server-side attacks. Also, their proposed system aims to implements a voting system with low FRR rate.

Mona F. M. Mursi et al [2015], proposed a new cryptographic electronic voting scheme based on public key cryptosystem. The new scheme is named SAC after its key properties, Security And Audit Ability With Strong Cryptographic Mechanisms hence the name *SAC*. This scheme is proposed to replace the conventional voting methods that are widely used in most developing countries such as Egypt. This proposed e-voting scheme is based on the concept of Prêt à Voter, a paper ballot e-voting scheme that includes the use paper ballots, due to its familiarity among the public, but with strong encryption protocols that provide an enhanced level of ballot secrecy, verifiability and voter privacy. It includes three stages: Stage 1 is the pre-election stage, Stage -2 is the vote-capture "cast vote" stage and Stage 3 is the post-election stage which includes tallying of votes and announcing results. These are auditable with the use of risk-limiting audits and parallel test of voting machines. This proposed scheme concludes the replacement of paper-based voting by cryptographic electronic voting to conduct large-scale elections is feasible.

X. Yi et al [2016], propose a real-world electronic voting system for mobile phone. The idea is to merge mix network and blind signature protocols and blindly authorizing each vote twice. Voter verification is achieved by a collaboration of SIM card and identity card (IC) fixed in a mobile phone with dual SIM card holder. The proposed framework consists of the mobile voter, a base station (BS), a certificate authority (CA), electoral commission (EC), mix server (MS) and court for election (CE). Mobile phone voting system runs in three phases: setup and registering phase, voting phase, and totalling phase. At least one of mix servers should be reliable and tampering proof. Certificate authority, electoral commission, and mix server have own public/private keys. When mobile phone voters registers with a certificate authority, CA will compute two PINs and issue an identity card and passes PIN1 to voter via the safe channel. Voter has no access to PIN2 protected in the secure memory of IC. After voter registration with election commission, it will calculates PIN3 and passes to voter via the protected channel. During polling period voters reminded by SMS to cast their votes to the election commission. First voter inserts SIM card and IC into his mobile phone with dual SIM card holder. Secondly, voter chooses their selected candidate. CA and EC jointly validate voter on the basis of MAC (Message Authentication Code). During polling election commission, certificate authority and base station preserve all exchanged messages. When voting

ended, election commission shows all votes in lexicographic order. Mix server collects all votes and confirms their signs. If signs are real then decrypt votes by their private key. Mix server will organize all votes in lexicographic order and forwards them to EC with its signs. Election commission validates these signs. During totaling EC and every mix server preserve all substituted messages and non-repudiation evidence of message source and message transfer for record purposes.

R. Lakhotia et al [2017], proposes mobile phone voting uses global system for mobile communication technology where GSM verification system used to provide voter confirmation, enhanced security, voter mobility and reduce public-key overhead. For registration purposes, user will register their mobile number to election commission (EC) of India and will get voter ID for identification purposes. The voter has to activate their mobile number for voting and only one vote will be cast on each mobile number. The protocol has three stages: Pre voting stage, voting stage and post voting stage. In pre-voting stage when the user wishes to vote, presses "Vote" button assumes to exist on the set. Base station instructs user through SMS to switch off their mobile phone. Switching on again by pressing "vote" button, the mobile phone will be reserved only for voting purposes and no outgoing and incoming call can be received on that mobile phone. When authentic voters cast their vote, they will get SMS from EC of India having a list of candidates, their parties name, and symbols. The user has to simply reply to this SMS. The message holds ten number destination field filled partly (eight digits) by the base station with servers number and last two by the user for identification of different areas. The area code is provided by the government before the voting day. The eight number destination codes are kept the secret to make the application secured. If in case of hacking the intruder will not be able to get the destination number. The cryptographic application will be installed earlier in the mobile phone. The message will request for voter id and mobile number. If voter ID matches with EC voter list, the election commission will approve to the voter to cast their vote. Counting server receives an encrypted message with the encryption key from authentication center else vote will be rejected. User will acquire acknowledgment message on the same registered number after vote acceptance. Advantages of the system are if SMS gets hacked intruder can't cast a fake vote as key already passed. If user's mobile phone is stolen then the user can contact with EC help centre to block the number and can also register new mobile number. No need of internet as voting is done over SMS while one vote per mobile phone is the shortcoming of the system. Making authentication centre more secure and reliable is the future work of the system.

