International Journal of Innovative Research in Computerand CommunicationEngineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.194 |

||Volume 8, Issue 4, April 2020||

Fingerprint Recognition Based Biometric Voting Machine

Dr. Latha. L, Aravind. M, Sipinath. S. V, Hari Prem Kumar. S

Professor, Dept of Computer Science & Engineering, Kumaraguru College of Technology, Coimbatore, India

Final year, Dept of Computer Science & Engineering, Kumaraguru College of Technology, Coimbatore, India

Final year, Dept of Computer Science & Engineering, Kumaraguru College of Technology, Coimbatore, India

Final year, Dept of Computer Science & Engineering, Kumaraguru College of Technology, Coimbatore, India

ABSTRACT: Fingerprint Voting Machine will be implemented using the Arduino technology. In this system, a voter can poll his/her vote easily. In this database server, all voter information will be stored to register in the system. This information will be checked by the database server and allows the user to see the list of candidates that re displayed on random order in TFT screen if and only he is first time voter. After the successful voting the machine displays the voted details and stored in database for future counting process.

KEYWORDS: fingerprint voting system, Arduino, touchscreen display, a biometric sensor, clustering algorithm.

INTRODUCTION

Biometrics refers to technologies that measure and unriddle human soul characteristics, such as DNA, fingerprints, eye retinas and irises, voice patterns, facial patterns, and hand measurements, for hallmark purposes. India is the largest democracy in the world. But India faces a huge threat of rigging in the election, due to the population of over a billion in which many of the voters fails to validity to vote. This is used as a wholesomeness by some political parties to impersonate the absentee voters to rig the elections to their advantage. This poses a threat to the integrity of our country and the citizen's trust in the electoral commission. To eliminate such limitation and modernize the reliability of the voting processes, the government initiative Aadhar is utilized to identify the individuality of each voter and at the same time ensuring their anonymity and their nomination of the candidate. This paper proposes a system that would replace the standard Electronic Voting Machine with an updated bio-metric identification system using a fingerprint scanner which is interfaced with the voting machine and the government database containing the data of each resider and verifying the eligibility of each voter. It prevents fake voting plane if the card is stolen the biometric data of the resider is sectional to each individual. This system can moreover be improvised to remove postal voting and the need for the voter to travel to their constituency as all such data is once present in the Aadhar database.

II.LITERATURE REVIEW

Vishal Vilas Natu [1] proposed the voting system is completely depending on paperwork and electronics machine. There is increasingly paperwork to save the information of voter and the voter must go to the ballot box by delivering voter id for authentication. One hallmark is washed-up by referendum executive then voter donates their vote by using electronic machines. The machine consists of a list of candidates and presents multiple buttons in front of their particular name by pushing the sawed-off voter can donate their vote to candidates. To overcome this traditional referendum system there has to study digital technology and their security.

Khasawneh, M., et al. said in paper-based elections voters tint their votes by simply depositing their ballots in sealed boxes distributed wideness the electoral circuits virtually a given country. When the referendum period ends, all these boxes are opened, and votes are counted manually in the presence of the certified officials. In this process, there can be an error in counting of votes or some cases voters find ways to vote increasingly than once. Sometimes votes are plane manipulated to misconstrue the results of a referendum in favor of unrepeatable candidates [2].

Virendra Kumar, et al. [3] proposed An Electronic Voting System that will automatically perform authentication, validation and counting with the help of UIDAI. The proposed electronic voting system can be implemented withal with the traditional referendum system. The proposed tideway will use the information provided by UIDAI in the electronic voting system.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.194 |

||Volume 8, Issue 4, April 2020||

David Chaum [4] addressed the concepts of untraceable electronic mail and digital pseudonyms, which can wield for electronic voting for anonymity.
Virendra Kumar Yadav et al. [5], a tideway that will use the information provided by UIDAI in the smart voting system. The proposed system procedure is carried out in mainly a few stages: registration, verification, and validation. These stages of the proposed system are illustrated.

D. Ashok Kumar et al. [6] made a comparative Study on Fingerprint Matching Algorithms for EVM. Then fingerprint matches voters can vote to the candidate by using EVM. The fingerprint is a secure method for EVM.

Jefferson D., et al. [7] reviewed and computer of critique and security liaison insecure voting system. The web-based voting system stuff built by Accenture. And insecurity the fingerprint technology is used.

