BIO-METRICS BASED ELECTRONIC VOTING MACHINE USING WIRELESS FIDELITY

*S. Allwin Devaraj **M.Muthamil Jothi ***A.Nancy
Francis Xavier Engineering College

***ABSTRACT*-Biometric identification technologies have been associated generally with very costly secure applications. IRIS recognition and authentication which is a recent one is a well secured method. Here in this paper, the implementation of electronic polling system. Here the two unsocial practices bogus vote and booth capturing is being tried to be eradicated based on "One election -One vote- one person" Election process is made mobile by employing wireless fidelity in it. Any person can cast his/her vote any where in the country. The wi-fi are used only during counting process, and one more added advantage is that one Biometric Voting Machine (BVM) accepts only one vote at a time and one vote for that election from the same user, not like in the case of present EVM's. The hardware is done with conventional storage IC's available in the market and the software is written in Visual Basic 6.0.**

I INTRODUCTION

"A biometric is a unique, measurable characteristic or trait of a human being for automatically recognizing or verifying identity. "This measurable characteristic, biometric, can be physical, such as eye, face, finger image, hand and voice or behavioural, like signature and typing rhythm. Biometric system must be able to recognize or verify it quickly and automatically.

a) IRIS RECOGNITION

Of all the biometric technologies used for human authentication today, it is generally conceded that iris recognition is the most accurate. Coupling this high confidence authentication with factors like outlier group size, speed, usage/human factors, platform versatility and flexibility for use in identification or verification modes - as well as addressing issues like database size/management and privacy concerns - iris recognition has also shown it to be exceedingly versatile and suited for large population applications.

b) THE BIOLOGY BEHIND THE TECHNOLOGY:

The iris - the externally visible colored ring around the pupil - of every human eye is absolutely unique, exhibiting a distinctive pattern that forms randomly in utero in a process called chaotic morphogenesis. In fact, it's estimated the chance of two irises (irides) being identical is 1 in 10^{78}.

A. ELECTRONIC VOTING MACHINES: Electronic voting machines use a two-piece system with a balloting unit presenting the voter with a button (momentary switch) for each choice connected by a cable to an electronic ballot box.

An EVM consists of two units:

1. Control Unit 2. Balloting Unit

A five-meter cable joins the two units. The Control Unit is with the Presiding Officer or a Polling Officer and the Balloting Unit is placed inside the voting compartment. Instead of issuing a ballot paper, the Polling Officer in-charge of the Control Unit will press the Ballot Button. This will enable the voter to cast his vote by pressing the blue button on the Balloting Unit against the candidate and symbol of his choice. The microchip used in EVMs is manufactured in Japan and it is sealed at the time of import. It cannot be opened and any attempt to rewrite the program cannot be done without damaging the chip.

B. FEATURES

Currently, an EVM can record a maximum of 3840 votes, can cater to a maximum of 64 candidates. There is provision for 16 candidates in a Balloting Unit. If the total number of candidates exceeds 16, a second Balloting Unit can be linked parallel to the first Balloting Unit. Similarly, if the total number of candidates exceeds 32, a third Balloting Unit can be attached and if the total number of candidates exceeds 48, a fourth Balloting Unit can be attached to cater to a maximum of 64 candidates.

II PROPOSED METHODOLOGY

Booth capturing - the major drawback in the conventional voting system, where a person can cast as many as votes he / she can. With dropping bunch of ballot papers at a time and pressing the EVMs any number of times. This paper eliminates the above through **"one election - one person – one vote"** agenda.

The very first aim of this paper is to provide an effective technology in the voting system.

1) Making more secure method of election process
2) Making the voting process much easier than the present scenario

Strengthening the democracy by eliminating bogus votes

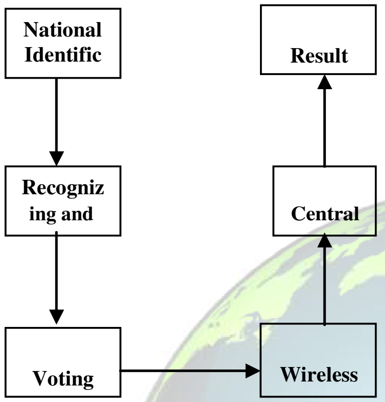


Fig. 1General Block Diagram

NATIONAL IDENTIFICATION CARD:

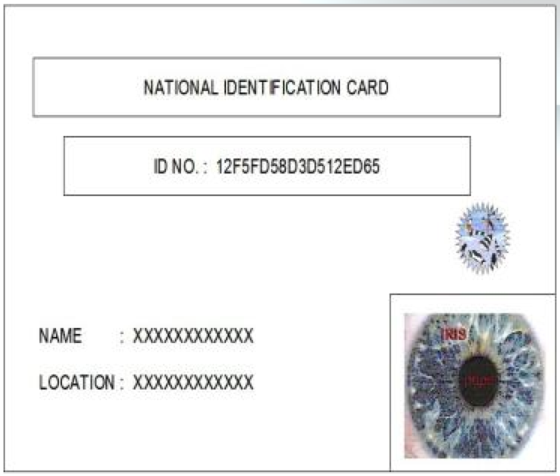
It furnishes all the details about the voter. It consists of three parts.

1. Name

2. Location

3. 2D image of iris pattern

This card provides multi utility service (MUS) which can be used in all security applications wherever necessary



NATIONAL IDENTIFICATION CARD

ID NO. : 12F5FD58D3D512ED65

NAME : XXXXXXXXXXXX

LOCATION : XXXXXXXXXXXX

Fig. 2 National Identification Card

The data's retrieved from this NIC:

1. A recognized hologram of the government.
2. An identification number of that person.
3. A 2-D image of that person's iris..
4. A general list of his / her details of location or constituency.

This type of card is issued to all the voters of the country, where the specimen is taken from each individual to print it on the card and to maintain a database. (Fig 2)

III **RECOGNIZING AND VERIFYING OF IRIS PATTERN**

It employs iris recognition technology to provide accurate identity authentication without PIN numbers, passwords or cards. Enrollment takes less than 2 minutes. Authentication takes less than 2 seconds.

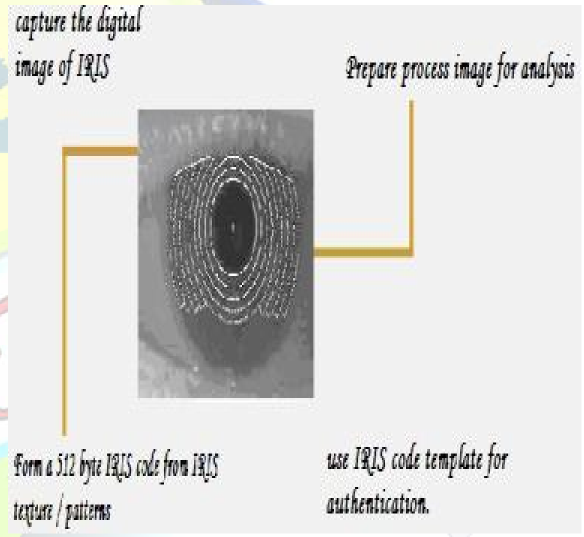

capture the digital image of IRIS
Prepare process image for analysis
Form a 512 byte IRIS code from IRIS texture / patterns
use IRIS code template for authentication.

Fig. 3 Capturing Image Pattern

With a device activated by proximity sensor, a subject positioned 3" to 10" from the Enrolment Optional Unit is guided by a mirrored, audio-assisted interactive interface to allow an auto-focus camera to take a digital video of the iris. Individual images from the live video are captured using a frame grabber. The innovative algorithm of the iris recognition process analyses the patterns in the iris that are visible between the pupil and sclera (white of the eye) and converts them into a 512-byte digital template.

This value is stored in a database and communicated to Identification Control Units associated with portals where the subject has access privileges. The Recognition takes just 2 seconds in this method. Upon approaching a portal protected by Iris Access, proximity sensors activate the Remote Optical Unit (ROU) when the subject nears the operational range of the unit.

became familiar with at enrolment helps ensure proper positioning and speedy recognition.

The ROU uses the same video and frame-grabbing methodology to create, select and digitize an image to be compared against the data retrieved on the spot. The live presented value is compared against the data took from the NIC inserted Once the iris is matched, either a direct signal is sent to unlock the voting pad.

IV VOTING PROCESS

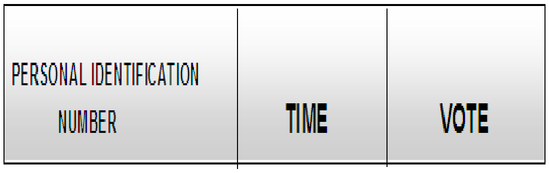
A. VOTING THROUGH ELECTRONIC VOTING MACHINE:

Voter will be called by name as usual to put his signature on Voting Register.
Electoral Officer will put special ink on his finger as usual. Electoral Officer will hand over a slip containing voter's serial number as shown in the Voter Register.
Voter will hand over the slip to Presiding Officer. He will satisfy himself about the genuineness of the particulars of the voter.
After all these formalities, voter will be asked to reach at Electronic Voting Machine kept in a corner covered from sides to maintain secrecy of the vote.