3. PROPOSED METHODOLOGY

The solution to these problems is given by the following way. Initially, after checking for validity of cards by the authorized personnel, the voter is again validated by his/her RFID card to proceed with the voting task. Normally the fingerprint can be stored in databases and cross-validated using an internet-based Client Server Topology, but if the connection with the server gets disconnected it might create problems in a Voting Environment. Hence a system wherein the Voters Fingerprint is stored in the RFID card and the validation is carried on. By doing so the time consumed for checking the Identity is also reduced.

Once the voter casts his vote, the vote count increases in the database and the entire scene is captured using the camera and the image is secured by means of Steganography. The captured image is stored using Steganography process which will be verified at the time of recounting if necessary. The Steganography concepts state that the images are hidden in a constant image. If the image is retrieved from the constant image then the actual image can be gained. During the counting of votes, the secured images are restored and the following image processing techniques are applied. The RGB format of the picture is converted to Grey scale and the vote that is cast by the Voter is calculated from the image and two databases are incremented: one by the press of the voter and the other by the image processing software. This can prevent the counting of fake votes. These images are matched with the RFID number of the corresponding voter and checked. This process in shown in fig.1.

4. BLOCK DIAGRAM OF THE PROPOSED SYSTEM

The fig 2 shows the proposed block diagram which is cheaper and more efficient compared conventional method.

5. HARDWARE USED

a. Microcontroller:

A 40 pin At89t51 microcontroller which is a low power but high-performance 8-bit CMOS microcontroller is being used. It possesses 4Kbytes of flash programmable and erasable ROM and 128 Bytes RAM which can be programmed and erased to the maximum of 1000 times as shown in fig.3.

Fig.3: At89t51

b. Fingerprint sensor:

A transducer used to convert the biometrics of the human finger into the electric signals which determine the person's details from the main server. Fig 4. Shows the fingerprint module used.

