ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 3, March 2013

Biometrics using Electronic Voting System with Embedded Security

Alaguvel.R [1], Gnanavel.G [2],Jagadhambal.K [3]

[1]Department of Electrical and Electronics Engineering, V.R.S Engineering College &Technology, Arasur, Villupuram, Tamilnadu, India

[2] Assistant Professor ,Department of Electrical and Electronics Engineering, V.R.S Engineering College &Technology,Arasur ,Villupuram, Tamilnadu, India

[3]Department of Electrical and Electronics Engineering, V.R.S Engineering College &Technology, Arasur, Villupuram, Tamilnadu, India

Abstract-An electronic voting (e-voting) system is a voting system in which the election data is recorded, stored and processed primarily as digital information. There are two types of e-voting: On-Line and Offline. On-line, e.g. via Internet, and offline, by using a voting machine or an electronic polling booth. Authentication of Voters, Security of voting process, Securing voted data are the main challenge of e-voting. This is the reason why designing a secure e-voting system is very important. In many proposals, the security of the system relies mainly on the black box voting machine. But security of data, privacy of the voters and the accuracy of the vote are also main aspects that have to be taken into consideration while building secure e-voting system. In this project the authenticating voters and polling data security aspects for e-voting systems was discussed. It ensures that vote casting cannot be altered by unauthorized person. The voter authentication in online e-voting process can be done by formal registration through administrators and by entering One time password. In Offline e-voting process authentication can be done using Iris recognization, finger vein sensing which enables the electronic ballot reset for allowing voters to cast their votes. Also the voted data and voters details can be sent to the nearby Database Administration unit in a timely manner using GSM System with cryptography technique.

Keywords—,**Iris Recognization; Fingerprint; Offline e-voting; Online e-voting; Electronic Voting.**

I INTRODUCTION

As the modern communications and Internet, today are almost accessible electronically, the computer technology users, brings the increasing need for electronic services and their security. Usages of new technology in the voting process improve the elections in natural. This new technology refers to electronic voting systems where the election data is recorded, stored and processed primarily as digital information. In the past, usually, information security was used mostly in military and government institutions. But, now need for this type of security is growing in everyday usage. In computing, e-services and information security it is necessary to ensure that data, communications or documents (electronic or physical) are enough secure and privacy enabled. Advances in cryptographic techniques allow pretty good privacy on e-voting systems.

Security is a heart of e-voting process. Therefore the necessity of designing a secure e-voting system is very important. Usually, mechanisms that ensure the security and privacy of an election can be time-consuming, expensive for election administrators, and inconvenient for voters.

There are different levels of e-voting security. Therefore serious measures must be taken to keep it out of public domain. Also, security must be applied to hide votes from publicity. There is no measurement for acceptable security level, because the level depends on type of the information. An acceptable security level is always a compromise between usability and strength of security method.

The authenticating voters and polling data security aspects for e-voting systems are discussed here. It ensures that vote casting cannot be altered by unauthorized person. The voter authentication in online e-voting process can be done by formal registration through administrators and by entering OTPCertificate. In Offline e-voting process authentication can be done using facial recognization, fingerprint sensing and RFID (smart cards) which enables the electronic ballot reset for allowing voters to cast their votes. Also the voted data and voters details can be sent to the nearby Database Administration unit in a timely manner using GSM System with cryptography technique.

The criteria are Registration through Administrator, Voter identification and verification process is done through GSM with one time password. The second Offline e-voting process includes Facial Recognization; Fingerprint sensing, RFID and Polling data processing using Cryptography Technique with RC4 Algorithm. The final process concludes the analysis of polling data in real time and immediate resulting system of e-voting system.

II ELECTRONIC VOTING SYSTEMS

An electronic voting system is a voting system in which the election data is recorded, stored and processed primarily as digital information. E-voting is referred as “electronic voting” and defined as any voting process where an electronic means is used for votes casting and results counting. E-voting is an election system that allows a voter to record their ballots in a electrically secured method. A number of electronic voting systems are used in large applications like optical scanners

All Rights Reserved © 2013 IJARCET

which read manually marked ballots to entirely electronic touch screen voting systems. Specialized voting systems like DRE (direct recording electronic) voting systems, RFID, national IDs, the Internet, computer networks, and cellular systems are also used in voting processes.

A.Securities of the E-voting systems

The main goal of a secure e-voting is to ensure the privacy of the voters and accuracy of the votes. A secure e-voting system are satisfies the following requirements, *Eligibility*: only votes of legitimate voters shall be taken into account; *Unreusability*: each voter is allowed to cast one vote; *Anonymity*: votes are set secret; *Accuracy*: cast ballot cannot be altered. Therefore, it must not be possible to delete ballots nor to add ballots, once the election has been closed; *Fairness*: partial tabulation is impossible; *Vote and go*: once a voter has casted their vote, no further action prior to the end of the election; *Public verifiability*: anyone should be able to readily check the validity of the whole voting process.

B. Issues of Present Voting System

There have been several studies on using computer technologies to improve elections these studies caution against the risks of moving too quickly to adopt electronic voting system, because of the software engineering challenges, insider threats, network vulnerabilities, and the challenges of auditing. *Accuracy:* It is not possible for a vote to be altered eliminated the invalid vote cannot be counted from the finally tally .*Democracy:* It permits only eligible voters to vote and, it ensures that eligible voters vote only once. *Privacy:* Neither authority nor anyone else can link any ballot to the voter *verifiability:* Independently verification of that all votes have been counted correctly. *Resistance:* No electoral entity (any server participating in the election) or group of entities, running the election can work in a conspiracy to introduce votes or to prevent voters from voting. *Availability:* The system works properly as long as the poll stands and any voter can have access to it from the beginning to the end of the poll. *Resume Ability:* The system allows any voter to interrupt the voting process to resume it or restart it while the poll stands

The existing elections were done in traditional way, using ballot, ink and tallying the votes later. But the proposed system prevents the election from being accurate. Problems encountered during the usual elections are as follows:

- It requires human participation, in tallying the votes that makes the elections time consuming and prone to human error.
- The voter finds the event boring resulting to a small number of voters.
- Deceitful election mechanism.
- Constant spending funds for the elections staff are provided

So, the proposed electronic voting system has to be addressed with these problems.

