A Secure Approach for Authenticated and Secure Online Voting System by Using Homo-Morphic Stegnography

Miss. Prerana Santosh Mali, Mr.Rahul Gaikwad
Department of Computer Engineering
Godavari College Of Engineering, Jalgaon

Abstract-- Many voters would appreciate the possibility of voting from anywhere election and voting well known things in modern days of democracy. Electronic online voting over the Internet would be much more profitable. The Secured online voting system is today's need. We proposed a new secured online voting system by using biometric and steganographic authentication. In proposed model, voter's system generated security Password is verified before the vote is accepted and encrypt vote is stored form in the main database of Election of India. The additional feature of the model is that privacy of casted vote is preserved using homomorphic encryption. Blind signature is used for providing the anonymous voting environment. In this model a person can also vote from outside of his/her allocated electorate or from his/her chosen location. In the proposed system, counting of votes will be done fast and correctly.

Keywords—Homomorphic encryption, blind signature, biometric security, steganography, Web Server, Digital Signature, Internet Voting.

I. INTRODUCTION

Now a day's election process plays a very important role in Indian government. The election is a process to select a perfect candidate for who will lead our nation. In a democracy, people choose there leader by giving their valuable vote. Recently used Indian voting system is an electronic voting system, In that system voter availability, is compulsory, is the drawback of electronic voting system. An online voting system is the solution for this drawback voter can be voting the candidate for everywhere from specified Election Day and date.

Provide security to the online voting system is an important issue in real life. This model proposed helps in achieving the authenticity, non-traceability of vote cast and security with privacy also being imposed. This is handled in the proposed system by combining bio-metric with homomorphic encryption.

Online voting system security is the main concern [2]. Online voting process maintains the strict privacy and uprightness of the vote cast and authentication before the voter is cast their votes. An online voting system authentication is the main problem, only approve someone can give their vote. A person can be authorizing by some methods that can be personal identification number (PIN), secrete message or user identity proof. All authenticated data can be collocated by the user. All authentications are verified by the main database then allow for that voter to vote for a candidate. Authentication is verified by biometric identification process and steganography.

II. LITERATURE SURVEY

1.Pashine, ninave and kelapure [3] proposed an android platform for the online voting system. This application provides a diversion of the long process also provide security to the voter and its voter comfort system voter no need to go polling booth easily vote for the applicant in hometown itself. And also provide the option of gesture recognition but authentication is the problem of the android platform.

In this application which is divided into three panels on the basis of its users as follows:

Admin Model: This panel will be specifically used by members of the election commission to administer all the electoral processes including registrations of candidates & voters, and monitor all other actions carried out by them.

Candidate Model: This panel will be specifically used by electoral candidates to interact with the election commission & voters which will help them to work efficiently not only before the election but also after the election if elected.

Voter Model: This panel will be specifically used by each individual voter who is eligible for casting his vote i. e. a person ageing 18 years or the above. These are the main users, for whom the application is developed.

2. Jambhulakar, chakole and pradhi [4] proposed a novel security for the online voting system by using multiple encryption schemes. Provide security for cast vote when it is submitted from voting poll to voting server. Multiple encryptions to pass up DOS attack. Security provides obedient as well as an active intruder. This system is to take a decision on certain issues. This

paper uses cryptography concepts to take Advantages of the digital signature. Encrypting the send forth vote to client server then send to voting server with the help of the net. After sending encrypted vote then server side decrypts the vote before counting.
On server side decryption of that vote is done before counting. We need two keys, for this reason, one for encryption on voter system, which should be freely known and the second key for decryption of encrypted vote before counting on the voting server, this key must be confidential. So, for this reason, we require a couple of asymmetric keys. To give safety from active interloper who can change or fiddle the casted vote when the vote is transferring from voter to voting server, we are using a digital signature. When a voter cast his/her vote after that he/she will digitally sign on that by using his/her own private digital signature, and send this to the voting server, on the voting server side that signature is checked by digital signature verifier of that voter which is publicly known. For this purpose each voter should have a private digital signature and a public digital signature verifier, for this, we are using a pair of asymmetric keys for each registered voter.

