CONVENIENT VOTING MACHINE

Chinna V Gowdar[1], Palle Jeevan Kumar[2], Akash Reddy.R.S[3], Santosh Kumar.K[4], Sameena[5]

[1]Asst.Proffesor, Dept of ECE, R.Y.M Engineering College, Bellary, Karnataka, India
[2]Student (BE 8TH SEM), Dept of ECE, R.Y.M Engineering College, Bellary, Karnataka, India
[3]Student (BE 8TH SEM), Dept of ECE, R.Y.M Engineering College, Bellary, Karnataka, India
[4]Student (BE 8TH SEM), Dept of ECE, R.Y.M Engineering College, Bellary, Karnataka, India
[5]Student (BE 8TH SEM), Dept of ECE, R.Y.M Engineering College, Bellary, Karnataka, India

Abstract

An electronic voting (e-voting) system is a polling system in which the election statistics is recorded, stored and processed mainly as numerical 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 voting booth. Verification of Voters, Safety of voting process, Locking voted data are the chief challenge of e-voting. This is the reason why planning a secure e-voting system is very important. In many presentations, the safety of the system depends mainly on the black box voting device. But security of data, confidentiality of the voters and the exactness of the vote are also main features that have to be taken into observation while building secure e-voting system. In this project the authenticating voters and voting data security aspects for e-voting systems was chatted. It guarantees that vote casting cannot be altered by unofficial person. The voter verification in online e-voting process can be done by official registration through supervisors and by entering one time password. In Offline e-voting process confirmation can be done using finger vein identifying which permits the electronic ballot retuned for allowing voters to cast their votes. Also the voted data and voter's statistics can be sent to the nearby Database Supervision unit in a timely custom using GSM System based on .NET with cryptography technique.

***Keywords**: Fingerprint; .NET; Offline e-voting; Online e-voting; Electronic voting.*

---***---

1. INTRODUCTION

As the current communications and Internet, today are almost accessible electronically, the computer technology customers, brings the amassed need for electronic services and their safety. Usages of new technology in the voting process develop the elections in normal. This new technology refers to electronic voting systems where the election statistics is recorded, stored and processed mainly as digital statistics. In the earlier, usually, information security was used generally in military and government institutions. But, now necessity for this type of security is growing in daily usage. In computing, eservices and information security it is necessary to confirm that data, communications or official papers (electronic or physical) are sufficient protected and privacy enabled. Advances in cryptographic techniques allow appealing good privacy on e-voting systems.

Security is a heart of e-voting process. Therefore the requirement of scheming a secure e-voting system is real important. Usually, mechanisms that certify the security and confidentiality of an election can be slow, costly for election supervisors, and problematic for voters.

There are different levels of e-voting security. Therefore thoughtful methods must be taken to keep it out of public dominion. Also, security must be realistic to skin votes from publicity. There is no measurement for satisfactory security level, because the levelrely on type of the data. An satisfactory security level is always a negotiation between usability and strength of security method.

The authenticating voters and voting data security aspects for e-voting systems are discussed here. It ensures that vote casting cannot be altered by unofficial person. The voter authentication in online e-voting process can be done by formal registration through administrators and by entering OTP Certificate. In Offline e-voting process verification can be done using fingerprint sensing and RFID (smart cards) which permits the electronic ballot rearrange for permitting voters to cast their votes. Also the voted data and voters details can be sent to the nearby Database Supervision unit in a timely manner using GSM System with cryptography technique.

The criteria are Registration through Supervisor, Voter identification and verification process is completed through GSM with one time password. The second Offline e-voting process includes Fingerprint sensing, RFID and Voting data processing using Cryptography Technique with RC4 Algorithm. The final process defines the analysis of voting data in real time and immediate resulting system of e-voting system.