C. Proposed system of online e-voting

The process of voter registration before the election process is always done by Administrator as follows the before. Registration phase begins by storing the Voter information such as Unique Voter ID (11-digit number TN/99/0000012—In this, TN specifies the State, Next two digit specifies District Id and third one specifies the Unique id for each eligible voter), Name, Age, Sex, Address and District in the database, polling questions answer and GSM one time password .this condition are stratification means person has valid the polling section.

III OFFLINE E-VOTING SYSTEMS

A. Fingerprint Recognition

Fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics usedto identify individuals

and verify their identity. A fingerprint looks at the patterns found on a fingertip. There are a variety of approaches to fingerprint verification. Some emulate the traditional police method of matching pattern; others use straight minutiae matching devices and still others are a bit more unique, including things like moiré fringe patterns and ultrasonic. A greater variety of fingerprint devices are available than for any other biometric. Fingerprint verification may be a good choice for in e-voting systems, where you can give users adequate explanation and training, and where the system operates in a controlled environment. It is not surprising that the work-station access application area seems to be based almost exclusively on fingerprints, due to the relatively low cost, small size, and ease of integration of fingerprint authentication devicesthat will be implemented is shown in Fig.1.

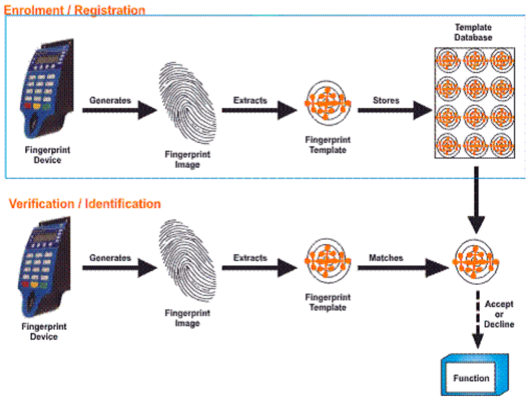


Fig. 1. Finger Print Enroiment and Verification

B. Facial recognition

Iris recognition systems have the same block diagram as any other biometric modality (see fig. 2). After capturing an image of the eye, the iris is located and segmented to extract its features; these features are then compared to a previously stored template .This section describes each of these blocks in detail, providing information on the approaches found in previous publications.

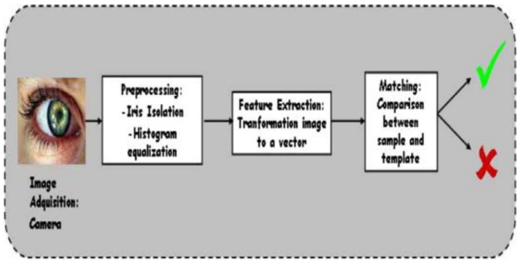

Preprocessing:
-Iris Isolation
-Histogram equalization
Feature Extraction: Tranformation image to a vector
Matching: Comparison between sample and template
✓
✗
Image Adquisition: Camera

Fig .2 Iris biometric systems

Two different strategies are followed in offline biometric authentication systems: 1) the token provides the biometric template and 2) the token performs the verification tasks and supplies the result, avoiding external access to the user's personal template. This paper recommends the second strategy for security and privacy motivations. Thus, different architecture approaches to build personal tokens will be described. These tokens are designed as tamper-proof devices, maintaining not only internal data security, but also a secure communications channel with the external world.

A. Iris Acquisition

Contrary to popular belief, iris biometrics systems do not use laser-scans to capture the image of the human eye. Instead, an infrared photo or video camera is used at a set distance to capture a high quality image of the iris. Working in the infrared range provides many advantages when compared to the visible range: iris ridges, nerves, and crypts are more evident the border between the iris and the pupil is more pronounced; and users are not exposed to annoying flashes. Currently, most of the work performed in this area has been dedicated to improving user-system interaction by developing cameras where the focusing system is automatic, such that users are not required to remain steady at a fixed point in front of the camera.

B. Iris Segmentation

The main purpose of this process is to locate the iris on theimage and isolate it from the rest of the eye image for furtherprocessing. Some other important tasks that are also performedin this iris segmentation block include image quality enhancement,noise reduction, and emphasis of the ridges of the iris.Several proposals have been made by different authors foriris location and segmentation, wherein most consider iris detectionas finding two circumferences that model the iris boundaries.Daugman has proposed an integro-differencial operator,which works by examining the difference in pixel levelsbetween circles drawn in the image. Sanchez-Avila have used a similar operator, but search for the maximum differencein lines drawn crossing the entire image. Other authors use the Hough transform for circle detection.Recently, Daugman has proposed a new method for seekingthe iris boundary by using active contour models Here, theiris location varies depending on preset external and internalforces until an equilibrium state is reached. Similar solutionshave also been used by Ritter and Ross.