3. Himanshu Agarwal and G.N.Pandey [8] proposed aadhar id based online voting system for Indian election is proposed for the first time in this paper. The proposed model has a greater security in the sense that voter high-security password is confirmed before the vote is accepted in the main database of Election Commission of India. The additional feature of the model is that the voter can confirm if his/her vote has gone to correct candidate/party. In this model a person can also vote from outside of his/her allotted constituency or from his/her preferred location. In the proposed system the tallying of the votes will be done automatically, thus saving a huge time and enabling Election Commissioner of India to announce the result within a very short period.

This system is much secured and efficient than the traditional voting system. Manipulation of votes and delay of results can be avoided easily. A unique AADHAAR identity is the center point of our proposed model. It leads to the easier verification of both voters and candidates. This AADHAAR Identity number is unique for every citizen or voter of India. This AADHAAR Identity number has been introduced by the government of India and this also recognizes the constituency of the voter. But the registration of the voter should be completed only after the verification of all documents by the field officer. The field officer also verifies AADHAAR Identity Number from the main AADHAAR card database. After completing verification, the registration of the voter should be complete and the voter will get an auto-generated e-mail which has all these information of the voter with the system generated a password. The Voter can use this password for login and he/she can also change the system generated an old password. The voter can also set the verification keys to ensure security. There should be a restriction to use only virtual/on-screen keyboard to type the password or to change the password. The main purpose of using the virtual/on-screen keyboard is to stop capturing the password, if the voter changes his/her password from some public place.

4. Shridharan [1] Implemented a three models such as Authentication model, franchise excising model, distributed database and central server model. In authentication model voter with smart card and voter identification number and also gives the biometric information this all information is used in future election voting process. After verification and validation voting interface means candidate name and sign are displayed, this is verified by vote casting database, and then votes are counted and declared the result. In this system security and traceability also ensures to auditing the vote and voter information.

In such a system, the correctness burden on the voting terminal's code is significantly less as voters can see and verify a physical object that describes their vote and are allowed to vote in terminal only after their identity is proved. The voters, who cast multiple votes during the process of voting is ensured to be prevented. Also to ensure the maintenance of authenticity, any biometric identification of the voters could be used for accessing the terminal to cast their vote and restricting them to cast again. The process of online voting could be deployed with three phases - the voter registration online vote capturing and the instant online counting and result declaration.

III. PROPOSED IDEA

Proposed Architecture is the online voting system. In this system, there are three models.

i. Voter registration by Admin
ii. Voter Authentication by OTP verification
iii. Vote casting and recording
iv. Vote Counting

In voter registration server, the voter will be registered personal information and biometric information e.g. Thumb Impression. Only registered users are allowing to vote at the time of the election.

In the proposed system, the user does registration process first. Send all information to authentication server send password and ID to voter after he/she is login. If it is authenticated then allowing for voting after voter cast his/her vote and this vote is encrypted form stored in vote casting and recording server.

A. Voter registration by Admin

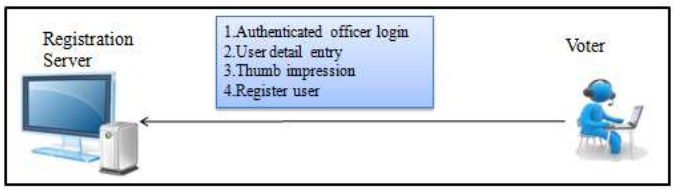


Fig. 3.1 Registration Module

1. Authenticated officer login in voter registration first login Election commission of India

2. After register voter detail information like Name, Age, and DOB...Etc.

3. Give voter finger print image. Each one has unique finger print. Finger print scanner is used to scan finger print.

4. All details are entered then register voter.

The election commission will update voter's details to database regularly. In registration module following steps are involved,

B. Authentication module by OTP Verification

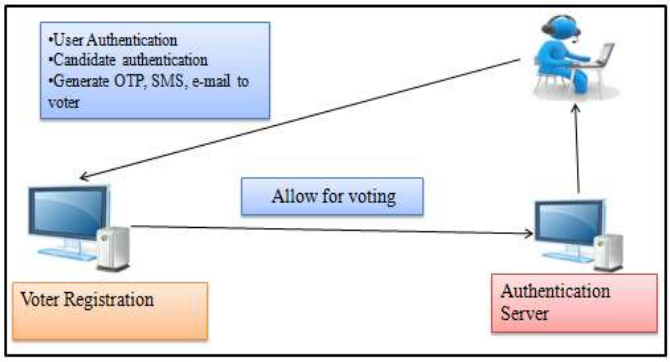


Fig.3.2 Authentication Module

In authentication server at the time of voter login to verify the voter is authenticated or unauthenticated using biometric security and steganography. Use finger print image and cover image generate stego image for authentication.