2. ELECTRONIC VOTING SYSTEMS

An electronic voting system is a polling system in which the election statistics is recorded, stored and processed mainly as digital information. E-voting is chatted as “electronic voting” and distinct as any voting modeling process where an electronic means is cast-off for votes and results counting. E-voting is an election system that license’s a voter to record their ballots in a electrically secured system. A number of electronic voting systems are used in huge applications like optical scanners which read manually marked ballots to exclusively electronic touch screen voting systems. Expert voting systems like DRE (direct recording electronic) voting systems, RFID, national IDs, the Internet, computer networks, and cellular structures are also used in voting processes [1].

2.1 Securities of the e-voting Systems

The main goal of a secure e-voting is to confirm the privacy of the voters and correctness of the votes. A secure e-voting system are fulfils the following requirements, Eligibility: only votes of reasonable voters shall be taken into account; Unre-usability: each voter is allowed to cast one vote; Anonymity: votes are set secret; Exactness: cast ballot cannot be changed. Therefore, it must not be likely to delete ballots nor to add ballots, once the election has been closed; Fairness: incomplete tabulation is not possible; Vote and go: once a voter has casted their vote, no additional action preceding to the end of the election; Public verifiability: anyone should be able to freely check the cogency of the whole voting process.

2.2 Issues of Present Voting System

There have been several studies on using computer technologies to develop elections these studies attention against the threats of moving too speedily to approve electronic voting system, because of the software engineering tasks, insider extortions, network struggles, and the challenges of examining. Accuracy: It is not possible for a vote to be changed removed the invalid vote cannot be calculated from the finally tally .Democracy: It license’s only authorized voters to vote and, it confirms that qualified voters, vote only once. Privacy: Neither expert witness 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 playing a part in the election) or group of objects, running the election can work in a plan 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 permits any voter to disturb the voting process to resume it or restart it while the poll stands.

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

- It requires human contribution, in tallying the votes that makes the elections time intense and prone to human error.
- The voter finds the event boring resulting to a lesser number of voters.
- Deceiving election mechanism.
- Continuous spending funds for the elections staff are provided so, the suggested electronic voting system has to be addressed with these problems.

2.3 Proposed System of Online e-Voting

The process of voter registering before the election process is always done by Supervisor as follows the before. Registration phase begins by filling the Voter information such as Solitary Voter ID (11-digit number KA/99/0000012— In this, KA specifies the State, Next two digit specifies District Id and third one specifies the Unique id for each qualified voter), Name, Age, Sex, Address and District in the database, voting questions answer and GSM one time password. This condition is stratification means person has in force the voting unit.

3. OFFLINE E-VOTING SYSTEMS

3.1 Fingerprint Recognition

Fingerprint recognition or fingerprint verification refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics used to identify individuals and verify their identity. A fingerprint looks at the arrays found on a fingertip. There are a range of methods to fingerprint verification. Some match the old-style police method of matching form; others use straight details matching devices and still others are a bit more exclusive, including stuffs like moiré fringe patterns and ultrasonic. A greater variability of fingerprint devices are available than for any other biometric. Fingerprint verification may be a good optimum for in e-voting systems, where you can give users suitable explanation and teaching, and where the system functions in a organized environment. It is not amazing that the workstation entrance application area seems to be based almost completely on fingerprints, due to the pretty low cost, small size, and ease of blend of fingerprint confirmation devices that will be employed is shown in Fig.1 [2].

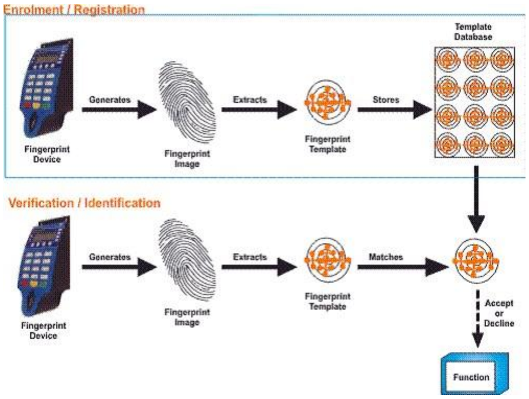


Fig -1: Finger Print Enrolment and Verification

proof devices, sustaining not only internal data security, but also a safe communications channel with the external world.