C. Feature Extraction

In the feature extraction block, different authors have presented a wide variety of proposals. The majority of these begin with a normalization of the segmented iris image. This normalization becomes necessary when considering that the pupil varies in size for different light intensities. The normalization method varies from changes to the polar coordinate system, as Daugman proposed, to only considering a virtual line drawn around the pupil, known as the iris signature. After normalization, Daugman has studied the phase information by applying different Gabor filters. This was followed by the codification of this information in terms of the quadrant where the phase belongs however, Wildes, performs the extraction using Laplacian or Gaussian filters by obtaining several images of different scales for posterior comparison . Sanchez–Avila *et al.* have proposed in two different feature extraction approaches: one using Gabor filters weighting for small portions of the segmented iris image and another one based on the use of dyadic wavelet transformations and their zero-crossing representation. Li Ma have proposed a similar approach, but applies the dyadic wavelet transformation on a 1-D intensity signal instead of the iris signature approach used by Sanchez–Avila. Boles have also based their proposal on the dyadic wavelet transform, but on a normalized iris image (as proposed by Daugman), i.e., by using a 2-D wavelet transform on the polar scale representation of the iris, as opposed to the two previous algorithms that work in 1-D.

D. Matching

Although some authors have studied other matching algorithms the most employed matching algorithm has been the Hamming distance, as was initially proposed by Daugman . The Hamming distance is described by the following equation: where is the vector length and are the component of the template and sample vector, respectively, which are XOR in the equation. If the distance obtained is below a predefined threshold level, the studied sample is considered to belong to the user whose template is being studied. Selection of the threshold level usually depends on the final application.

All Rights Reserved © 2013 IJARCET

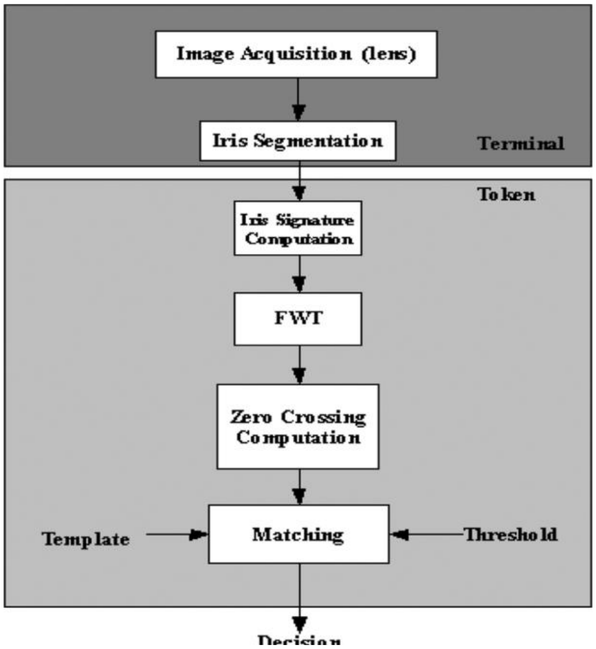


Fig.3.Terminal and platform functionalities.

C. Finger Vein

Finger vein has three hardware modules: image acquisition module, DSP main board, and human machine communication module. The structure diagram of the system is shown in Fig. 4. The image acquisition module is used to collect finger-vein images. The DSP main board including the DSP chip, memory (flash), and communication port is used to execute the finger-vein recognition algorithm and communicate with the peripheral device. The human machine communication module (LED or keyboard) is used to display recognition results and receive inputs from users.

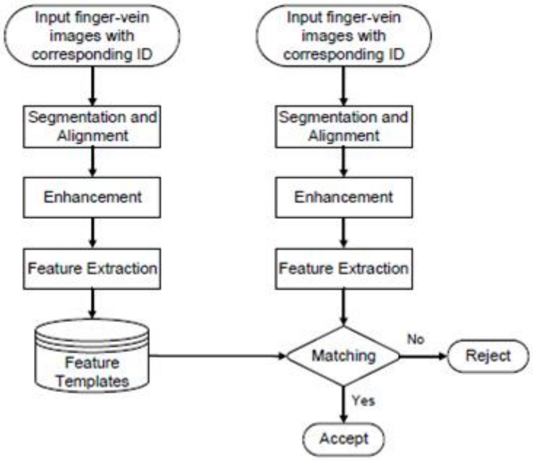

Input finger-vein images with corresponding ID
Segmentation and Alignment
Enhancement
Feature Extraction
Feature Templates
Input finger-vein images with corresponding ID
Segmentation and Alignment
Enhancement
Feature Extraction
Matching
No
Reject
Yes
Accept

Fig.4.The flow-chart of the proposed recognition algorithm

The proposed finger-vein recognition algorithm contains two stages: the enrollment stage and the verification stage. Both stages start with finger-vein image pre-processing, which includes detection of the region of interest (ROI), image segmentation, alignment, and enhancement. For the enrollment stage, after the pre-processing and the feature extraction step, the finger-vein template database is built. For the verification stage, the input finger-vein image is matched with the corresponding template after its features are extracted. Fig. 4 shows the flow chart of the proposed algorithm. Some different methods may have been proposed for finger-vein matching. Considering the computation complexity, efficiency, and practicability, however, we propose a novel method based on the fractal theory, which will be introduced in Section 4 in detail

A. Image acquisition

To obtain high quality near-infrared (NIR) images, a special device was developed for acquiring the images of the finger vein without being affected by ambient temperature. Generally, finger-vein patterns can be imaged based on the principles of light reflection or light transmission. We developed a finger-vein imaging device based on light transmission for more distinct imaging.

Our device mainly includes the following modules: a monochromatic camera of resolution 580 × 600 pixels, daylight cut-off filters (lights with the wavelength less than 800 nm are cut off), transparent acryl (thickness is 10 mm), and the NIR light source. The structure of this device is illustrated in Fig. 5. The transparent acryl serves as the platform for locating the finger and removing uneven illumination.