Embedding algorithm and authentication algorithm are used. To use biometric security and steganography both are used the same time to provide strong authentication. After authentication was completed then allow the voter for voting.

In Authentication module following steps are involved, after voter was registered after check authentication, voter is authenticated then,

1. After registration send all information to Authentication module.
2. Compare with database registration database and authentication database.
3. Then Generate OTP, SMS, Email to voter
4. Authentication is complete then allow for a voter to voting.

Our proposed work [7] is a mixture of steganography and biometric security. Uses the steganography is to various type of steganography like text, image, audio, video, in our work image is used to hide secret data. This image is used as a cover image they changing one or more bits of an image. System hides the message. In this system, steganography uses the image as a cover image. Using an image of steganogrphy is a better choice of all kind of data is hidden.

To work with system user should be.

- Personal identification number this is allocated to every user.
- Also every user thumb impression
- And at the time of account is opened secret key is given to every user which should hide from every single person.

All information is collected from every user the system will work as follows. All users has to sign the account with its personal identification number then user gives thumb impression, then ask secret key embedding it. Then authenticate the user that time ask the personal identification number.

a. Cover image

Every user has a 16 digit personal identification number this number is hidden automatically over base image base image is same for all users this image is predefine font and style image. This cover image is a simple inscription of personal identification number over base image.

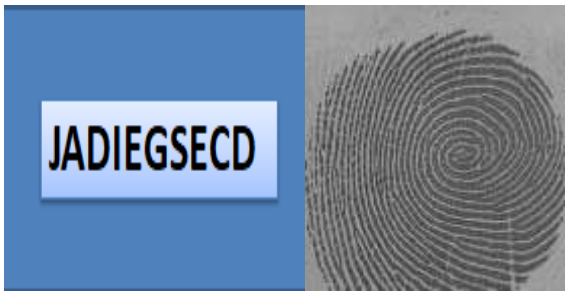


Figure 1.1

b. Secrete message

Using 16 bits secret key and time stamp value means current date value is 32 bits both are concatenated and apply SHA256. Use this algorithm because SHA256 is a secure hash algorithm its fix 236bit algorithm and solve complex mathematical problems so used SHA256. Then this hash code and time stamp value 32bits again concatenate and generate a secreted message.