Finger vein has three hardware modules: image acquisition component, DSP main board, and human machine communication piece. The structure diagram of the system is shown in Fig. 4. The image acquisition module is used to save finger-vein pictures. The DSP main board containing the DSP chip, memory (flash), and communication port is used to implement the finger vein algorithm and communicate with the central device. The human machine communication element (LED) is used to display credit results and receive inputs from users.

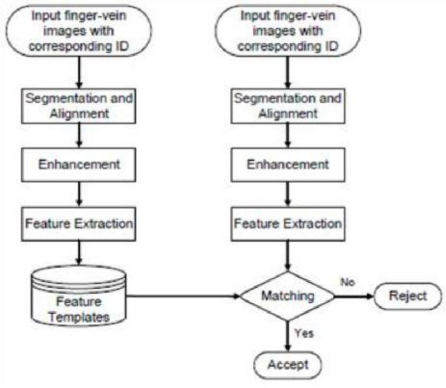

Input finger-vein images with corresponding ID
Segmentation and Alignment
Enhancement
Feature Extraction
Feature Templates
Input finger-vein images with corresponding ID
Segmentation and Alignment
Enhancement
Feature Extraction
Matching
No
Reject
Yes
Accept

Fig -2: The flow-chart of the suggested recognition algorithm

The suggested finger-vein recognition algorithm contains two stages: the enrollment stage and the authentication stage. Both stages start with finger-vein image pre-processing, which contains detection of the region of interest (ROI), image segmentation, arrangement, and enrichment. For the enrollment stage, after the pre-processing and the feature concept step, the finger-vein pattern database is built. For the authentication stage, the input finger-vein image is synchronized with the parallel template after its features are removed. Fig. 2 shows the flow chart of the suggested algorithm. Some different methods may have been suggested for finger-vein matching. Considering the computation difficulty, efficiency, and practicability, however, we suggest a novel method based on the fractal theory, which will be introduced in Section 4 in detail.

3.2 Image acquisition

To obtain high quality near-infrared (NIR) images, a special device was developed for attaining the images of the finger vein without being affected by ambient temperature. Generally, finger-vein patterns can be imaged based on the values of light reflection or light transmission. We developed a finger-vein imaging device centered 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 sifts (lights with the wavelength less than 800 nm are cut off), see-through acryl (thickness is 10 mm), and the NIR light source. The structure of this device is clarified in Fig. 3. The see-through acryl serves as the stage for locating the finger and removing uneven illumination [3].

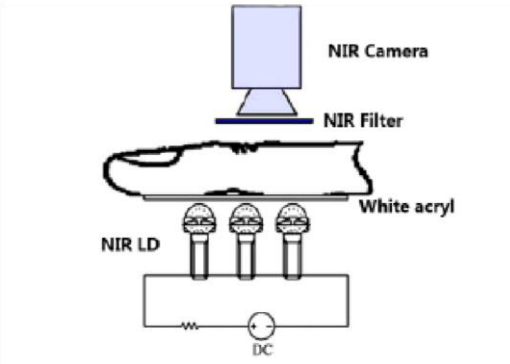


Fig -3: An example raw finger-vein copy taken by our device

The NIR light exposes the back side of the finger. In, a light-emitting diode (LED) was used as the explanation source for NIR light. With the LED clarification source, however, the shadow of the finger-vein perceptibly appears in the captured images. To address this problem, an NIR laser diode (LD) was used in our system. Co-ordinated with LED, LD has stronger penetrability and higher power. In our device, the wavelength of LD is 808 nm. Fig. 4 shows an example erratic finger-vein image captured by using our device.

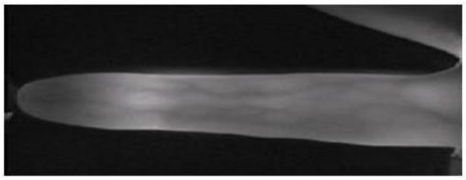


Fig-4: Illustration of the imaging device

4. OFFLINE E-VOTING PROCESSES

When the voter enters the voting place, he/she must have same kind of valid identity, which has been stowed in the database for Authentication. Certified person choose to offline e-voting system. There are three conditions for legal identity Verification to permit voting section system that will be executed is shown in Figure 5

Condition1: Capture the finger vein image and match to database, capture finger vein and database finger vein coordinated means this person will be valid for voting unit and if two conditions are stratified automatically, E-voting machine buttons will be activate or else deactivate buttons.