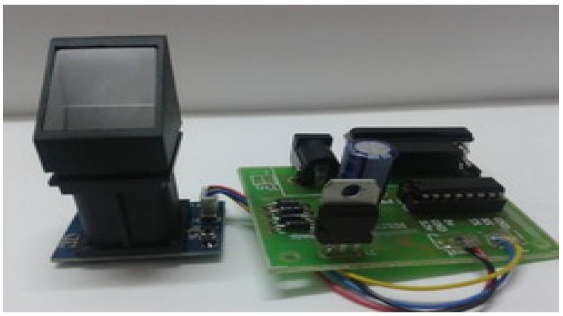

Fig.4: Fingerprint Module

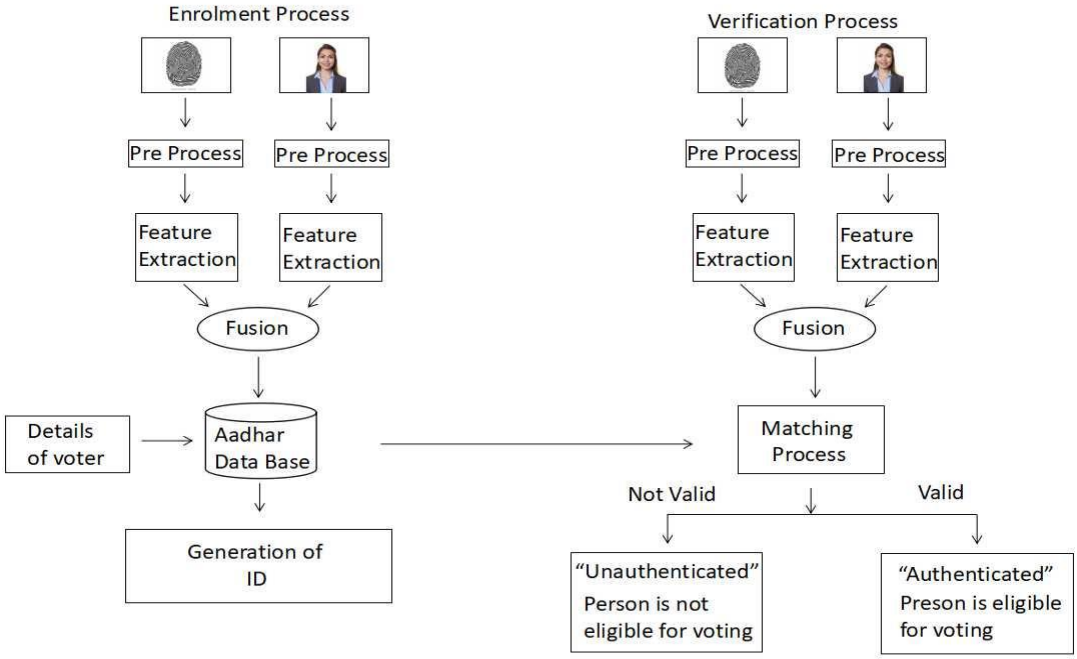

Fig.1: Proposed Method

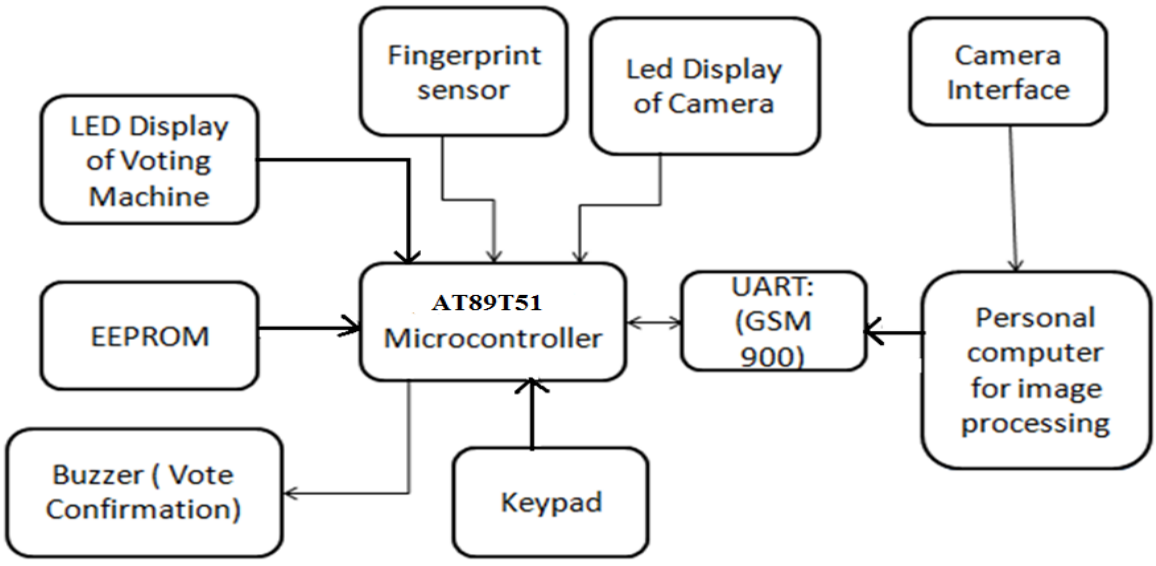

Fig.2: Block Diagram of the Proposed System

c. UART:

UART (Universal Asynchronous Receiver Transmitter) as shown in fig.5, is an asynchronous serial communicator generally used over a computer or peripheral serial port where the data format and transmission speeds are configurable.

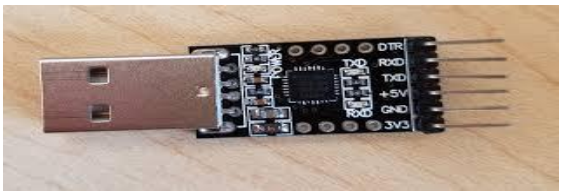

Fig.5: UART

d. EEPROM:

EEPROM (Electrically Erasable Programmable Read Only Memory) as shown in fig.6, is a non-volatile memory which electrically stores data and primarily allows individual bytes to be erased and reprogrammed.

Fig.6: EEPROM

6. SOFTWARE IMPLEMENTATION

I. ENROLLMENT PHASE:

a. Pro-processing

Initially in this, the fingerprints of voter are collected using the finger print module along with the photo of the voter's face.

b. Features Extraction

In this, the features of the image are converted to the digital form and stored in the date base. This feature extraction is done from both finger print data that is taken from the voter and his details during the registration process

c. Fusion

In this process, the features that are extracted from the fingerprint and the respective details collected from the voters are concatenated together and stored.

d. Voters details

Here the voter's general details are included. This includes age, permanent address, voter's name and other details**.** These are stored in the separate database.

e. Adhaar database

This consists of the voter's data which is stored from the process of fusion and from the data base of the voter's detail. It includes the details of the voter which usually includes the photo of the voter and their finger print.

f. Generation of voter ID

After collecting all the data and stored in the data base an identity card will be generated as shown in fig 7, which will be given to all the candidates who are eligible for voting. This card will be generated which will be sent to the voter's respective address mentioned during the general details.