Voting Machine will contain candidates name and symbol against each name. There will be a red light and a blue button. Red light will appear on the pressing of blue button and sound like whistle will also be heard which will indicate that the ballot has been casted.

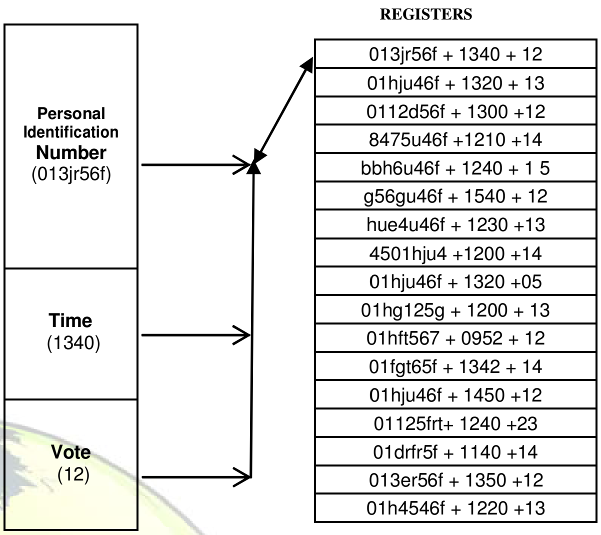
BIOMETRIC VOTING MACHINE (BVM):

- The person can cast his valuable vote at any of the polling booths available around his proximity
- Only by using his / her NIC (National Identification Card), he / she can have access with the BVMs.
- The voter has to insert his NIC into a 2D – scanner and also provide his on spot IRIS authentication.
- Only if the data's took fro the NIC and his / her on-spot IRIS pattern matches the BVM will go hand to hand with the voter otherwise it sounds an alarm to alert the security personnel present in there.
- Now the voter can cast his / her vote towards the party he / she desires.
- This casted vote will get stored in a memory register along with the PIN provided in the NIC .



PERSONAL IDENTIFICATION NUMBER	TIME	VOTE

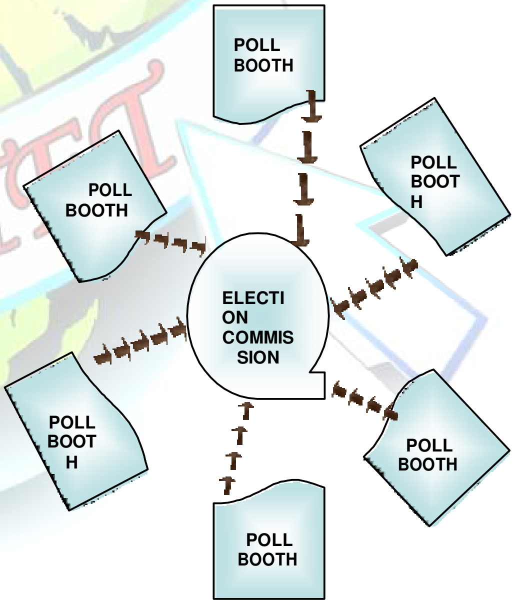
Fig. 4 Register split



REGISTERS
013jr56f + 1340 + 12
01hju46f + 1320 + 13
0112d56f + 1300 +12
8475u46f +1210 +14
bbh6u46f + 1240 + 1 5
g56gu46f + 1540 + 12
hue4u46f + 1230 +13
4501hju4 +1200 +14
01hju46f + 1320 +05
01hg125g + 1200 + 13
01hft567 + 0952 + 12
01fgt65f + 1342 + 14
01hju46f + 1450 +12
01125frt+ 1240 +23
01drfr5f + 1140 +14
013er56f + 1350 +12
01h4546f + 1220 +13