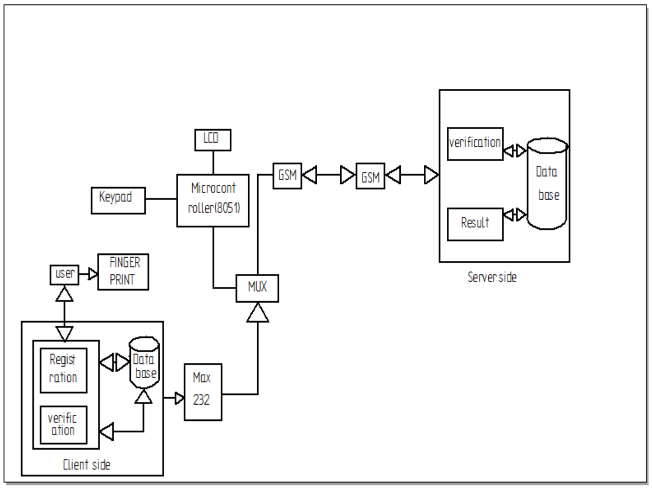


Fig -5: Offline E-Voting Block Diagram

5. ONLINE E -VOTING PROCESS

When the voter pass in the voting place, he must have same kind of valid identity, which has been stowed in database verification, approved person choose to online e-voting system. Two conditions are definite to allow voting section.

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

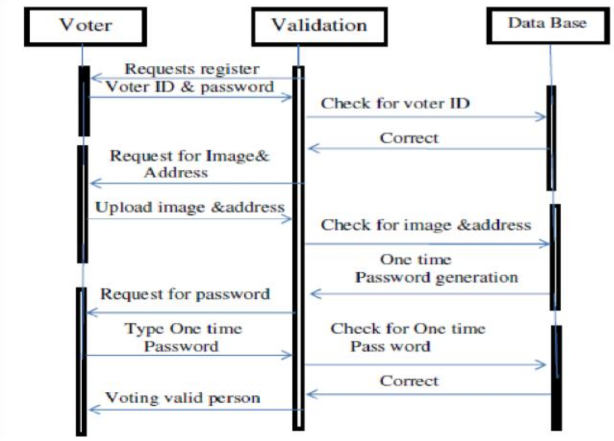


Fig -6: Authentication Sequence Diagram

Condition2: Arbitrarily generated to one time password will be impulsively sending through SMS to the approved person's mobile device using GSM. Then approved person type the password, if password correct means then he enters into the voting window [1].

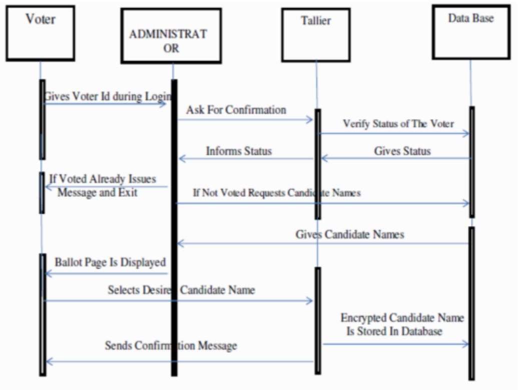
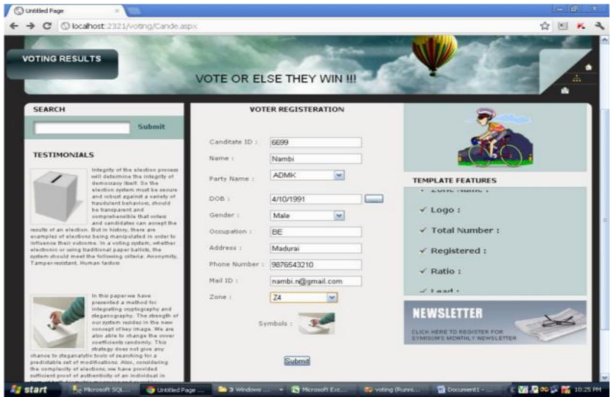

