International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 3

Manifest Electronic Voting Machine Using Image Processing

Jones Arthi S, Kousalya R, Kumari M
Department of Computer Science and Engineering,
Sri Muthukumaran Institute of Technology, Chennai, Tamil Nadu, India

ABSTRACT

Electing an Eligible leader is a highest and prestigious responsibilities of every citizen of the country. Conducting the election and announcing the election results is a time and resource consuming task. Introduction of Electronic Voting Machines (EVM) greatly reduced the burden of operation but raises many concerns about the authentication of the results. Failure political parties often blame the functioning of the EVM is compromised with hacking techniques and intentional malpractice. This project work endeavors to solve the continuous accusations over EVM through following multi verification methods. Wireless voting copy machine and surveillance camera based voting counting. When a voter cast his/her vote a local copy of the data will be stored inside the EVM. Along with this verification a surveillance camera will recognize the casting vote with motion estimation. After the election, during data counting all the above two types of results will be compared to get a unique and authenticated result, which cannot be accused for malpractice.

Keywords: *EVM; Verification; Voting; Malpractice; Authentication; Motion Estimation; Surveillance camera*

I. INTRODUCTION

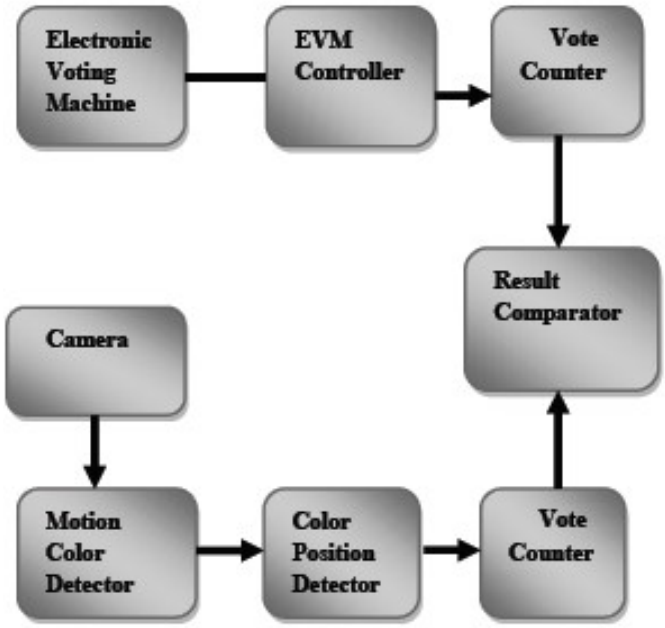
Voting is a basic right of every citizen in a democratic country. Free and fair election are very basic for endurance of democracy. Exercising of right to vote and for assuring that the vote which is cast is accounted in favor of the candidate and party which one likes is the very essence of democracy. First, the ballot paper were used for the election and the votes were casted manually. Now, the ballot paper based voting is replaced by electronic voting machine as the technology has improved a lot. It also gives quick result. On the other hand, many people's think that the electronic voting machines are hackable. They believe that the technology can be hacked and manipulated in support or beside a candidate/political party. If this be true, then the election process would end up being a shambles and democracy would be at risk. Most of the countries like Europe have shifted from normal paper ballot system to E.V.M with Voter Verifiable Paper Audit Trial System[V.V.P.A.T]. The system of the V.V.P.A.T is that one casts one's vote electronically but a receipt is printed by the machine attached to the system, where one's vote has been cast, whereas in the normal E.V.M that are used at present one just presses the button as per the choice of symbol allotted to candidate, but the voter never knows as to where the vote has been cast and whether it is as per the choice of voter. In this, the proposed system the surveillance camera is used to store the local copy of the vote with the vote timing. At last, the local copy stored inside the EVM and the data stored through surveillance camera are compared to get a authenticated result, which cannot be accused for malpractice.

