Online Voting System Using Biometrics Based On Aadhar Card Data

Rasika Ashok Patil.
Student, Dept. of I.T.
C. K.Thakur A.C.S College New Panvel
rasika1245@gmail.com

Krutika Vijay Patil.
Student, Dept. of I.T.
C. K.Thakur A.C.S College New Panvel
krutika18patil@gmail.com

Mohini Mohod.
Professor, Dept. of I.T.
C. K.Thakur A.C.S College New Panvel
mohinimohod02@gmail.com

Abstract: In every country Election is the basic embellish of democracy which allows country persons to give their thoughts by electing the leader in accordance with their choice.

In India, the percentage of voting is very poor and it is reducing day by day, also during voting there are many chances of cheating like Booth Capturing or people votes can be casted to different candidates other than the one whom they wanted to give their votes. This Problem can happen in our regular voting system. To avoid all these drawbacks in the traditional manual voting System applying biometrics in order to Put a stop to the cheating and to increase the Correctness and speed of the election so that one can cast his or her vote irrespective of his or her location.

Biometric systems are the system which make identification of person according to his/her physical characteristics which are unique. The Biometric methods which consist of fingerprints, face, hand shape, retina, iris, and voice track methods. We tried to make a sincere effort to stop this malicious activities & frauds.

The software which we are going to use will provide a user friendly GUI, so the one who are going to vote can cast their votes according to their choices. Our plan is to make the voting process friendly, secure & effective one

Keywords: Online Voting, Steganography, Biometrics, Authentication.

I. INTRODUCTION

In online voting system people can vote through the internet from anywhere.

The main aim of online Voting is good way to provide voters a comfortable environment so that voter will vote with less efforts using the internet. Until now there are so many properties have been used to make an Online Voting secure process, among them some are the below given must be satisfied.

- Eligibility: Only certified voter is allowed to give their votes.
- Privacy: There is no leak of information about voter's identification and a marked ballot.
- Uniqueness: The voter cannot cast his/her vote twice.
- Completeness: No voter can fake a valid ballot and a ballot should not be change, only correct ballots are counted correctly.
- Fairness: one should not untruth the voting result.
- Efficiency: The computations have to be done in a reasonable amount of time. 7.Mobility: The voter can vote from anywhere through internet.

So Paper we are making are using following concept for secure Online Voting process.

A. Steganography:-

Steganography is art or science to hide information during transmission of data. So Here, in the process of a steganography system the hiding of information is begin by recognizing a cover which can be altered without changing or destroying that embedding process creates a stego medium(This is the last segment of details that the casual viewer can see) by replacing these redundant bits with data from the hidden message. In our system we have used the steganography concept for transmitting casted vote from the voter machine to the system machine.

B. Biometrics:-

Biometrics is the calculation and analytical examination of persons distinctive physical and behavioral feature. A biometrics is a physiological feature of human being that can distinct a person from other and that intellectually can used for the identification of the person identity. It is much more dependable than any ID . also ID can be get thieve but biometric be duplicated. In our proposed system biometrics is used to take fingerprint of people which going to give vote for their valid identification. After the identification process system proceed further or system can block the further processing for unidentified voter.

II. LITERATURE SURVEY

Shivendra Katiyar, Kullai Reddy Meka, Ferdous A. Barbhuiya, Sukumar Nandi proposed online voting system using techniques like Steganography and Biometrics to secure online voting, but there was a drawback that during transferring of casted vote system can't provide best security from unauthorized access[1]. Johnson, N.F.,and Jajodia, S., Exploring steganography. This paper describes the Steganography techniques[2] Tadayoshi Kohno, Adam

Stubble_eld, Aviel D. Rubin, and Dan S. Wallach proposed methodology which describe electronic voting system and security [3]

III. PROPOSED METHODOLOGY

By Using the proposed system, the voting process can be complete using internet with the secure concept of biometrics and Steganography. to the server securely using Steganography.

Steganography is the art of hiding the private data within something that seem to be nothing and which can be easily get ignore. The model of Steganography tells that if someone wanting to send the secret messages then he/she will choose a cover image, find its redundant bits and replace these bits with data bits of the message.