Voter
ADMINISTRATOR
Tallier
Data Base
Gives Voter Id during Login
Ask For Confirmation
Verify Status of The Voter
Informs Status
Gives Status
If Voted Already Issues Message and Exit
If Not Voted Requests Candidate Names
Gives Candidate Names
Ballot Page Is Displayed
Selects Desired Candidate Name
Encrypted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

Fig -7: Voting Sequence Diagram

6. SCREEN SHORT RESULT



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 behavior, 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

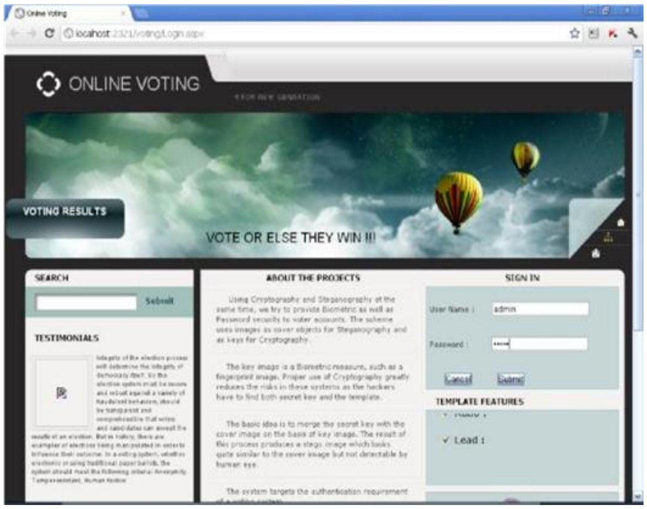
In this paper we have presented a method for integrating cryptography and steganography. The strength of our system resides in the new concept of key image. We are also able to change the cover coefficients randomly. This strategy does not give any chance to steganalytic tools of searching for a predictable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

VOTER REGISTERATION

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 -8: User registration



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 factor

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.

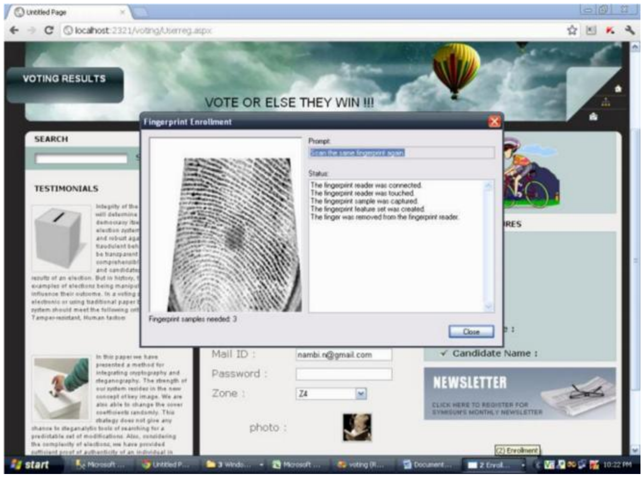
The basic idea is to merge the secret key with the cover image on the basis of key image. The result of this process produces a stego image which looks quite similar to the cover image but not detectable by human eye.