II. PROPOSED SYSTEM

Electronic voting machine has a ballot and control unit. All the voting results will in offline chip.. A ballot based cross check mechanism is used to recount the voting in Old manual counting method.

This proposed system is camera based vote counting mechanism. A Non-hackable Multi vote count mechanism is introduced with camera based non contact vote counting. Voting timing details will be

available in camera and controller log which leads to accurate voting information. As this proposed system has complete verification, there need not be any worry to candidate as it checks for the authentication. Voter Verifiable Paper Audit Trial System[.V.P.A.T.S] is also don't need when the authenticated result only will publish.



III. HARDWARE

1. CAMERA

The name camera comes from camera obscure which means ―dark chamber‖. A camera is an optical instrument for recording or capturing images, which may be stored locally, transmitted to another location or both. It is used to senses objects without any contact with it. The functioning of the camera is related to the functioning of human eye. This camera is used to capture the image of electronic voting machine and stores the voting data with timing.

Figure 1

2. ELECTRONIC VOTING MACHINE:

Electronic Voting Machine used since 1999 and recently in 2018 state elections. This device is used to register or store votes. It consists of ballot unit and control unit. The ballot unit contains both blue buttons and corresponding party symbol and the control unit consists of battery section, display section, result section and ballot section.

Figure 2 BALLOT UNIT

Figure 3 CONTROL UNIT

3. ARDUINO KIT [UNO]:

Arduino kit is an open-source electronics board and the software used to program it. This board contains sets of digital and analog input/output pins and it consists of microprocessors and microcontrollers.

Figure 4

4. INFRARED LED's:

Infrared light emitting diode emitting range is between 700 nm to 1 mm wavelength. This led is madeup of aluminium gallium arsenide. A camera or cellphone camera is used to see this emission since human eye cannot see high emitting range.

Figure 5

IV. SOFTWARE:

1. MAT LAB:

MATRIX LABORATORY is used here for the color filtering process. It is a multi-paradigm numerical computing environment. MATLAB allows matrix manipulations, plotting of functions and data. It has five important parts namely the MATLAB language, the MATLAB working environment, Handle graphics, mathematical function library, application programming interface.

Figure 6

2. PYTHON:

Python is an interpreted, object oriented programming language similar to PERL. python is easy to learn and portable. Because the statements can be interpreted in many os like MAC os,MS DOS.

Figure 7

V. RESULTS:

MODULE NAME: COLOR FILTERING

An image contains RED, GREEN, and BLUE bands. Imread() is used to read the image. Imshow() is used to show the array values of the image. Color value can be predicted based on the dominant pixel he range in each image band. imread(filename), function reads color image from the file specified by the string filename. If the file is not present in the current directory, type the full path of the file on your system.

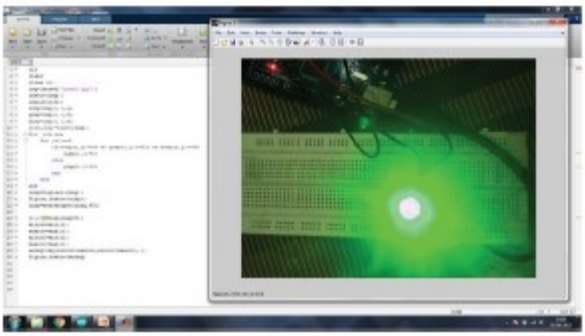


Figure 8

Figure 8 shows the image before color filtering. The green color is filtered by using threshold value.

Example: To produce a pure Red color pixel at(1,1) position,

Rband(1,1)=255,Gband(1,1)=0,Bband(1,1)=0.

The threshold value is used here to extract only the green light.