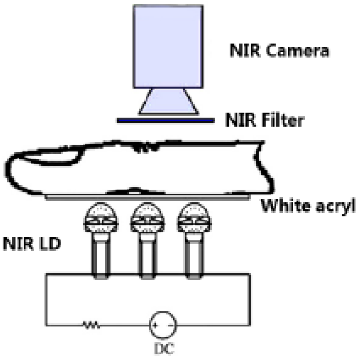


Fig.5.An example raw finger-vein image captured by our device

The NIR light irradiates the backside of the finger. In, a light-emitting diode (LED) was used as the illumination source for NIR light. With the LED illumination source, however, the shadow of the finger-vein obviously appears in the captured images. To address this problem, an NIR laser diode (LD) was used in our system. Compared with LED, LD has stronger permeability and higher power. In our device, the wavelength of LD is 808 nm. Fig. 6 shows an example raw finger-vein image captured by using our device.

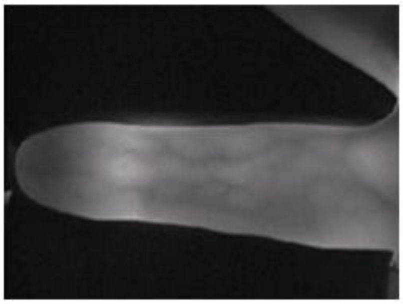


Fig.6. Illustration of the imaging device

All Rights Reserved © 2013 IJARCET

VOFFLINE E-VOTING PROCESSES

When the voter enters the voting place, he must have same kind of valid identity, which has been stored in the database for Verification. Authorized person choose to offline e-voting system. Thereare threeconditions for valid identity Verification to allow polling sectionsystem that will be implemented is shown in Figure 5

condition1: Capture the Iris image and compare or match to database, captured Iris image and database Iris image matched means that person will be valid for next condition otherwise exit the person.

Condition2: Capture the finger vein image and compare or match to database, capture finger vein and database finger veinmatched means this person will be valid for polling section and if two conditions are stratified automatically, E-voting machine buttons will be activate otherwise deactivate buttons.

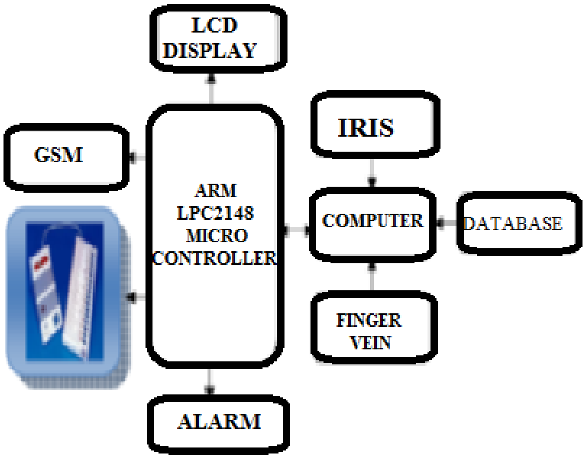


Fig.7. Offline E-Voting Block Diagram

VIONLINE E -VOTING PROCESS

When the voter enters the voting place, he must have same kind of valid identity, which has been stored in database verification, authorized person choose to online e-voting system. Two conditions are verified to allow polling section.

Condition1: When a poll worker confirms that the voter is registered, login the website ,type voter ID no and password correct means go to next state, answer to polling question ,this answer correct means go to next state finger print matched to database , matched means this person valid to next condition otherwise automatically closed web site.

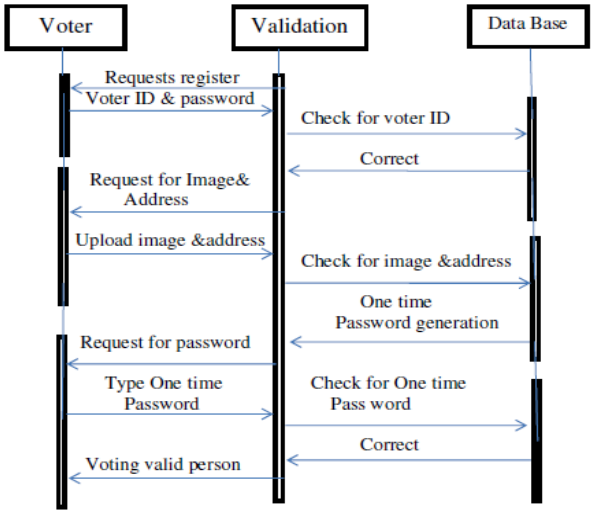


Fig.8 Authentication Sequence Diagram

Condition2: Randomly generated to one time password will be automatically sending through SMS to the authorized person’s mobile device using GSM. Then authorized person type to password, if password correct means open the polling window then entered**.**

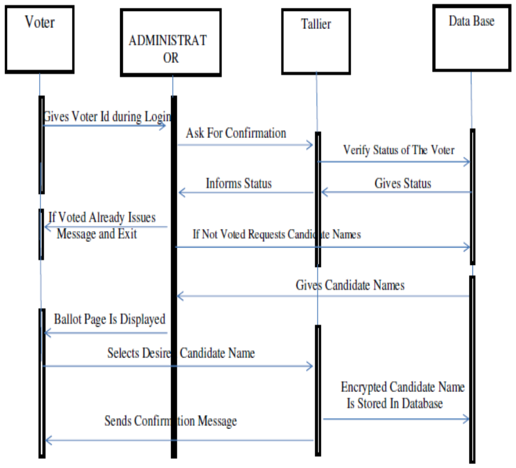
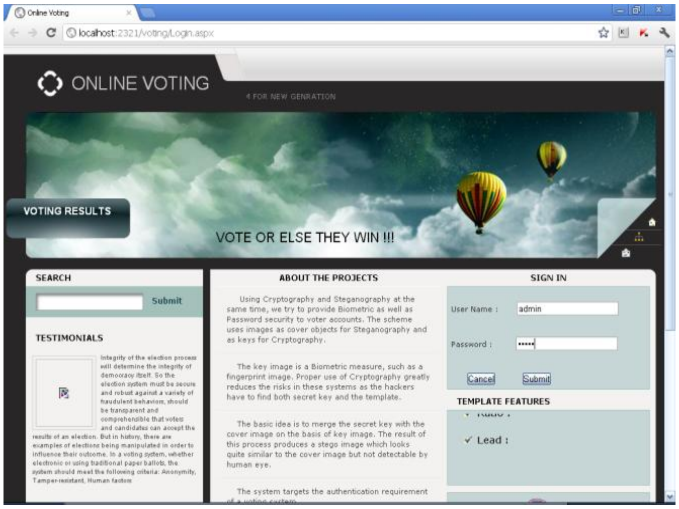