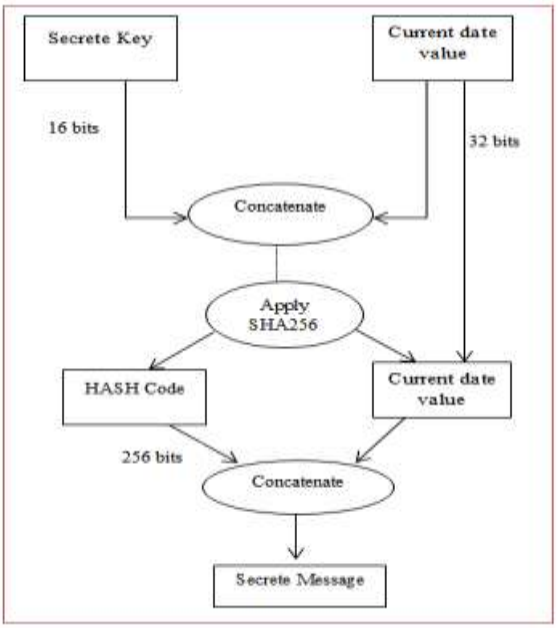


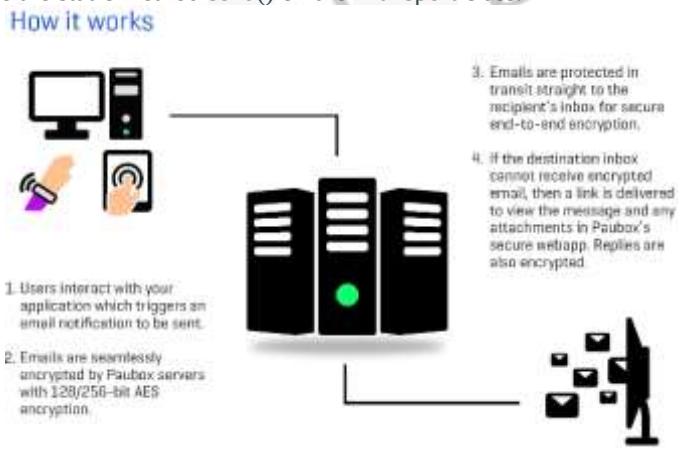
Figure 1.2

c. Autometic email sending

To send a message:

1. Create a message using a JavaMail Session object.
2. Create a MimeMessage object.
3. To set the message sender and recipient, use the InternetAddress class.
    a. Identify the sender by calling the setFrom() method on the MimeMessage object. Optionally, you can provide a personal name as a string in the second parameter.
    b. Identify the recipient by passing a recipient type and an address to the addRecipient() method. The recipient type can be Message.RecipientType.TO, Message.RecipientType.CC orMessage.RecipientType.BCC.

    The InternetAddress constructor raises an AddressException if the email address appears to be invalid.
4. To set a "reply to" address, use the setReplyTo() method.
5. Establish the contents of the message by calling methods on the MimeMessage object. Set the subject with setSubject() and set the plaintext body content with setText().
6. To send the message, use the static method send() on the Transport class.



d. Registration of valid Voter

Cover image, secret message and key image are used to generate stego image. Generated stego image is store in the database. The cover image has hidden 16 bits personal identification number and the key image has user thumb impression and generated a secreted message and generate stego image for each user.

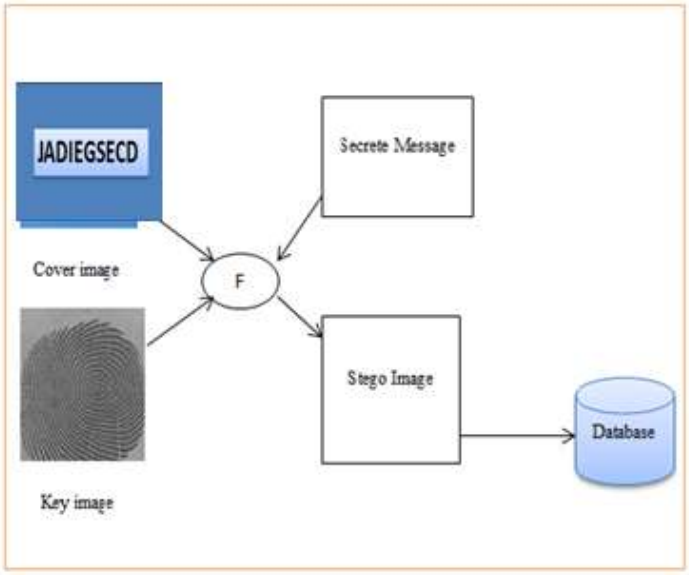


Figure 1.3

In figure 1.3 from the cryptography view, the key image will remain under-utilized as well. As the fingerprint image is also of the same size and dimension, we will be very fewer features of the key image. So, to increase the complexity of analysis, the 2-byte secret key is increased to 32-byte key by applying SHA 256 hashing algorithm. Now these 256 bits will become a part of the actual secret message. When the secret message is embedded in the cover image, its statistical properties will not same. The stego image will remain more complex to be analyzed because more features of the key image are utilized in this case. So, even if eavesdroppers know that this is a stego image, it would be more difficult for them to predict the embedded data.
By using Secured Email generation API algorithm automatically generate secret OTP and send to Voter's email if it is valid email then only and it generate message using secured message generation API which is govern by Government it send same OTP which is generated by algorithm and it send to same voter on their mobile number which voter register at the registration time for double verification of user.
If both OTP is same then only user validate otherwise user is unauthorized.

e. Authenticate The authorised Voter
In the authentication phase retrieved the stego image from database and key image. For authenticate the user in figure 1.4.