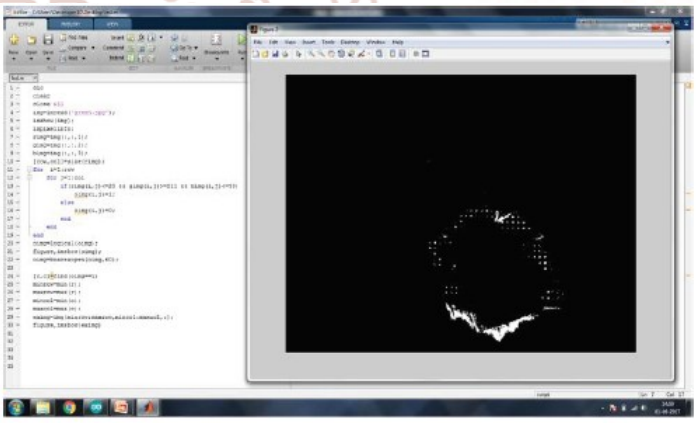


Figure 9

Figure 9 shows the binary image that is converted from RGB image[figure 5].Binary images is also called as bi-level or two-level.it is a digital image has only two possible values for each pixel which is either o or 1.A binary image can be stored in memory as a bitmap , a packed array of bits.

The below code is used here to convert the RGB image into binary image.

```
For(i=1:row)
   For(j=1:col)
If(rimg(i,j)<23&&gimg(I,j)>=211&& bimg(I,j)<=33)
          Oimg(i,j)=1;
       Else
          Oimg(i,j)=0;
       End
   End
End
```

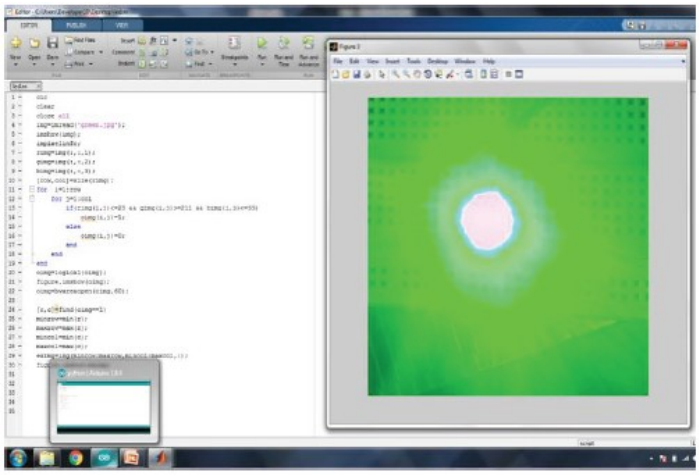


Figure 10

Figure 10 shows the green light extracted from the figure 8 by color filtering using the below code in mat lab.

```
[r,c]=find(oimg==1)
Minrow=min(r);
Mincol=min(c);
Maxrow=max(r);
Maxcol=max(c);
Eximg=img(minrow:maxrow,mincol:maxcol);
Figure,imshow(eximg);
```

MODULE 2: BUTTON MATRIX

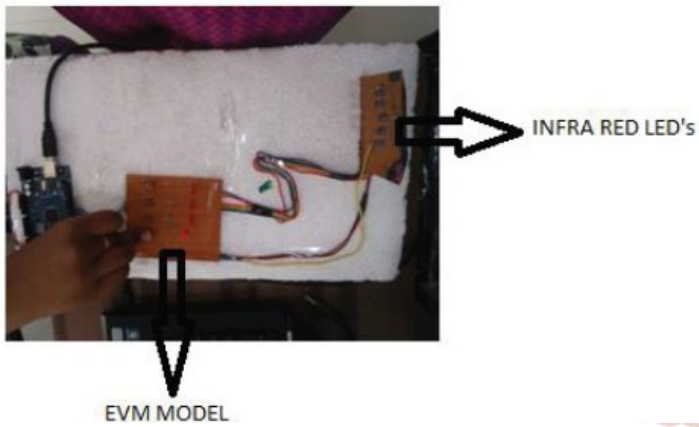
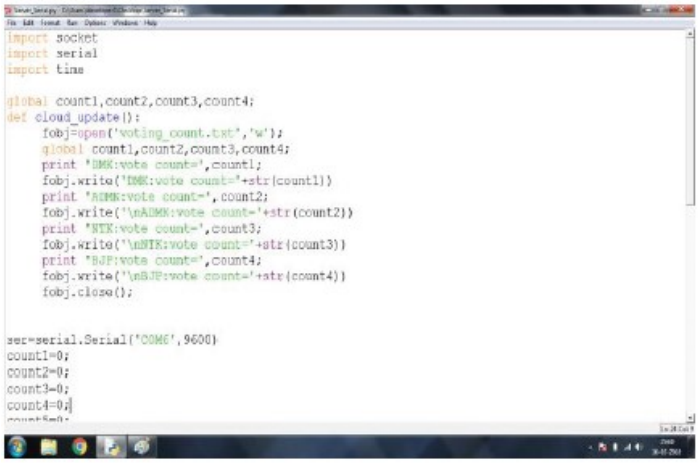