Voter
ADMINISTRATOR
Tallier
Data Base
Gives Voter Id during Login
Ask For Confirmation
Verify Status of The Voter
Informs Status
Gives Status
If Voted Already Issues Message and Exit
If Not Voted Requests Candidate Names
Gives Candidate Names
Ballot Page Is Displayed
Selects Desired Candidate Name
Encrypted Candidate Name Is Stored In Database
Sends Confirmation Message

Fig.9. Polling Sequence Diagram

VIISCREEN SHORT RESULT

All Rights Reserved © 2013 IJARCET



Integrity of the election process will determine the integrity of democracy itself. So the election system must be secure and robust against a variety of fraudulent behaviors, should be transparent and comprehensible that voters and candidates can accept the results of an election. But in history, there are examples of elections being manipulated in order to influence their outcome. In a voting system, whether electronic or using traditional paper ballots, the system should meet the following criteria: Anonymity, Tamper-resistant, Human factors

Using Cryptography and Steganography at the same time, we try to provide Biometric as well as Password security to voter accounts. The scheme uses images as cover objects for Steganography and as keys for Cryptography.

The key image is a Biometric measure, such as a fingerprint image. Proper use of Cryptography greatly reduces the risks in these systems as the hackers have to find both secret key and the template.

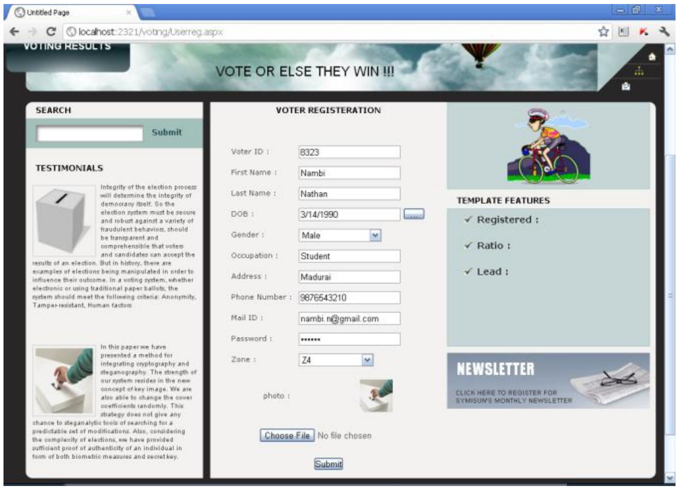
The basic idea is to merge the secret key with the cover image on the basis of key image. The result of this process produces a stego image which looks quite similar to the cover image but not detectable by human eye.

The system targets the authentication requirement of a voting system.

User Name : admin
Password : •••••

Cancel Submit

Fig.10 Admin Login

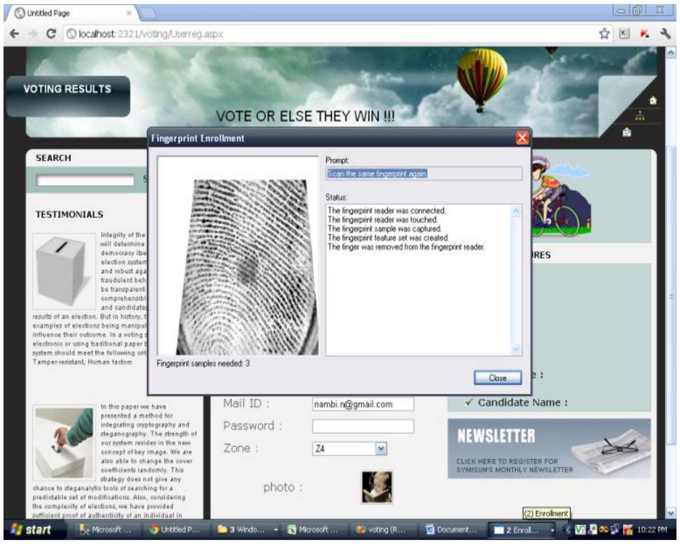


Integrity of the election process will determine the integrity of democracy itself. So the election system must be secure and robust against a variety of fraudulent behaviors, should be transparent and comprehensible that voters and candidates can accept the results of an election. But in history, there are examples of elections being manipulated in order to influence their outcome. In a voting system, whether electronic or using traditional paper ballots, the system should meet the following criteria: Anonymity, Tamper-resistant, Human factors

In this paper we have presented a method for integrating cryptography and steganography. The strength of our system resides in the new concept of key image. We are also able to change the cover coefficients randomly. This strategy does not give any chance to steganalytic tools of searching for a predictable set of modifications. Also, considering the complexity of elections, we have provided sufficient proof of authenticity of an individual in form of both biometric measures and secret key.