Qijun Zhao, et al. [8] proposed an adaptive pore model for fingerprint pore extraction. Sweat pores have been recently employed for streamlined fingerprint recognition, in which the pores are usually extracted by using a computationally expensive skeletonization method or a unitary scale isotropic pore model.

R. Moheb et al. [9] proposed a tideway to image extraction and well-judged skin detection from web pages. Their system to periscope images from web pages and then snift the skin verisimilitude regions of these images.

Manjeet Kaur et al. [10] proposed a fingerprint verification system using the minutiae extraction technique. Most fingerprint recognition techniques are based on minutiae matching and have been well studied.

Hoi Le and The Duy Bui, [11] proposed online fingerprint identification with a fast and distortion tolerant hashing method. They present a specific contribution by introducing a new robust indexing scheme that is worldly-wise not only to spike the fingerprint recognition process but moreover to modernize the verism of the system.

Mayank Vatsa et al. [12] proposed combining pores and ridges with minutiae for improved fingerprint verification. This paper presents a fast fingerprint verification algorithm using level-2 minutiae and level-3 pore and ridge features. The proposed algorithm uses a two-stage process to register fingerprint images.

UmutUludag et al. [13] proposed a Biometric template selection and update: a specimen study in fingerprints. Sweat pores have been recently employed for streamlined fingerprint recognition, in which the pores are usually extracted by using a computationally expensive skeletonization method or a unitary scale isotropic pore model.

Andrew Ackerman [14], the smart e-voting system has been washed-up on fingerprints in humans. Two fundamentally main goals have risen from the voting process first A person's fingerprint will not transpiration the structure naturally without well-nigh one year without lineage and second, the fingerprints of individuals are different. Plane the twins in fingerprints are not the same. In practice, two humans with the same fingerprint have never been found.

III.EXISTING SYSTEM

An EVM consists of two units namely Tenancy Unit and Balloting Unit. The two units are joined by a five-meter cable. The Tenancy Unit is with the Presiding Officer or a Polling Officer and the Ballot Unit is placed inside the voting compartment. Instead of issuing a ballot paper, the Polling Officer-in-charge of the Tenancy Unit will be printing the Ballot Button. This will enable the voter to tint his/her vote by pressing the indecorous sawed-off on the Ballot Unit versus the candidate and symbol of his/her choice. The controller used in EVMs has its operating program etched permanently in silicon at the time of manufacturing by the manufacturer. No one (including the manufacturer) can transpiration the program once the controller is manufactured. EVMs can cater to a maximum of 64 contesting candidates. There is provision for only 16 candidates in a Bu if the total number of candidates exceeds 16, then a second BU is to be linked parallel to the first BU. Similarly, if the total number of candidates exceeds 32, then a third BU is to be unfluctuating and if the total number of candidates exceeds 48, fourth BU is to be unfluctuating to cater to a maximum of 64 candidates. As the process is faster and increasingly reliable, the EVMs save a considerable value of time, money, paper and manpower. The Actual process of identifying the voter has to be washed-up by the polling officer. For the tossing of votes with EVMs, the voters have to produce their Referendum Photo Identity Card(EPIC) issued by the Referendum Commission. The polling officer needs to verify the EPIC with the official list he has, then he needs to personalize whether it is authorized card or not and he allows the voters to tint their votes. Therefore, EVMs depend upon transmission verification of the EPIC. Consequently, this slows lanugo the voting process. This limitation is overcome with the help of the fingerprint identification module. The second limitation is the number of contesting candidate’s misogynists in the EVM. The EVMs can cater to a maximum of 64 candidates with the use of

one CU and four BUs. If the number of contestant candidates exceeds 64, then the polling officer needs to siphon one increasingly set of EVM that necessitates increasingly material and spare manpower.