Figure 11

Figure 11, represents a model voting machine with four buttons and corresponding led's. This model is connected with the arduino kit to read the voting information.

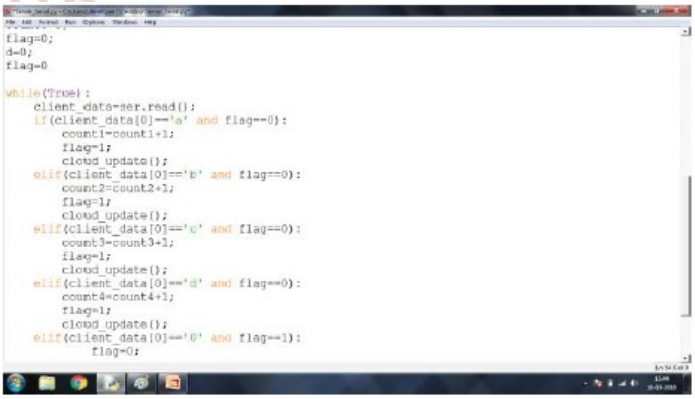


```
import socket
import serial
import time

global count1,count2,count3,count4;
def cloud_update():
    fobj=open('voting_count.txt','w');
    global count1,count2,count3,count4;
    print 'DMK:vote count=',count1;
    fobj.write('DMK:vote count='+str(count1))
    print 'ADMK:vote count=',count2;
    fobj.write('\nADMK:vote count='+str(count2))
    print 'NTK:vote count=',count3;
    fobj.write('\nNTK:vote count='+str(count3))
    print 'BJP:vote count=',count4;
    fobj.write('\nBJP:vote count='+str(count4))
    fobj.close();


ser=serial.Serial('COM6',9600)
count1=0;
count2=0;
count3=0;
count4=0;
```

Figure 12



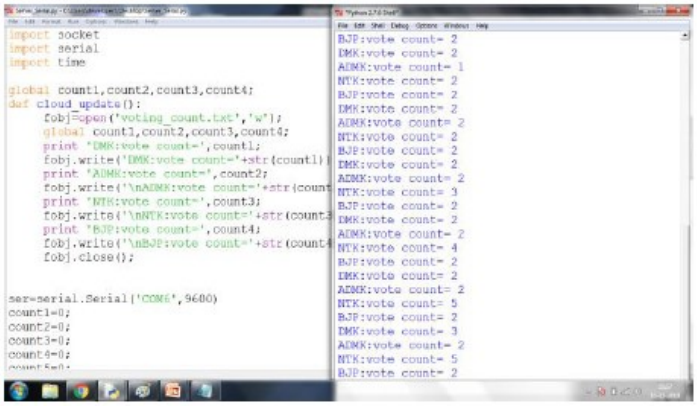
```
flag=0;
d=0;
flag=0

while(True):
    client_data=ser.read();
    if(client_data[0]=='a' and flag==0):
        count1=count1+1;
        flag=1;
        cloud_update();
    elif(client_data[0]=='b' and flag==0):
        count2=count2+1;
        flag=1;
        cloud_update();
    elif(client_data[0]=='c' and flag==0):
        count3=count3+1;
        flag=1;
        cloud_update();
    elif(client_data[0]=='d' and flag==0):
        count4=count4+1;
        flag=1;
        cloud_update();
    elif(client_data[0]=='0' and flag==1):
            flag=0;
```

Figure 13

Figure 12 & 13 represents the python code to store the voting information using arduino kit. This code is fully write by using python.