The system targets the authentication requirement of a voting system

User Name : admin

Password : *****

Fig -9: Admin login


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

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

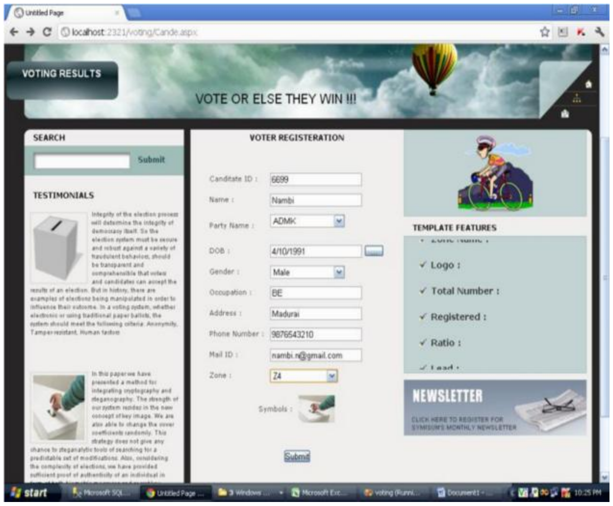
Mail ID : nambi.n@gmail.com

Password :

Zone : Z4

photo :

Fig -10: user finger print enrollment



VOTER REGISTERATION

Canditate ID : 6699

Name : Nambi

Party Name : ADMK

DOB : 4/10/1991

Gender : Male

Occupation : BE

Address : Madurai

Phone Number : 9876543210

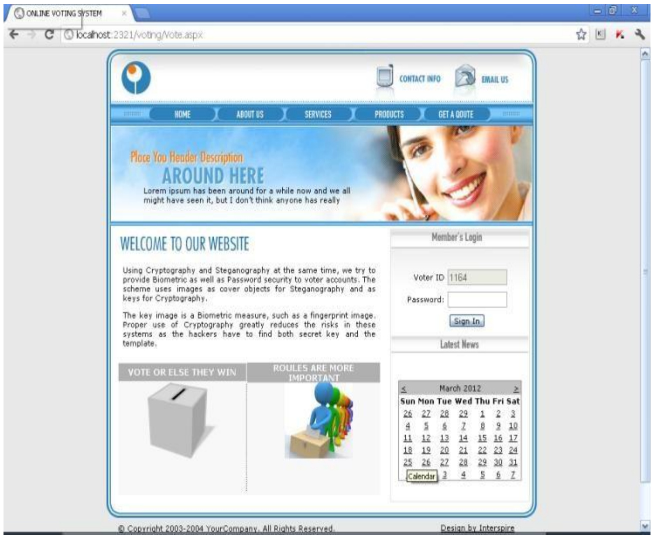
Mail ID : nambi.n@gmail.com

Zone : Z4

Symbols :

Submit

Fig -11: 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

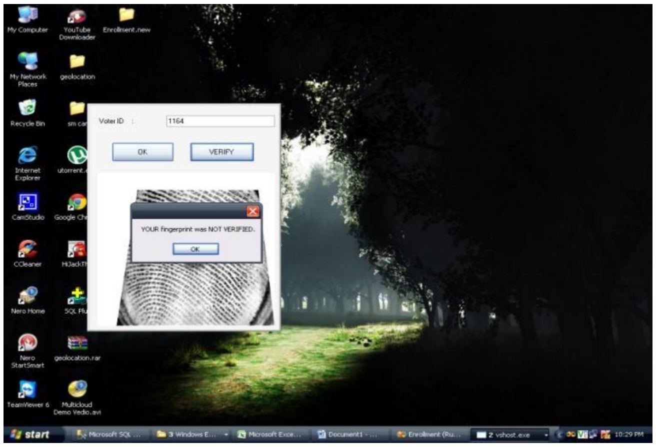
Password:

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 -12: user ID verification



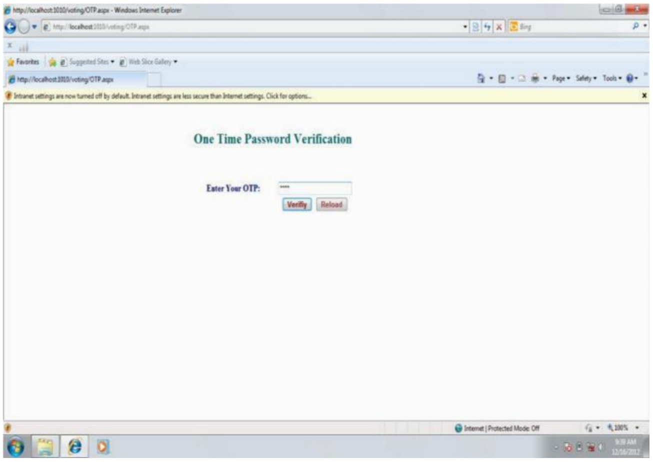
Voter ID : 1164

OK VERIFY

YOUR fingerprint was NOT VERIFIED.