Fig 7: Sample ID

II. VERIFICATION PROCESS:

a. Pre-processing

At the polling booth, the finger print module is kept which is used for processing the finger print of the person and a camera to capture the image of the face of the voter

.

b. Feature extraction

Here the data of the finger print and image captured are usually in the RGB format. These are converted to the respective gray image and digital data which are used for analysis.

c. Fusion

In this the fingerprint and the voter's image are combined together and used for further processing.

d. Matching

The fused data are matched with the data already taken during enrolment phase. These data are present in the adhaar data base. Usually this gives two different results.

1. Not valid: This means the fingerprint of the voter does not match with the data already present or that particular voter might not have enrolled himself.

2. Valid: This means that the fingerprint of the voter matches with the database collected and that voter is authenticated which means he/she is allowed to vote.

III. PROCESS OF STEGNOGRAPHY:

a. Conversion of image to matrix

In the conversion process of image to matrix the input cover image is converted into matrix values which is stored in a image file. First the camera captured image is read from the computer. The original image is in the form of RGB which is converted into gray image. This grey image is resized to a particular size of 256*256. Each image has its intensity values for every pixel. Figure 8 shows the cover image used and figure 9 shows the intensity values of cover image obtained during the conversion of image to matrix.

Fig.8: Cover Image

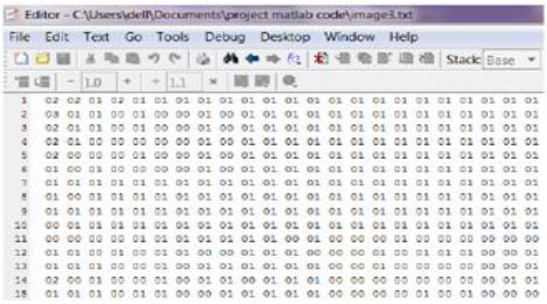

Fig.9: Intensity Value of the Cover Image

b. Embedding process:

After completion of image to matrix the next step is to embed the captured image into another image. The image obtained during this process is called as stegano-embed image. The message is embedded into the intensity values of image obtained during image to matrix conversion. The intensity values of the em-bedded image are same as the stegano image shown in figure 10,which is also know as secret image.

Fig.10: Secret Image

c. Conversion of the matrix to the image

In this stage intensity values are converted back to the image. The image obtained has the message embedded into it. The cover image and the image obtained here have to be identical. Thus the objective of steganography is satisfied as shown in fig 11.

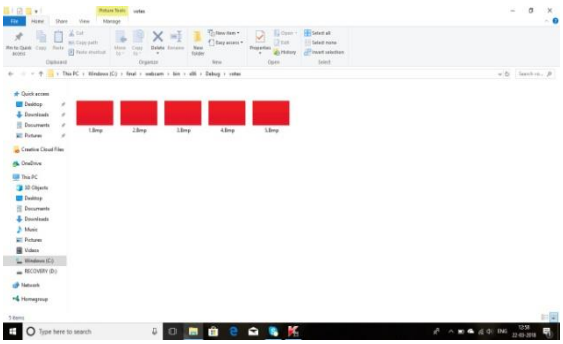

Fig.11: Stegno-image

d. Extraction process

In this process the message which was embedded during embedding process is extracted. At first a message byte is declared, where the size of the message is 8 bits. It reads a pixel from the array starting from address=0, then extracts the LSB and replace the i th bit in the message byte where i =1 to 8 Ad-dress=address=1. When i =8, a byte is extracted and repeats this for extracting next byte as shown in fig 12.