Voter ID : 8323
First Name : Nambi
Last Name : Nathan
DOB : 3/14/1990
Gender : Male
Occupation : Student
Address : Madurai
Phone Number : 9876543210
Mail ID : nambi.n@gmail.com
Password : ••••••
Zone : Z4
photo :
Choose File No file chosen
Submit

Fig.11Users Registration


Untitled Page
localhost:2321/voting/Userreg.aspx
VOTING RESULTS
VOTE OR ELSE THEY WIN !!!
SEARCH
TESTIMONIALS
✓ Candidate Name :
NEWSLETTER
CLICK HERE TO REGISTER FOR SYMISUN'S MONTHLY NEWSLETTER
start
10:22 PM

Fingerprint Enrollment

Prompt:
Scan the same fingerprint again

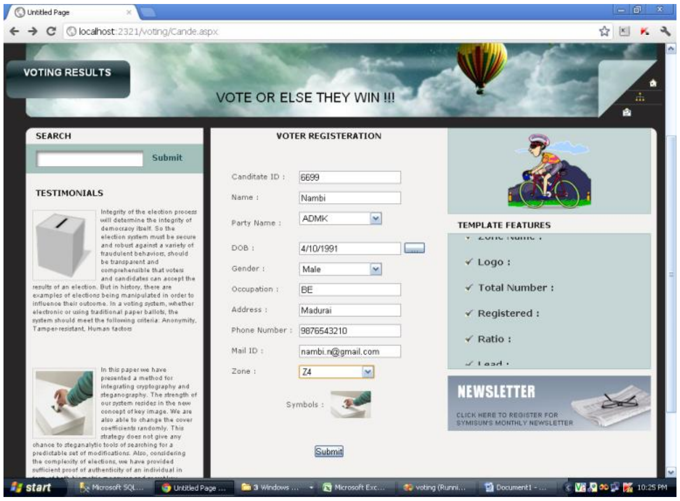
Status:
The fingerprint reader was connected.
The fingerprint reader was touched.
The fingerprint sample was captured.
The fingerprint feature set was created.
The finger was removed from the fingerprint reader.

Fingerprint samples needed: 3

Close

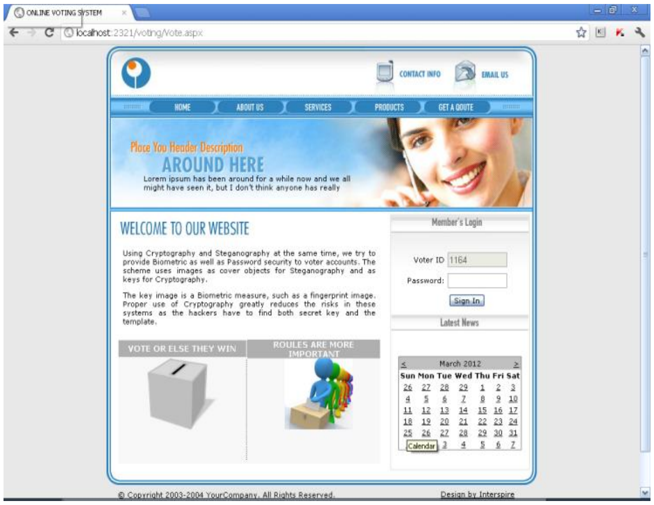
Mail ID : nambi.n@gmail.com
Password :
Zone : Z4
photo :

Fig.12 User Finger Print Enrollment



Canditate ID : 6699
Name : Nambi
Party Name : ADMK
DOB : 4/10/1991
Gender : Male
Occupation : BE
Address : Madurai
Phone Number : 9876543210
Mail ID : nambi.n@gmail.com
Zone : Z4
Symbols :
Submit

Fig.13 Voter Candidate Registration



Lorem ipsum has been around for a while now and we all might have seen it, but I don't think anyone has really

WELCOME TO OUR WEBSITE

Using Cryptography and Steganography at the same time, we try to provide Biometric as well as Password security to voter accounts. The scheme uses images as cover objects for Steganography and as keys for Cryptography.

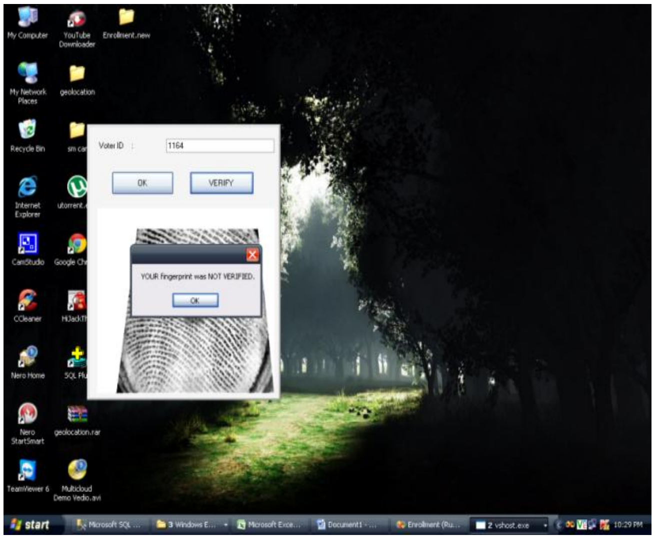
The key image is a Biometric measure, such as a fingerprint image. Proper use of Cryptography greatly reduces the risks in these systems as the hackers have to find both secret key and the template.

