IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 4, Issue 1, January 2016

Bio-metric Electronic Voting System for Election Process

RathnaPrabha.S[1], Trini Xavier.X[2], Deepika.V[3], Iswarya.C[4]

Assistant Professor, Saranathan College of Engineering, Trichy[1]

Final year-ICE, Saranathan College of Engineering, Trichy[2,3,4]

Abstract: There is lot of methods to avoid fraudulence in voting systems, but we are not able to eradicate it completely. This project will give solutions for the above mentioned problem. Fingerprint is one of the unique identities of a human being which is being used in the aadhar system. By using arduino software and by using image processing we capture the finger print of every individual and the face of the individual is being captured. Face of the person captured is compared to aadhaar details using lab view. In future, it could also be implemented using eye trace which will give more accurate results.

Keywords: Finger print, arduino, LabVIEW.

I.INTRODUCTION

In paper-based elections voters cast their votes by simply depositing their ballots in sealed boxes distributed across the electoral circuits around a given country. When the election period ends, all these boxes are opened and votes are counted manually in presence of the certified officials. In this process there can be error in counting of votes or in some cases voters find ways to vote more than once. Sometimes votes are even manipulated to distort the results of an election in favour of certain candidates [1]. In order to avoid these shortcomings the government of India came up with Direct-recording electronic (DRE) voting system which are usually referred as Electronic Voting Machines or EVMs. These devices have been praised for their simple design, ease of use and reliability. However it has been found that EVMs are not tamper proof and are easily hackable. Moreover this attacks, hardware as well as software, go without any detection but are quite simple to implement. This made us to bring forth a system that is secure, transparent, reliable as well as easy to use for the citizens. Biometric e-voting systems are not a phenomenon anymore they are being actively used in countries like Ghana and Ireland and are spreading to many other developing nations.[4,5] In this project we propose an avoid fraudulence in mechanism to make e-voting in India a reality.

II. BLOCK DIAGRAM

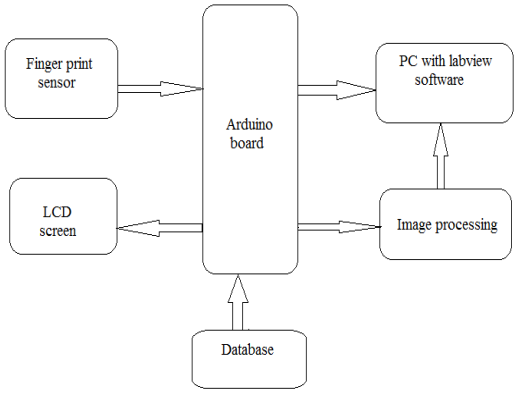

Fig.1.Block diagram of e-voting process

The above block diagram projects the microcontroller based architecture of the E-Voting system.

III. HARDWARE CONFIGURATION

ARDUINO :

There are many different types of electronics hardware development boards featuring embedded processors and the most famous species like Raspberry pi, BeagleBone, Arduino Galileo. The embedded world evolved very differently there were too many choices for processors, which were mainly chosen for price and features. The devices like Raspberry pi and Beagle Board are best for handling media such as video. They are designed to function on a much higher level with already integrated hardware that takes care of things like Ethernet, video processing, large quantities of RAM and an almost unlimited amount of storage space. In the other side the Arduino is an excellent choice if we have a project requiring sensors (and decent memory and processing power), monitoring, or have productivity-related applications (Galileo has a real time clock.) Galileo could be used to develop smart everyday "things" with lots of sensors, such as health monitoring, security system, home automation, fitness devices, or simply be an inexpensive personal computer running Linux sans all things Arduino.

1) Fingerprint stage:

This system registered the users that consideras authority to access control inthe enrollment model as shown in the (Fig.2).Each user in this stage will take theAadhaar ID number that save in the database. Fig.2 The fingerprint enrollment block diagram

In(Fig.3)showstheblokdiagramofthefingerprintverification model.Fig.3The fingerprint verification block diagram . In fingerprint stage we used two important functions: feature extraction and the matching function. The briefdescription of these functions as follow:

2) Feature Extraction

The feature extraction isresponsible for expressing fingerprint's unique characteristics adequately such as

directions of the lines, terminals of lines, bifurcation and so on. To ensure the accuracy of comparison, the method of feature extraction must extract useful features as such as possible; meanwhile, filter false features for various reasons. There are two kinds of features in fingerprint images: global feature and local feature. Global feature can reflect overall shaper of fingerprint, which usually applies to fingerprints'classification,the process of extract global feature frequently belongs to procedure of fingerprint classification. TheLocal feature can reflect minutiae of fingerprint, usually applies to fingerprints' comparison. [16]Strict feature extraction means local features' extraction. Two fingerprints often have the same global features, but their local features cannot be exactly the same. The importantinformation of fingerprints' local feature isfollowing: terminals, bifurcations, branch points, isolated points, enclosures, short lines and so on. In fact, not all the fingerprints have these two features, it often be used as fingerprints' sub-matches [17].This systemuses terminals and bifurcations infeature extraction and matching algorithm.

3)Feature Matching:

The matching function, features extracted from the input fingerprint is compared against those in a database, which represents a single user (retrieved from the system database based on the claimed identity). The result of such a procedure is either adegree of similarity (also called matching score) or an acceptance/rejection decision. There are fingerprint matching techniques that directly compare gray scale images using correlation-based methods, so that the fingerprint template coincides with the gray scale image. However, most of the fingerprint matching algorithms use features that are extracted from the gray scale image. A large number of approaches to fingerprint matching can be found in previous work[17,18]. In this proposed work we used the matching algorithm that support theoptical fingerprint reader moduleSFG algorithm is specially designed according to the image generation theory of the optical fingerprint collection device. It has excellent correction &tolerance to deformed and poor-quality fingerprint and work with both 1:1 and 1:N.Fingerprint SensorFeature ExtractionEnrollment modelDBID.

4. Face recognition:

Every human could be identified by the faces and could be easily recognised by the faces. Early face recognition algorithms used simple geometric models, but the recognition process has now matured into a science of sophisticated mathematical representations and matching processes. Thus the face recognised could be both verified and identified. Thus, by using face recognition here we could avoid the fraudulence

OVERVIEW OF Lab VIEW

ACQUISTION OF SIGNAL

Designing of LABVIEW is used with hardware supported by National Instrument MYRIO driver. USB communication cable, PCI device with analog input also include in that. NI MYRIO device is device created using MYRIO option in the menu of function block of lab view for operating the program without use hardware.

PROCESSING AND ANALYSING OF SIGNAL

There is a lot of built in analysis function available in Lab VIEW, which is used to easily create the program for complementary problem. Filter, PID control algorithm, converter and correction factor, simulated signals these are commonly used library.

DISTRIBUTED APPLICATION

Lab VIEW has some important features to develop the distributed application using internet toolkit, VI, MYRIO-Wi-Fi.

IV. WORKING

The personal details of the voters in an area are already registered in the database. Duringelection, the voter keeps their finger print in the biometric sensor. At the same time, a camera captures the image of the voter and compares the image and the details, stored in the database. If the same person was found to be voted already, the voting would be cancelled.

V. CONCLUSION

Thus, the arduino controller could be interfaced in LabVIEW environment. The real time vote monitoring is made possible and finding of repeated voting by same voter could be detected easily.

REFERENCES

[1] Khasawneh, M., Malkawi, M., & Al-Jarrah, O. (2008). A Biometric-Secure e-Voting System for Election Process. Proceeding of the 5th International Symposium on Mechatronics and its Applications (ISMA08). Amman, Jordan.

[2] Prasad, H. K., Halderman, A. J., &Gonggrijp, R. (Oct. 2010). Security Analysis of India's Electronic Voting Machines. Proc. 17th ACM Conference on Computer and Communications Security (CCS '10). INTERNATIONAL JOURNAL FOR RESEARCH IN EMERGING SCIENCE AND TECHNOLOGY, VOLUME-2, ISSUE-3, MARCH-2015 E-ISSN: 2349-7610 VOLUME-2, ISSUE-3, MARCH-2015 COPYRIGHT © 2015 IJREST, ALL RIGHT RESERVED 90

[3] UIDAI. (2012). Role of Biometric Technology in Aadhaar Authentication.

[4] Yinyeh, M. O., &Gbolagade, K. A. (2013). Overview of Biometric Electronic Voting System in Ghana. International Journal of Advanced Research in Computer Science and Software Engineering.

[5] McGaley, Margaret. "Irish Citizens for Trustworthy Voting." 6 July 2004. http://evoting.cs.may.ie/

[6] UIDAI, Biometrics Design Standards For UID Applications, 2009

.