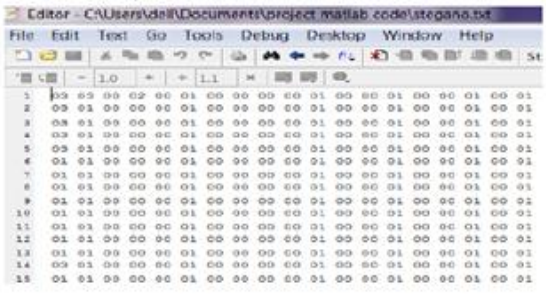

Fig.12: Intensity Value of Stegno-Image

7. RESULTS

Here in this paper, the votes are tallied using the number of votes that are counted from the image captured by the camera using the steganography image processing, with the votes that, voter put at the time of voting using EVMS as shown in fig 13. Thus using this it can be checked whether the votes using both processes are equal or not. Also using this we can determine which person is getting the duplicate votes.

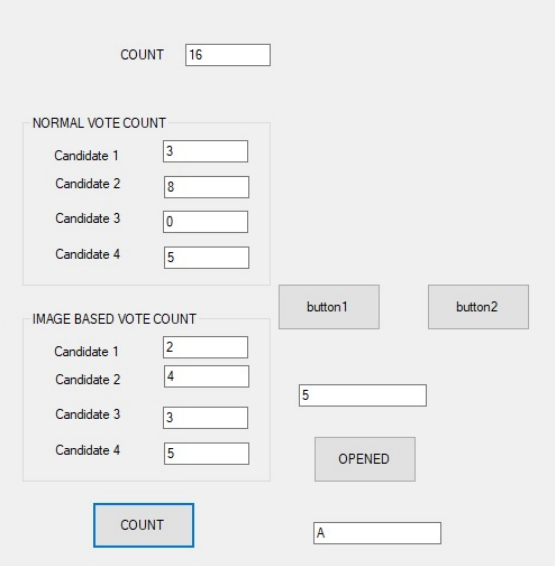

Fig 13: Voting Count

8. CONCLUSION

This project is designed to reduce the fake votes that are cast during the time of elections. This effectively increases the security and cross-checks the votes by counting the number of votes from the images captured during the election using image processing technique with the normal votes counted. This overcomes all the drawbacks that are faced in the current EVM.

9. REFERENCES

[1] J. Fridrich and J. Kodovsky, "Multivariate Gaussian model for designing additive distortion for steganography," Proc. of IEEE ICASSP, Vancouver, BC, May 26-31, 2013. [10] V. Sedighi, R. Cogranne, J. Fridrich, "Content-adaptive steganography by minimizing statistical detectability," IEEE Trans. on Inf. Forensics Security, vol. 11, no. 2, pp. 221-234, 2016.
[2] T. Filler, J. Judas, and J.Fridrich, "Minimizing additive distortion in steganography using syndrome trellis codes," IEEE Trans. on Inf. Forensics Security, vol. 6, no. 1, pp. 920-935, 2011.
[3] B. Li, M. Wang, X. L. Li, and S. Tan, "A strategy of clustering modification directions in spatial image steganography," IEEE Trans. on Inf. Forensics Security, vol. 10, no. 9, pp. 1905-1917, 2015.
[4] T. Denmark and J. Fridrich, "Improving steganographic security by synchronizing the selection shannel," Proc. of 3rd Workshop on IH&MMSec, Portland, Oregon, June 17-19, 2015.
[5] A. D. Ker, P. Bas, R. Bohme, et. al, "Moving steganography and steganalysis from the laboratory into the real world," in Proc. ftrst Int. Workshop Information Hiding and Multimedia Security, Jun. 1719, 2013, pp. 45-58.
[6] T. Filler and J. Fridrich, "Gibbs construction in steganography," IEEE Trans. on Inf. Forensics Security, vol. 5, no. 4, pp. 705-720, 2010.
[7] X. Zhang, W. Zhang and S. Wang, "Efficient double-layered steganographic embedding," IET Electronics Letters, vol. 43, no. 8, pp. 482-483, 2007.
[8] W. Zhang, X. Zhang and S. Wang, "A double layered "plus-minus one" data embedding scheme," IEEE Signal Processing Letters, vol.14, no.11, pp. 848-851. Nov. 2007.
[9] J. Fridrich and J. Kodovsky, "Rich models for steganalysis of digital images," IEEE Trans. on Inf. Forensics Security, vol. 7, pp. 868-882, 2012.
[10] J. Kodovsky, J. Fridrich, and V. Holub, "Ensemble classifiers for steganalysis of digital media," IEEE Trans. on Inf. Forensics Security, vol. 7, no. 2, pp. 432-444, 2012.