Fig. 5 memory registers will be stored in main memory

WIRELESS FIDELITY



A typical Wi-Fi setup contains one or more Access Points (APs) and one or more clients. An AP broadcasts its SSID (Service Set Identifier, "Network name") via packets that are called beacons, which are usually broadcast every 100 ms. The beacons are transmitted at 1 Mbit/s, and are of relatively short duration and therefore do not have a significant effect on performance. Since 1 Mbit/s is the lowest rate of Wi-Fi it assures that the client who receives the beacon can communicate at least 1 Mbit/s. based on the settings (e.g. the SSID), the client may decide whether to connect to an AP. If two APs of the same SSID are in range of the client, the client firmware might use signal strength to decide which of the two APs to make a connection to. The Wi-Fistandard leaves connection criteria and roaming totally open to the client. This is strength of Wi-Fi, but also means that one wireless adapter may perform substantially better than another. Since Wi-Fi transmits in the air, it has the same properties as a non-switched wired Ethernet network, and therefore collisions can occur. Unlike a wired Ethernet, and like most packet radios, Wi-Fi cannot do collision detection, and instead uses a packet exchange (RTS/CTS used for Collision Avoidance or CA) to try to avoid collisions. (Fig 6)

***CENTRAL SERVER**:*

When the election finishes the entire data present in the memory of the BVM is now brought to the central server and connected through WI-FI to the central server located at election commission office.Though they are connected in wi-fi, the data transfer is privatized, as in the case of electronic mails. This is the stage where the bogus votes are eliminated.

PROCESSING:

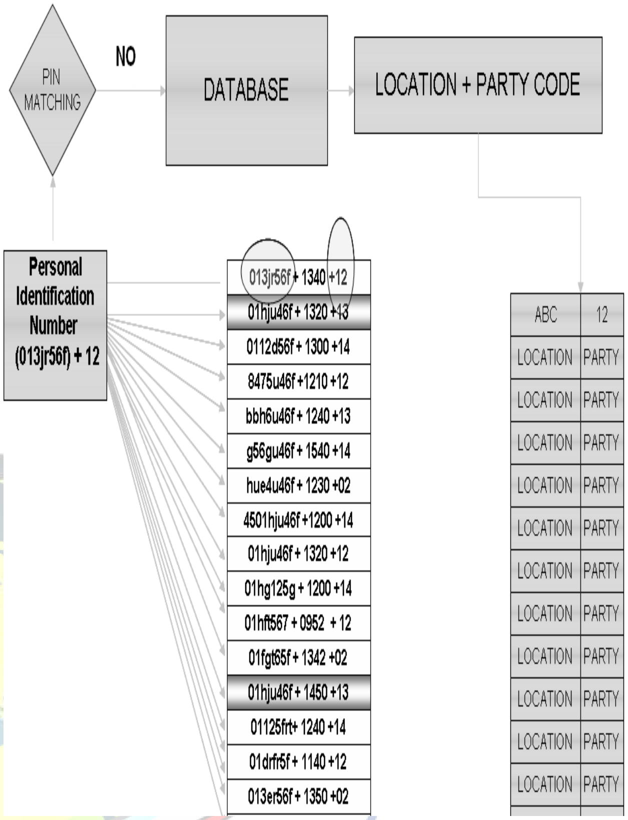
Here the data (9 bit) from the BVM is taken through Wi-Fi and finally stored in the central memory. Processing state decides the location of storage in the central memory by assigning the address to the data. If there are 5000 polling booths as a whole, a group of randomly selected polling booths are say 500 at a time will be connected to a central server through WI – fi system. Now the data present in the memories of these BVMSs will be transferred at a time, at a minimum rate of 1 Mbits/ sec. the server acts intelligently to receive the information through WI – fi system and store the data in its own memory locations. (Fig 6).

RESULT PROCESSING:

The array of memory registers bought, are to be processed for bogus votes before increasing the count of any political parties to which the vote has been casted. This can be explained well from the following For example, here there are two memory registers (highlighted) with different time at which the vote has been casted but they have the same PIN (8 bit). Here the priority has been set so that the memory register with low time will be taken in to account, while the other one will be discarded or it may be taken in to account for tracing the culprit. In other way around, the vote will be counted to the respective party say XYZ, with regards to the constituency of the voter.

TWO CASES OF RESULT PROCESSING:

Usually the memory registers are stored in array of stacks as shown in figure. From the top of the stack, two data's are retrieved for bogus vote correction, one being the PIN and other the TIME by which the vote has been casted.