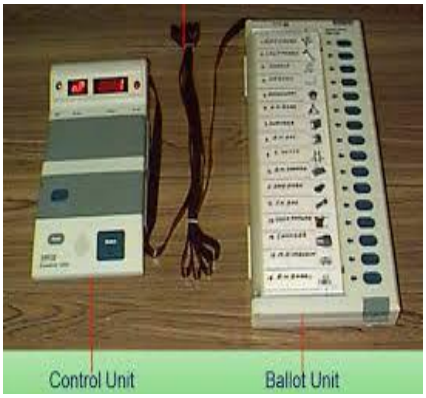

Fig.1: Electronic Voting Machine (EVM)

DISADVANTAGES OF THE EXISTING SYSTEM

- Less Authentication
- Duplication of votes
- Delaying in the declaration of results
- Subject to guessing of the candidate selected
- Repetition of candidates
- Inconsistency in final results

IV.OBJECTIVE

The fingerprint voting project demands the user to submit a Fingerprint at the polling booth. The project uses Fingerprint technology and Arduino Systems to diamond this application. The main objective of this project is to diamond a system that asks the user to show his/her Fingerprint as an identity proof. The system reads the data from the Fingerprint and verifies the data which is once stored data in the database. If the given details match with the database data, the system allows the person to tint their vote. If the given Fingerprint data does not match with the stored data, the system immediately activates the exhibit and the security authorities can come and take remoter action.

V.PROBLEM DEFINITION

In 21st century society where electronic technology is growing at an ever-increasing rate, it is difficult to understand why governments were not converting their paper-based referendum systems to electronic form to guaranty "One Person – One Vote and to eliminate fraud and corruption. An example of how a paper-based voting system is with disabilities and vulnerable to self-indulgence can be found in the elections, where the last referendum was invalidated due to fraudulent paper ballots used to stuff the ballot boxes and elect a president illegally. To repair this damage, it has once forfeit which could be a recurring forfeit if the fraud occurred then and it is difficult to bring charges versus the people committing the treason due to lack of vestige and a to inspect trail that could be used as a "Chain of Evidence" by lawyers. Flipside example is when paper referendum ballots ran out at an American referendum and spare ballots were produced using a printer and make-shift process for creating the new ballots on white paper instead of the normal indecorous ballots. People rushed to obtain the new white ballots and quickly completed them and stuffed them into the ballot boxes in a manner that was not traceable and could have been fraudulently submitted, showing that plane first world countries suffer from the use of paper-based ballots.

VI.FINGERPRINT VOTING SYSTEM

Our model contains a fingerprint scanner that scans the fingerprints of the voter and stores in the database. The details of the voter are moreover stored with the primary key and are stored in the same database. Our machine replaces traditional buttons with a touch screen to exhibit the candidate details that exhibit random order for each unique fingerprint. Our machine alerts if the same person tries to vote increasingly than a time.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.194 |

||Volume 8, Issue 4, April 2020||

ADVANTAGES OF THE PROPOSED MODEL

- It provides an endangerment to stave invalid votes.
- It reduces the polling time.
- Touch screen replacing the buttons which could be possible to a struck.
- Easy to siphon to polling part-way from the polling box.
- Reduce the number of staff at the voting center.
- It provides easy and well-judged counting without any troubles.

The Fingerprint Voting System (FVS). Since the under structure of any voting system is "One Person – One Vote", it stands to reason that must verify that a voter is whom they require to be and that they have not previously voted in this referendum at flipside site (to eliminate double voting). The main purpose of the fingerprint voting system is to 'Preventing Fraudulent Voting'. This system has 5 types of modules. They are

- Fingerprint Enrolment
- Fingerprint Verification
- Cast the Votes
- Alert for wrong voting
- Generate final report

Fingerprint voting elections midpoint that people can trust the results considering it allows for a process that is so auditable, transparent and secure. It moreover helps reduce human error. Fingerprint voting and electronic counting midpoint that people can get official referendum results within hours, instead of weeks. Again, this builds trust. Technology will be a useful way of improving voter education and registration, to increase engagement and voter turnout. It is very good at making voting increasingly accessible, meaning it's easier for disabled people to vote independently. One of the reasons this Fingerprint voting system has been complimented so highly is that it's designed virtually the idea that all parties, citizens and referendum commissions were worldly-wise to inspect the electoral process at every stage, including surpassing a referendum has plane begun. A voter can vote the candidate only once, the system will not indulge the candidate to vote for the second time. The number of candidates widow to the system by the admin will be automatically deleted without the completion of the election. People can't misuse their votes.This Fingerprint voting machine using Fingerprint is mainly an Arduino system that makes the things easy in the polling booths during the referendum time. The user, who wants to poll their vote, has to submit the identity proof at the counter at the polling booth. In the research project, the user now needs to siphon with their sufficient material and voter card. Voter card is nothing but Fingerprint which stores the details of the person like the name of the user, address, national identity card number, mobile number for contact, etc.When the referendum time polling booths power unit is turned on, the ballot unit displays its “welcome to voting” message on TFT indicating that the machine is ready and waits for voter input. The mode of operation depends on the writ given by the user from the pushbuttons.