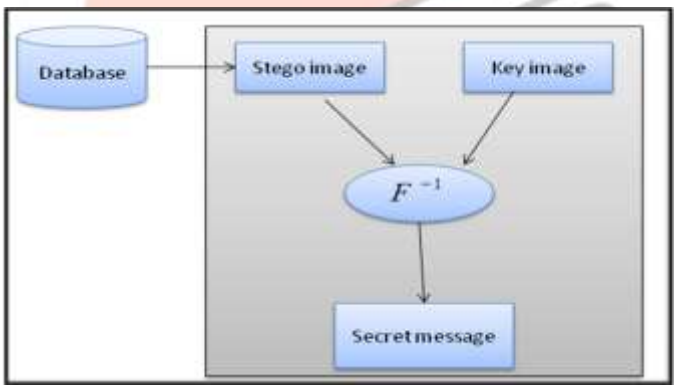
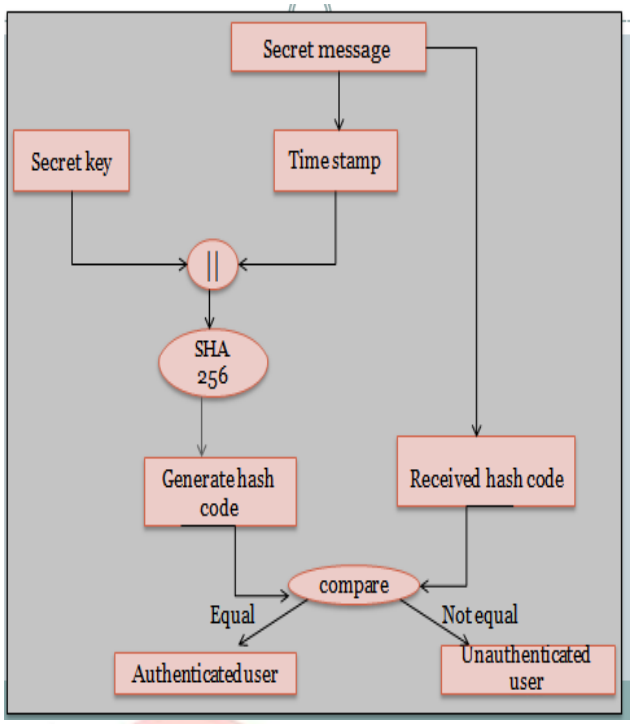


Figure 1.5

In figure 1.6 shows the authenticating user. In this phase, the key image is 256*256 pixels and the secreted message is 288 bits. In this 256bits secret message and 32 bits time stamp value. The timestamp
(E.g. Date) delivers the security from replay attacks so that the same stego image cannot be used again in future. This time stamp value and the secreted key are concatenated and apply SHA 256. This generated hash code and figure 1.2 retrieved hash code both hash code is compared if both are equal the person is authenticate does not equal then the person is not authenticated. But the actual secrete key is not embedded with stego image no chance of hacking secrete key.



f. Description Index generating algorithm

In index generating algorithm generate a unique index by using prime number, generator number, starting index generate the gen_ind[] array. Using following formula generate unique index array.

$$g^k \bmod p$$

g is the generator, k is starting index generator, p is a prime number.

The output of this algorithm is generating a unique index array, and inputs are a prime number, generator number, and index number. we have a need to 288 bits embed of secret message over cover image for encryption need to determine bytes of the cover image we are going to modify these are determined by index generator array[ ] of size 288 bits.

g. Authentication Algorithm

Personal identification number from stego image is read now correct entry in user database read the key image secret key o individual user key is a correct comparison with time stamp value 32 bit.

Using this secret key as a seed then we are generating ind_gen[ ] array of size 288. And setgo image array SI[ ] and also have key image array KI[ ] then we can extract secret message [ ] by applying authentication algorithm. In this algorithm verify the bytes of stego image and key image both are even or odd take secret message as one. Otherwise zero.

Input: SI[],KI[], ,Ind_gen[], SecretKey
Output: Authentic Person/ Not an Authentic Person
Begin
$SMsg[], Date[32], SecretKeyDate, j = 0$
for i=0 to 287 do
if SI[,Ind_gen[i]] and KI[,Ind_gen[i]] both either **even or odd then**
SMsg [i] = 0
else
SMsg [i] = 1
end
end
for i = 256 to 287 do
Date [j++] =SMsg [i]
end
$SecretKeyDate = Concatenate(SecretKey, Date)$
if $Compare(SMsg[], SHA256(SecretKeyDate)$ **then**
Return: Authentic Person
Else
Return: Not an Authentic Person
end
End

Using date value contained a secret message and secret key we can verify the person is authenticated or not authenticated.