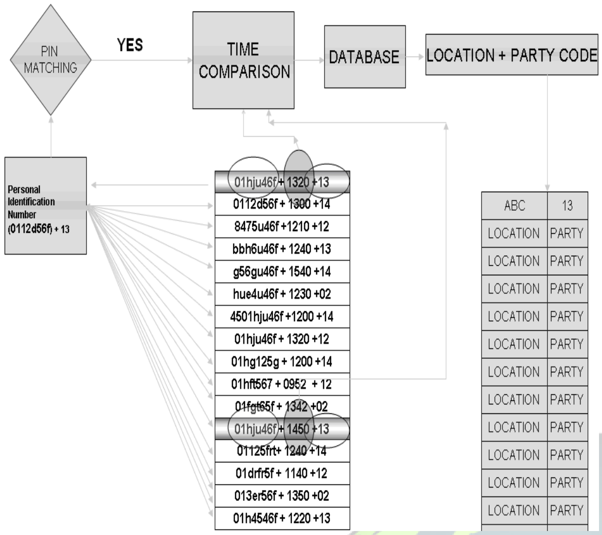
This is held in a buffer memory where the PIN no. alone is taken and compared with the other pin numbers in the rest of the stacks. (No matter what the number of stacks may be).

CASE 1*:* When the PIN number doesn't match: This is the case where no voter has casted his / her vote twice, that is, no same person has voted in one or more BVM's.

EXPLANATION:

Here the 4 byte PIN number (013jr56f) and the Party code that he has voted for, is taken into a buffer memory. From here the PIN number alone is taken and compared with the other PIN numbers in the stacks. Here, no two PIN numbers are same and so, the case is set as "NO PIN MATCH FOUND ". Now the PIN number and the party code (12) are forwarded to the DATABASE. Here, the Location (ABC) of the corresponding pin numbered person is now taken from the database and combined with the party code as shown and is now forwarded to a memory from where the results can be declared easily.

CASE 2: When the PIN number matches: This is the case where a voter has casted his / her vote twice, that is, the same per son has voted in one or more BVM's.



Here the 4 byte PIN number (01hju46f) and the Party code that he has voted for (13), is taken into a buffer memory. From here the PIN number alone is taken and compared with the other PIN numbers in the stacks. Here, no two PIN numbers are same and so, the case is set as "A PIN MATCH FOUND ". So a bogus vote has been casted. So, the time factor comes in to matter, that is, the least time (1320 >1450) from the matches found is taken. Then the other matches found are determined and deleted from the memory. (This PIN number may be forwarded to the crime department) Now the PIN number retrieved and the respective party code (13) are forwarded to the DATABASE. Here, the Location of the corresponding pin numbered person is now taken from the database (ABC) and combined with the party code as shown in fig. and is now forwarded to a memory from where the results can be declared easily. In both the cases, when the Location + party code are to be stored in the memory, a search process goes on, as to locate the address where the data for the Location is same as this. if it is found , then an another search process takes place, for finding the same party and if it is found , this LOCATION + PARTYCODE is saved next to that match found by altering the stack. If a match doesn't exist, this will be saved in a new location.

RESULT ANNOUNCEMENT:

For this, just locate the address where the location of the constituency exists in the memory and the number of votes is counted by proceeding to the next stack. This is an easy process and takes a very less time, depending on the votes casted for that constituency.

V ADVANTAGES

One vote per machine- In EVM's in an hour a person can cast 150 votes, but in the same BVM a person cannot recast vote another time as it will compare with its memory for the PIN and will not unlock its voting pad.

Defined mobility- A person can cast his/her vote anywhere else in the country. During result processing his/her vote will be separated according to his/her constituency, without giving up their constitutional rights.

Bogus voting- The major disadvantage of all other voting machine has been eliminated in this BVM's

Booth capturing- As only one vote will be accepted per machine a person cannot practice these kind of criminal activities.

Less number of personnel- One booth officer and one or two persons for security purpose is enough.

COST:Nowadays IRIS scanner costs around Rs.4500 and the memory storage device is a 1 GB memory chip. This cost seems to be high gut it will get reduced during mass production.

VI CONCLUSION

While the most common use of iris recognition to date is physical access control in private enterprise and government, the versatility of the technology will lead to its growing use in large sectors of the economy such as transportation, healthcare, and national identification programs. Managing this convergence of physical and information security requirements now drives security system architecture design and implementation, and is an increasingly key factor in biometric technology selection. Managing convergence will only become a more complex task because as the IT and communications becomes increasingly wireless, the need for robust identity management will become more acute

REFERENCES

1) www.biometrics.org/html/REPORTS/BioRef.html
2) www.scholarpedia.org/article/Biometric_authentication
3) ngm.nationalgeographic.com/your-shot/voting-machine