FINGERPRINT ENROLMENT

The first-time voter saves their fingerprint in enrolment processing. If the enrolling mode writ is given, the controller waits for input and activates the scanner to winnow the fingerprint, displaying "Enroll a fingerprint!" on the TFT display. The candidate's fingerprint is scanned and convert image in the first time to place the finger. Then second time ask the voter to place the same finger and create a unique template and trammels its match with the first scan then two prints were matched store in given id. This unique id is stored in the Fingerprint module memory of the controller for future reference. Without all enrolments, the system is ready for vote cast.

FINGERPRINT VERIFICATION

Before the vote tossing voter has to trammels for validity to the voting. During this verification time ask voter "PLACE YOUR FINGER" without the voter's fingerprint scanned, it is compared with the fingerprints once enrolled in the memory. If it is matched, then the message "Cast your vote." will be displayed on TFT. If the fingerprint did not match with once saved memory the TFT exhibit a message "Did not match!" and not unreliable to vote to cast. If the voter once voted, in verification time the fingerprint matched and exhibit the message on TFT “YOU VOTED ALREADY!” and requite red light alert.

CAST THE VOTES

After the verification, the voter unreliable to voting, in the first sawed-off pressed within five buttons which goes to party select, if a voter selects a party then cannot select flipside party. Then pressed three buttons within flipside five

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.194 |

||Volume 8, Issue 4, April 2020||

buttons, it goes to which candidate select in that party. If the voter printing party selection sawed-off increasingly than one time and candidate selection sawed-off increasingly than three-time, produce the zestful message on TFT "No Access" and sawed-off pressed were not counted.

GENERATE FINAL REPORT

After finished vote tossing to find who the winner and which party is a win in the referendum and counting the voting from report sawed-off pressed. For the security problem, the system has reported a generate sawed-off inside the box. Its wangle only by admin. Without the referendum finished all data deleted from the machine without getting the backup.

HOW WE VALIDATE VOTERS?

- AADHAAR issued by UIDAI has all the biometric and residential information of all civilians.
- Extracting the residential details without the successful hallmark of biometrics.
- Verifying the polling station for the specified address.
- It allows the civilians to tint votes for his desired candidate.

Block Diagram

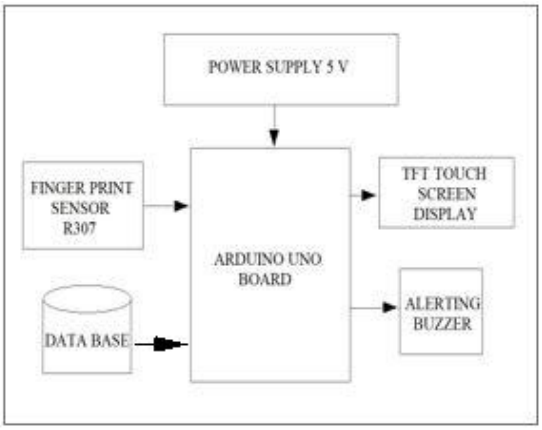

Fig.4: Block diagram of the proposed system

Algorithm of Fingerprint Voting System

Step 1: Start
Step 2: Scan your Fingerprint
Step 3: Fingerprint matched
Step 4: Exhibit candidate details randomly
Step 5: Tint vote
Step 6: Exhibit the voting details to voters.
Step 7: End

ARDUINO UNO

The Arduino Uno is a microcontroller workbench based on the ATmega328. It has 14 digital input/output pins, 6 analog inputs, a 16 MHz crystal oscillator, a USB port, a power slot, an ICSP header, and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB subscription or power it with AC-to-DC connector or shower to get started. The Arduino variegated from all previous boards in that it does not use the FTDI USB-to-serial suburbanite chip. Instead, it features the Atmega8U2 programmed as a USB-to-serial converter.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.194 |

||Volume 8, Issue 4, April 2020||

Fig.5: Arduino UNO R3

FINGERPRINT MODULE

The fingerprint module is an input device used for Fingerprint processing and captures a digital image of the fingerprint pattern. Fingerprint enrolment and fingerprint matching (the matching can be 1:1 or 1: N). When enrolling, the user needs to enter the finger two times. The system will process the two-time finger images, generate a template of the finger based on processing results and store the template. The captured image is tabbed a live scan. This live scan is digitally processed to create a biometric which is stored and used for matching. When matching, the user enters the finger on the optical sensor and the system will generate a template of the finger and compare it with templates of the finger library. For 1:1 matching, the system will compare the live finger specific template designated in the Module, for 1: N matching, or searching, the system will search the whole finger library for the matching finger. Many technologies have been used including optical, capacitive, RF, thermal. This is an overview of some of the increasingly wontedly used fingerprint sensor technologies.