If button 1 is pressed the vote will be stored to party1 and likewise button 2 for party 2 , button 3 for party 3 and so on.



```
import socket
import serial
import time

global count1,count2,count3,count4;
def cloud_update():
    fobj=open('voting_count.txt','w');
    global count1,count2,count3,count4;
    print 'DMK:vote count=',count1;
    fobj.write('DMK:vote count='+str(count1))
    print 'ADMK:vote count=',count2;
    fobj.write('\nADMK:vote count='+str(count
    print 'NTK:vote count=',count3;
    fobj.write('\nNTK:vote count='+str(count
    print 'BJP:vote count=',count4;
    fobj.write('\nBJP:vote count='+str(count
    fobj.close();


ser=serial.Serial('COM6',9600)
count1=0;
count2=0;
count3=0;
count4=0;
```

```
BJP:vote count= 2
DMK:vote count= 2
ADMK:vote count= 1
NTK:vote count= 2
BJP:vote count= 2
DMK:vote count= 2
ADMK:vote count= 2
NTK:vote count= 2
BJP:vote count= 2
DMK:vote count= 2
ADMK:vote count= 2
NTK:vote count= 3
BJP:vote count= 2
DMK:vote count= 2
ADMK:vote count= 2
NTK:vote count= 4
BJP:vote count= 2
DMK:vote count= 2
ADMK:vote count= 2
NTK:vote count= 5
BJP:vote count= 2
DMK:vote count= 3
ADMK:vote count= 2
NTK:vote count= 5
BJP:vote count= 2
```

Figure 14

Figure 14 represents the output got when run the above python code.

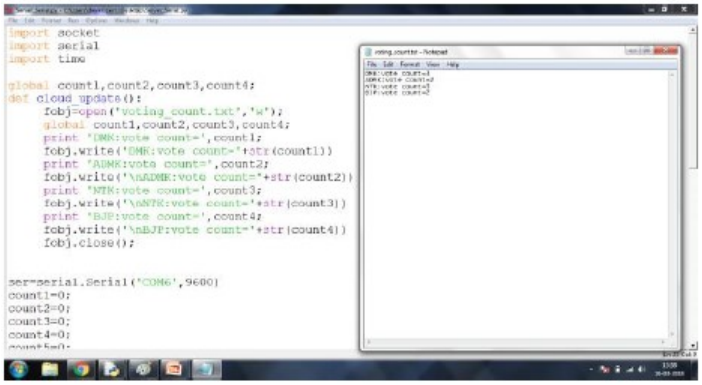


Figure 15

Figure 15 shows the voting counts stored in a file .we can store it in a database also. Finally, This local copy of the voted data will be compared with the data stored through surveillance camera.

VI. CONCLUSION:

By using this manifest voting machine we can check whether the EVM is secured or not to voting. This proposed system can compare the local copy of the data with the external copy of the data stored using image processing. The minimum amount to buy surveillance camera is 500. Hence, it is very economical to implement in election of India.

VII. FUTURE WORK:

This voting data can be stored in cloud for future work. and also can be encrypted by using encryption techniques.

VIII. REFERENCE:

1) Vote-switching software provided by vendors—A partial list reported in the news [Online]. Available: http://www.votersunite.org/info/Vote-Switchinginthenews.pdf

2) Project EVEREST: Risk assesment study of Ohio voting systems Dec14, 2007.