Member's Login
Voter ID 1164
Password:
Sign In

<			March 2012			>
Sun	Mon	Tue	Wed	Thu	Fri	Sat
26	27	28	29	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31
1	2	3	4	5	6	7

© Copyright 2003-2004 YourCompany. All Rights Reserved. Design by Interspire

Fig.14.User ID Verification



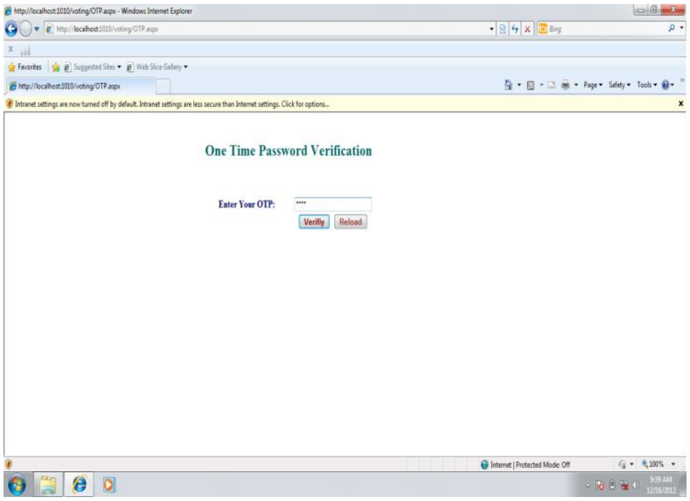
Voter ID : 1164

OK VERIFY

YOUR fingerprint was NOT VERIFIED.

OK

Fig.15. Finger Print Verification

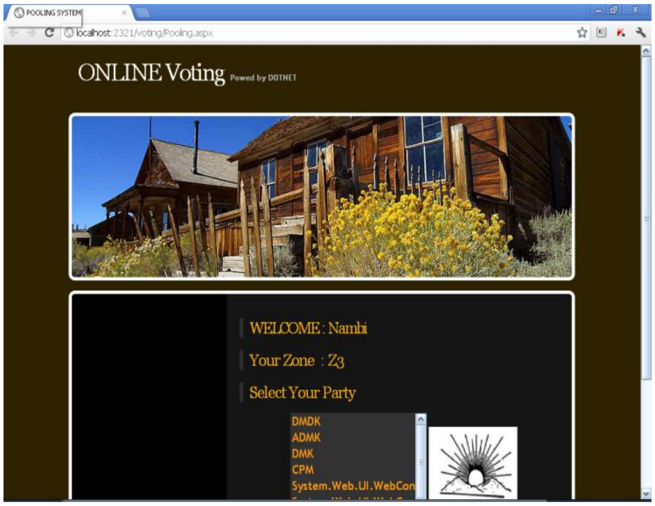


One Time Password Verification

Enter Your OTP: ****

http://localhost:1010/voting/OTP.aspx - Windows Internet Explorer
Verify
Reload
Internet | Protected Mode: Off
100%

Fig.16 One Time Password



ONLINE Voting Powered by DOTNET

WELCOME : Nambi

Your Zone : Z3

Select Your Party

DMDK
ADMK
DMK
CPM
System.Web.UI.WebCon

Fig.17 Online E-Voting Page

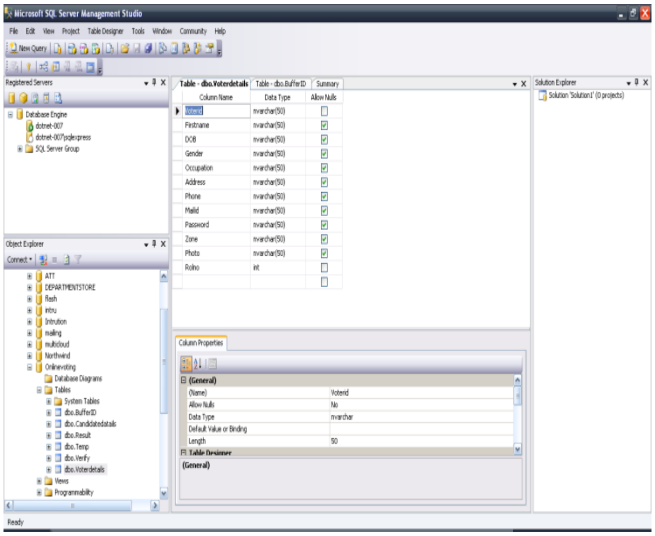


Table - dbo.Voterdetails | Table - dbo.BufferID | Summary

	Column Name	Data Type	Allow Nulls
▶	Voterid	nvarchar(50)	□
	Firstname	nvarchar(50)	☑
	DOB	nvarchar(50)	☑
	Gender	nvarchar(50)	☑
	Occupation	nvarchar(50)	☑
	Address	nvarchar(50)	☑
	Phone	nvarchar(50)	☑
	Mailid	nvarchar(50)	☑
	Password	nvarchar(50)	☑
	Zone	nvarchar(50)	☑
	Photo	nvarchar(50)	☑
	Rolno	int	□
			□

Column Properties

(General)	
(Name)	Voterid
Allow Nulls	No
Data Type	nvarchar
Default Value or Binding	
Length	50

Fig.18 SQL Database User Tables

VIII CONCLUSION AND FUTURE ENHANCEMENT

Electronic voting systems have many advantages over the traditional way of voting. Some of these advantages are lesser cost, faster tabulation of results, improved accessibility, greater accuracy, and lower risk of human and mechanical errors. It is very difficult to design ideal e-voting system which can allow security and privacy on the high level with no compromise. Future enhancements focused to design a system which can be easy to use and will provide security and privacy of votes on acceptable level by concentrating the authentication and processing section .In case of online e-voting some authentication parameters like facial recognization, In case of offline e-voting some authentication parameters like, Finger Vein and iris matching detection can be done.

ACKNOWLEDGEMENT

We are very much grateful to **GNANAVEL.G** for whom nothing is impossible in this world & we are very much thankful that he gave opportunity to complete this work in time to us. We would also like to be very much grateful to worthy Mrs.VijayaMuthuvannan, *chairperson*, Mr.N.Muthuvannan, *director*, Mr.R.Ramanathan, *Secretary*, Er.M.Saravanan, *C.E.O*, Dr.A.Anbalagan, *Principal*, Prof.A.Subramanian Head of the EEE Department , V.R.S.College of Engineering & Technology.