C. Vote-recording and casting module

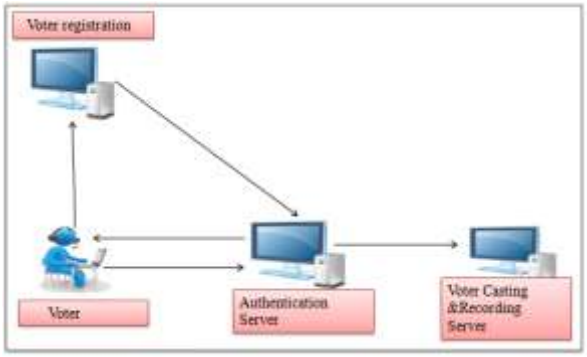


Fig.3.3 Voter Recording and Casting

In Vote, Recording and casting Module following steps are involved,
1. At the time of Election Day or date voter is Sign in.
2. after sign in voter to check authentication. Voter is authenticated then,
3. Select Candidate from ballot paper.
4. Cast their vote
5. Log out

If voter authenticated then the voter will allow for voting or if not authenticated then not allowed to vote. We use homomorphic encryption and blind signature algorithm. The homomorphic encryption algorithm is used to encrypt data, suppose there are five candidates. If voter presses button number 2, the signal will be generated and second bit will be set i.e. 0100. In the database this vote is not stored as it is in 0 and 1 form. It gets stored using homomorphic encryption. Blind signature is used to digitally authenticate a message without having knowledge of encrypted message content.

In voting to record and casting module separately stored vote and calculate candidate/party votes securely and immediately declared the results.

D. Vote Counting

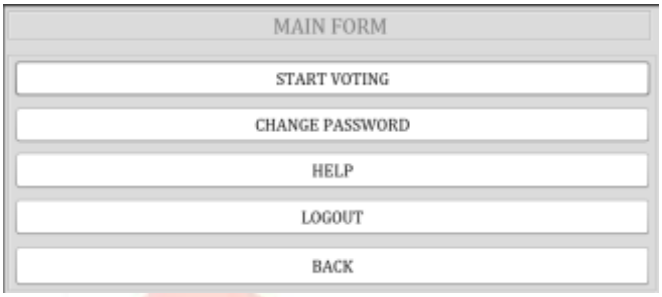
In counting votes, after that decryption algorithm of homomorphic decryption is applied to decrypt result. The system gives the accurate result, with the help of homomorphic encryption system overcome the problem of incorrect results. Results show high accuracy and high security of implemented system.

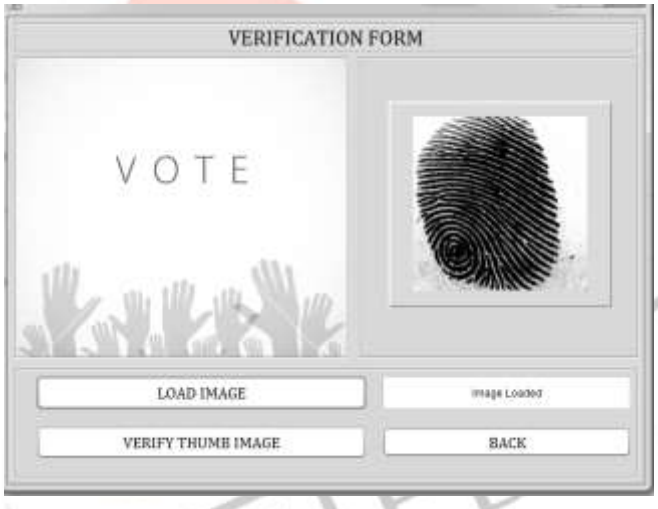
IV. EXPERIMENTAL RESULTS

The proposed algorithm new index generator array with the new index is generated. Avoid the repetition of pixels in this proposed algorithm.