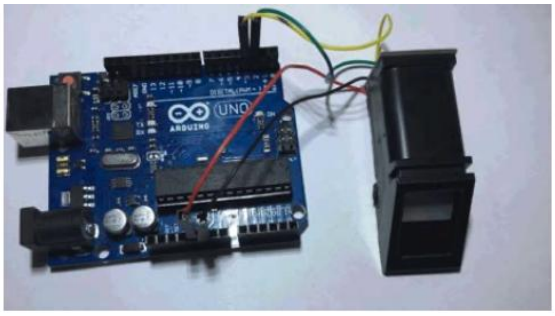

Fig.6: Fingerprint module TFT Display

A 2.4" TFT LCD module consists of an unexceptionable backlight (4 white LEDs) and a colorful 240X320 pixels display. A resistive touch screen comes pre-installed with the module as a bonus and hence you can hand snift your finger presses anywhere on the screen.

PIN Name	Description
GND	Power and signal ground pin.
Vin (3.5V)	Power pin that can be unfluctuating to 3-5VDC. It comes with reverse polarity protection.
Vout	The 3.3V output from the onboard regulator.
CLK	It is the SPI clock input pin.
MISO	This is the SPI Master in Slave Out pin which is mostly used by the SD card and for debugging TFT.
MOSO	This is the SPI Master Out Slave Out pin which is used to send data to the SD card or the TFT.
CS	SPI tweedle select pin.
D/C	SPI data or writ selector pin.
RST	The TFT comes with an auto-reset spin that gets zippy on every breakout. However, a user can

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.194 |

||Volume 8, Issue 4, April 2020||

	reset the module using this pin also, in specimen setup is not resetting clean.
Lite	It is the PWM input to tenancy the backlight. By default, it is pulled upper in which ways the backlight is ON. The PWM can be washed-up on any frequency and it can moreover be pulled lanugo to turn off the backlight.
IM3 IM2 IM1 IM0	These are the interface tenancy set pins. A user can unravel these out for wide use.
Card CS / CCS	SD card tweedled select pin is used to read from the SD card.
Card Detect/CD	The SD card detects pin is floating when the SD card is inserted and unfluctuating to Ground when there is no SD card.

VII.RESULTS& DISCUSSION

First enroll the voters' finger and save the fingerprint by given id.

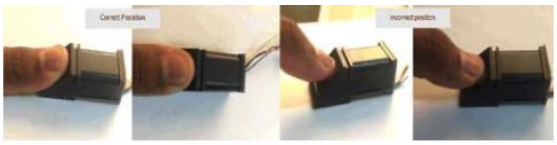

Fig.7: Place the fingerprint in fingerprint module

Fig.7 shows how to place finger on fingerprint module. The first two images were explained correct position and another two were wrong position of the fingerprint scanning.

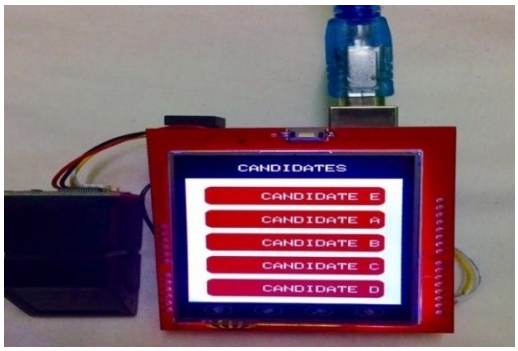

Fig.8:List of Candidates

After verification of voter the list of candidates is displayed on the TFT screen in any random order as shown in fig.The voter is now allowed to choose one of the candidates displayed.