3) J. Bannet, D. W. Price, A. Rudys, J. Singer, and D. S. Wallach,—Hack-a-vote: Security issues with electronic voting systems,‖ *IEEE Security Privacy, vol. 2, no. 1, pp. 32–37, Jan./Feb. 2004.*

4) Secretary of State Debra Bowen moves to strengthen voter confidence in election security following top-to-bottom review of voting systems 2007[Online].Available:http://www.sos.ca.gov/elections/voting_systems/ttbr/db07_042_ttbr_system_decisions_release.pdf

5) R. I. S. Cell, Trusted Agent Report Diebold AccuVote-TS Voting System Jan. 2004.

6) D. Chaum, R. Carback, J. Clark, A. Essex, S. Popoveniuc, R. L. Rivest, P. Y. A. Ryan, E. Shen, and A. T. Sherman, Scantegrity ii: End-to-End verifiability for optical scan election systems using invisible ink confirmation codes 2008.

7) S. Davtyan, S. Kentros, A. Kiayias, L. Michel, N. C. Nicolaou, A. Russell,A. See, N. Shashidhar, and A. A. Shvartsman, —Pre-election testing and postelection audit of optical scan voting terminal memory cards,‖in Proc. 2008 USENIX/ACCURATE Electronic Voting Workshop (EVT08), San Jose, CA, Jul. 28–29, 2008.

8) S. Davtyan, S. Kentros, A. Kiayias, L. Michel, N. C. Nicolaou, A. Russell,A. See, N. Shashidhar, and A. A. Shvartsman, —Taking total control of voting systems: Firmware manipulations on an optical scan voting terminal,‖ in Proc. 24th Annual ACM Symp. Applied Computing (SAC09), Hawaii, 2009, pp. 2049–2053.

9) A. J. Feldman, J. A. Halderman, and E. W. Felten, Security analysis of the Diebold AccuVote-TS voting machine Sep. 13, 2006 [Online].Available: http://itpolicy. princeton.edu/voting

10) Help America Vote Act [Online]. Available:http://www.fec.gov/hava/law_ext.txt

11) A. Fujioka, T. Okamoto, and K. Ohta, —A Practical Secret Voting Scheme for Large Scale Elections‖, Advances in Cryptology - AUSCRYPT, 1992.

12) Peter G. Neumann, —Security Criteria for Electronic Voting‖, 16Th Computers, Freedom, and Privacy, Burlingame, California, 1993.

13) Michael Ian Shamos, —Electronic Voting – Evaluating the Threat‖, International Conference on Computers, Freedom, and Privacy, Burlingame, California, 1993.

14) Philip Klein, —An Untraceable, Universally Verifiable Voting Scheme‖, Seminar in Cryptology, December 12, 1995.

15) Lorrie F. Cranor and Ron K. Cytron, —Sensus: A Security-Conscious Electronic Polling System for the Internet‖, in the proceedings of the Hawai

International Conference on System Sciences, Wailea, Hawai, USA, January 7-10, 1997.

16) Herschberg, Mark A. (Mark Allan), ―Secure Electronic Voting over the World Wide Web‖, Master's Thesis, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, May 1999.

17) Brandon William DuRette, ―Multiple Administrators for Electronic Voting‖, Bachelor's Thesis, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, May 1999.

18) A. K. Jain, A. Ross, and S. Pankanti, ―A Prototype Hand Geometry-Based Verification System‖, 2nd Int'l Conference on Audio- and Videobased Biometric Person Authentication, Washington D.C., pp. 166-171, March 22-24, 1999.

19) Hand Book for Presiding Officers‖ (At Elections where Electronic Voting Machines are used), published by ―West Bengal State Election Commission‖ in 2000.

20) David Clausen, Daryl Puryear and Adrian Rodriguez, ―Secure Voting Using Disconnected, Distributed Polling Devices‖, Department of Computer Science, Stanford University, June 05, 2000.