REFERENCES

[1].Tai-Pang Wu, , Sai-Kit, Yeung,JiayaJia, Chi-Keung Tang, AndGe´ RardMedioni Closed-Form Solution To Tensor Voting:Theory And ApplicationsTransactions On Pattern Analysis And Machine Intelligence, *Vol. 34, No. 8, August 2012*

[2].Scott Wolchok, Eric Wustrow, Dawn Isabel, and J. Alex Halderman Attacking the Washington, D.C. Internet Voting System In Proc. *16th Conference on Financial Cryptography & Data Security, Feb. 2012*

[3].Jossy P. George Saleem S TevaramaniAnd K B RajaPerformance Comparison Of Face Recognition Using Transform Domain Techniques World *Of Computer Science And Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 2, No. 3, 82-89, 2012*

[4].D. Ashok Kumar, T. UmmalSariba Begum A Novel design of Electronic Voting System Using Fingerprint *International Journal Of Innovative Technology & Creative Engineering (Issn: 2045-8711) Vol.1 No.1 January 2011*

[5].HongkaiXiong, Yang Xu,Yuan F. Zheng Wen Chen, *Fellow,* With Tensor Voting Projected Structure In Video Compression *Ieee Transactions On Circuits And Systems For Video Technology, Vol. 21, No. 8, August 2011*

[6].KashifHussainMemon, Dileep Kumar and Syed Muhammad Usman,Next Generation A Secure E-Voting System Based On Biometric Fingerprint Method *2011 International Conference On Information And Intelligent ComputingIPCSIT Vol.18 (2011)*

[7].ShivendraKatiyar, Kullai Reddy Meka, Ferdous A. Barbhuiya, Sukumar Nandi Online Voting System Powered By Biometric Security Using Steganography*International Conference On Emerging Applications Of Information Technology 2011*

[8]. KalaichelviVisvalingam, R. M. ChandrasekaranSecured Electronic Voting Protocol Using Biometric Authentication *Advances In Internet Of Things*, 2011 *Received June* 16, 2011; *Revised July* 5, 2011; *Accepted July* 11, 2011

[9].Feras A. Haziemeh, mutazKh. Khazaaleh, Khairall M. Al-Talafha New Applied E-Voting System *Journal Of Theoretical And Applied Information 31st March 2011*

[10].Hari K. Prasad_ J. Alex HaldermanyRopGonggrijp Scott Wolchoky Eric WustrowyArunKankipati_ Sai Krishna Sakhamuri_ VasavyaYagati_

_Netindia, Security Analysis Of India's Electronic Voting Machines *Hyderabad Y The University Of Michigan April 29, 2010*

[11].DavideBalzarotti, Greg Banks, Marco Cova, ViktoriaFelmetsger, Richard A. Kemmerer, William Robertson,
Fredrik Valeur, And Giovanni Vigna, An Experience In Testing The Security Of Real-World Electronic Voting Systems *Ieee Transactions On Software Engineering, Vol. 36, No. 4, July/August 2010*

[12].KshitijShinghal Dr. Arti Noor Dr. NeelamSrivastava Dr. RaghuvirWireless Sensor Networks InAgriculture: For Potato
Farming Singh International*JournalOf Engineering Science And Technologic Vol. 2(8), 2010,*

[13].Barbara OndrisekE-Voting System Security OptimizationProceedings of The42nd Hawaii International Conference on *System Sciences – 2009*

[14].Hari K. Prasad ArunKankipatiSai Krishna SakhamuriVasavyaYagatiNetindia, Security Analysis of India's Electronic Voting Machines *Scott Wolchok Eric Wustrow J. Alex HaldermanThe University of Michigan Hyderabad*

[15].HristinaMihajloska, VesnaDimitrova and LjupchoAntovski Security Aspects of Electronic Voting Systems *Cyril and Methodius UniversityFaculty of Natural Sciences and InformaticsInstitute of Informatics, Skopje, Macedonia*

[16].Xuejun Tan∗, BirBhanu Fingerprint matching by genetic algorithms *Center for Research in Intelligent System, University of California, Riverside, CA 92521, USA Received 24 February 2004; accepted 6 September 2005*

[17].Bernd Heisele,a,b, Purdy Ho,c Jane Wu,b and TomasoPoggiobFace recognition: component-based versus global approaches*Received 15 February 2002; accepted 11 February 2003*

Mr. ALAGUVEL.R, Receivedhis B.E(ECE) degree from V.R.S College of Engineering and Technology, Anna University in April 2010, has a Company experience of 1 years as a Network Engineer in Arshan Systech Pvt. Ltd., Chennai and currently pursuing his M.E (Embedded System Technologies) degree from V.R.S College of Engineering and Technology, Anna University. His areas of interest are Embedded Systems and VLSI.He presented papers in various conferences and Workshop's.

Mr. GNANAVEL.G, Received hisB.E (EEE) degree from Sri Jayaram Engineering College, Anna University in 2007, and also received his M.E (Embedded System Technologies) degree from SRM University in 2011. Now he is working as an Assistant Professor in the Department of EEE in V.R.S College of Engineering and Technology, has a teaching experience of 7 Years. His areas of interest are Embedded Systems, Power Electronics. He presented papers in various conferences and Workshop's.

Ms. Jagadhambal.K, Receivedhis B.E(ECE) degree from V.R.S College of Engineering and Technology, Anna University in April 2010, and currently pursuing his M.E (Embedded System Technologies) degree from V.R.S College of Engineering and Technology, Anna University. His areas of interest are Embedded Systems, VLSI and Cryptography. He presented papers in various conferences and Workshop's.