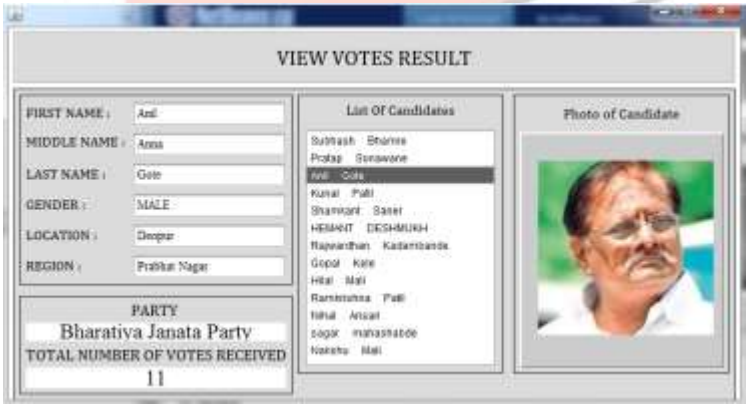
h. Results


LOGIN FORM
USER NAME
UIL8100701
PASSWORD
LOGIN
CLOSE


MAIN FORM
START VOTING
CHANGE PASSWORD
HELP
LOGOUT
BACK


VERIFICATION FORM
VOTE
LOAD IMAGE
VERIFY THUMB IMAGE
BACK


OTP VERIFICATION
ENTER OTP
LOAD IMAGE
SUBMIT
DE STEGNOGRAPH
BACK



V. CONCLUSION

The proposed secured online voting system uses biometric image and steganography for authentication. Homomorphic encryption is used for vote recording and counting. Blind signature is used for authenticating anonymous vote.

A system provides strong security for online voting. It is a reliable system for authentication, casting and recording anonymous vote. A proposed algorithm using homomorphic encryption gives correct results during vote counting phase.

REFERENCES

[1] Srivatsan Sridharan , " Implementation of Authenticated and Secured Online Voting System", 4th ICCCNT 2013, Tiruchengode, India No.6, July 2013. IEEE – 31661.

[2] Divya G Nair, Binu. V.P, G. Santhosh Kumar," An Improved E-voting scheme using Secret Sharing based Secured Multi-party Computation", arXiv: 1502.07469v1 [cs.CR] 26 Feb 2015

[3] Pranay R. Pashine, Dhiraj P. Ninave, Mahendra R. Kelapure, Sushil L. Raut, Rahul S. Rangari, Kamal O. Hajari," A Remotely Secured E-Voting and Social Governance System Using Android Platform", International Journal of Engineering Trends and Technology (IJETT) – Volume 9 Number 13 - Mar 2014

[4] Ms. Ashwini Walake, Prof. Ms. Pallavi Chavan," Efficient Voting system with (2,2) Secret Sharing Based Authentication", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (1) , 2015, 410-412
[5] Prof. S.M. Jambhulkar, Prof. Jagdish B. Chakole, Prof. Praful. R. Pardhi "A Secured Approach for Web Based Internet Voting System using Multiple Encryption", 2014 International Conference on Electronic Systems, Signal Processing, and Computing Technologies,2014.
[6] Firas I. Hazzaa, Seifedine Kadry, Oussama Kassem Zein,"Web-Based Voting System Using Fingerprint Design and Implementation",International Journal of Computer Applications In Engineering Sciences ISSN: 2231-4946.
[7] Shivendra Katiyar, Kullai Reddy Meka, Ferdous A.Barbhuiya, Sukumar Nandi, *"* Online Voting System Powered By Biometric Security Using Steganography*"* Second International Conference on Emerging Applications of Information Technology, 2011.
[8] Himanshu Agarwal, G.N.Pandey, "Online Voting System for India Based on AADHAAR ID", Eleventh International Conference on ICT and Knowledge Engineering 2013.
[9] K. P. Kaliyamurthie, R. Udayakumar, D. Parameswari and S. N. Mugunthan , "highly secure online voting system over network", 4833 Indian Journal Science and Technology Print ISSN: 0974-6846 Online ISSN: 0974-5645 Vol 6 (6S) May 2013.
[10] Gianluca Dini "Increasing Security and Availability of an Internet Voting System", Proceedings of the Seventh International Symposium on Computers and Communications (ISCC'02) 1530-1346/02 $17.00 © 2002 IEEE.
[11] Xun Yi, EijiOkamoto, "Practical Internet voting system", Journal of Network and Computer Applications 36 (2013) 378–387.