OK

Fig 13: finger print verification

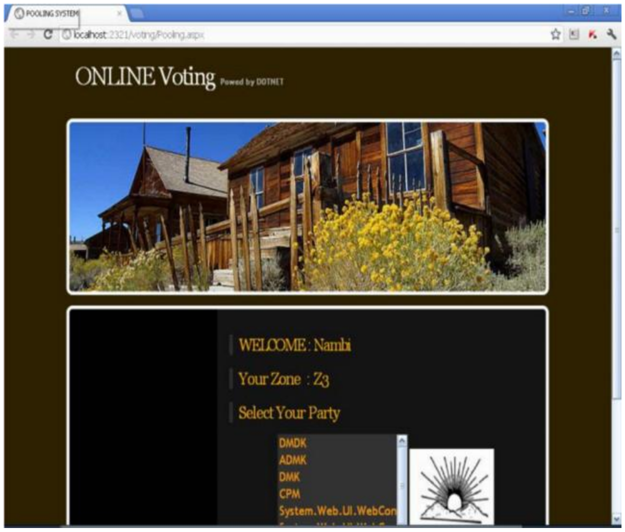

http://localhost:1010/voting/OTP.aspx - Windows Internet Explorer
Favorites
Suggested Sites
Web Slice Gallery
Page
Safety
Tools
Internet | Protected Mode: Off
100%

One Time Password Verification

Enter Your OTP: ****

Verify Reload

Fig 14: 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 15: online e-voting page

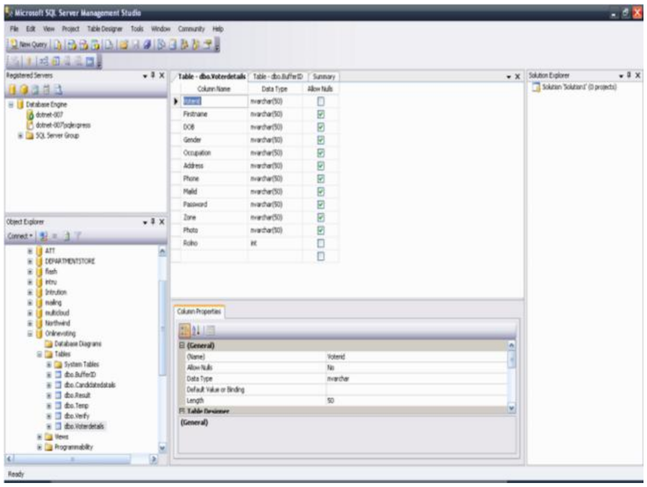


Table - dbo.Voterdetails

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)	☑
Rollno	int	□

Column Properties

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

Fig 16: SQL database user tables

7. CONCLUSIONS 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 satisfactory level by focused the verification and processing section .In case of online e-voting some verification parameters like facial recognition, In case of offline e-voting some verification constraints like, Finger Vein and iris matching detection can be done.

ACKNOWLEDGEMENTS

We are very much thankful to Mrs. Chinna V. Gowdar for whom nothing is challenging in this world & we are very much gratified that she gave chance to complete this work in time to us. We would also like to be very much gratifying to worthy Sri.Allum Gurubasavaraj, chief patrons, Sri.B.V.Basavaraj,chairpearson,Sri.H.M.GurusiddaSwamy,Secretary, Dr.T.Hanumantha Reddy, Principal, Dr.savita sonoli, Head of the ECE Department , R.Y.M. Engineering college.

REFERENCES

[1]. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)

[2]. 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

[3]. 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

[4]. 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

[5]. 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

[6]. 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

[7]. 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)

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

[9]. 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

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