Fig.9:Selected Candidate

Finally, the candidate selected by the voter is displayed on the TFT screen not more than 3 seconds as shown in fig.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.194 |

||Volume 8, Issue 4, April 2020||

VIII.CONCLUSION

In total, this system overcomes most of the problems faced during the voting period by the paper ballot system. The efficiency of this system depends upon the web interface, its usability. This will surely ensure a safer voting method which is very much what is required for the healthy growth of a developing nation.In this paper, the proposed Fingerprint-based voting system is better and faster than previous systems. The new system prevents access to illegal voters, provides ease of use, transparency and maintains the integrity of the voting process. The system also prevents multiple votes by the same person and checks eligibility of the voter. It also allows a person to vote from anywhere provided that the voter is within electoral limits.The fingerprint-based voting system has provided a chance to avoid invalid votes, It reduces the polling time, Easy to carrying to polling center from the polling box, Reduce the staff of the voting center, It provides easy and accurate counting without any troubles, Provisioning of voting preventive measures.

REFERENCES

1. Vishal Vilas Natu, 2014. Smart-Voting using Biometric “International Journal of Emerging Technology and Advanced Engineering, 4(6).
2. Khasawneh, M., M. Malkawi and O. Al-Jarrah, 2008. A Biometric-Secure e-Voting System for Election Process, Proceeding of the 5th International Symposium on Mechatronics and its Applications (ISMA08), Amman, Jordan.
3. Virendra Kumar Yadav, SaumyaBatham, Mradul Jain, Shivani Sharma, 2014. An Approach to Electronic Voting System using UIDAI, International Conference on Electronics and Communication Systems.
4. Chaum, D.L., 1981. Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms, Communications of the ACM, 24(2): 84-88.
5. Virendra Kumar Yadav, SaumyaBatham, Mradul Jain, Shivani Sharma, 2014. An Approach to Electronic Voting System using UIDAI, 2014 International Conference on Electronics and Communication Systems.
6. Ashok, Kumar D. and T. Ummal Begum, 2011. A Novel Design of Electronic Voting System Using Fingerprint.
7. Jefferson, D., A. Rubin, B. Simons, and D. Wagner, 2009. A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE), Technical Report, availableat http://www.servesecurityreport.org, last visited 2009.
8. Qijun Zhao, Lei Zhang, David Zhang, and Nan Luo, 2008. Adaptive Pore Model for Fingerprint Pore Extraction. Proc. IEEE, 978-1-4244- 2175-6/08.
9. Moheb R. Girgis, Tarek M. Mahmoud, and Tarek Abd-El-Hafeez, 2007. An Approach to Image Extraction and Accurate Skin Detection from Web Pages. World Academy of Science, Engineering, and Technology, pp: 27.
10. Manjeet Kaur, Mukhwinder Singh, AkshayGirdhar and Parvinder S. Sandhu, 2008. Fingerprint Verification System using Minutiae Extraction Technique. World Academy of Science, Engineering, and Technology, pp: 46.
11. Hoi Le and The Duy Bui, 2009. Online fingerprint identification with a fast and distortion tolerant hashing. Journal of Information Assurance and Security, 4: 117-123.
12. Mayank Vatsa, Richa Singh, AfzelNoore and Sanjay K. Singh, 2009. Combining pores and ridges with minutiae for improved fingerprint verification. Elsevier, Signal Processing, 89: 2676-2685.
13. UmutUludaga, Arun Rossb, Anil Jain, 2004. Biometric template selection and update: a case study in fingerprints. U. Uludag et al. / Pattern Recognition,, Elsavier? 37: 1533-1542.
14. Andrew Ackerman, 2002. Professor Rafail Ostrovsky “FINGERPRINT RECOGNITION”.
15. Secure fingerprint reader guide(Biometric System Based Electronic Voting Machine Using Arm9 Microcontroller- p- ISSN: 2278-8735, 10(1), Ver. II (Jan - Feb. 2015)).
16. Mahendheran, M., V.B. Ajith Rahavan, I. Vasu Devan, T.S. Kiruba Shankar, and S. Raja, 2016. Online Polling System to This Digital Era with Thumb Press and Image Capture, Middle-East Journal of Scientific Research, 24(3): 645-649.
17. Mohamed S. Sulaiman, M. Anto Bennet, A.A. Aravind, S.K. Rajvel and G. Janakiraman, 2016. A Design of E-Voting Using Fingerprint Recognition System for Secured Voting, Middle-East Journal of Scientific Research, 24(Techniques and Algorithms in Emerging Technologies): 385-390.