The message can be easily get to know by doing some operations on the other end. In this way the Voter who caste their vote will transmit without any interruption.

Fingerprint recognition is used for user authentication or identification because it is the mostly used biometric technique. In our proposed system the thumb impersonation of person who are going to vote is taken, system extract the features from the given thumb and compare it with the thumb which is already stored into the database during registration. If it matches, then voters are allowed to cast their vote otherwise system stop the voting untill the thumb impression get match. Once an voter passes all the security criteria he will get logged in his voting account. Once a particular voter is authenticated or identified by the system, one secure channel will get established using https and then voter will be able to vote. The vote will remain secret i.e. it will not be get reveal and not be reflected anywhere in the database that which user has voted for whom.

The casted vote will get added into the candidate's count.Then, the account will be closed if any voter will try to vote again throw his/her account that user will not allowed to cast vote again. So the ID which is used of the voter is nothier's Adhard ID. This is complete voting process. The methodology of the voting process is shown in figure below:

IV. SYSTEM IMPLEMENTATION

In our system we are focusing on the concept of security during casting vote through internet. Two strong security methodologies are used

A. Steganography

B. Biometrics

Algorithm used to perform Steganography described below:- a. Stego image creation algorithm:-

Input: Cover [], Core [], RN [], SM []

Output: Stego []

Begin

for every bit of Secret Message SM [i] do if SM [i] = 1 then
if Cover[RN[i]] and Core[RN[i]] both odd then
Stego[RN[i]] = Cover[RN[i]] – 1
else if Cover[RN[i]] and CI[RN[i]] both even then
Stego[RN[i]] = Cover[RN[i]] +1 End
Else

Stego[RN[i]] = Cover[RN[i]]

End
else if SM[i] = 0 then

if Cover[RN[i]] and Core[RN[i]] both either even or odd
then Stego[RN[i]] = Cover[RN[i]] else
Stego[RN[i]] = Cover[RN[i]] + 1 End
End End

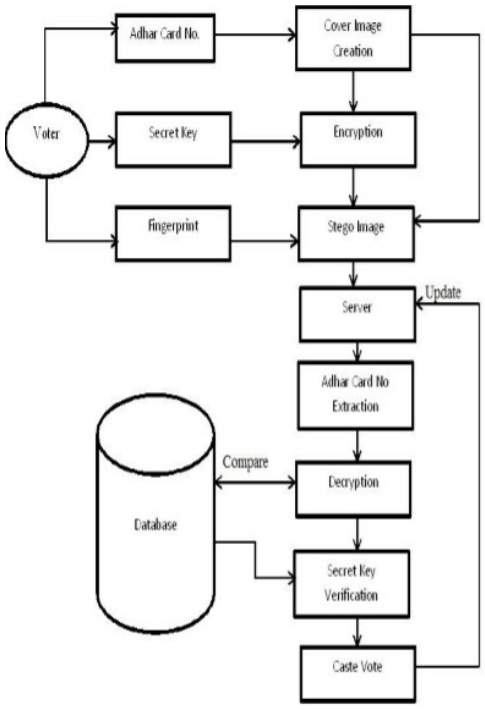


Fig. 1. Methodology of the Voting Process

According to the algorithm, if encrypted message bit is one and both cover image and key image byte values are odd we are making stegonographical image byte value one less than cover image byte, else 1 more than that.

If encrypted message bit is byte values are even or odd we are keeping stegonographical image byte value same as cover image byte value, else one more than that. We should check that during extraction have to apply the similar random function with the same seed.

Decryption algorithm for authentication:-

Input: Stego [], Cover [], RN[], Secret Key

Output: Authentic Voter/ Not an Authentic Voter

Begin

[], Da[], $SecretKeyDate$, k = 0 for i=0 to 287 do

if Stego[RN[i]] and Core[RN[i]] both either even or odd then

SM[i]= 0

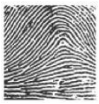
else SM[i] = 1

end

end

for i = 256 to 287 do

Date [


Se

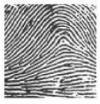
Concatenate(SecretKey,Date) if Compare(SM[], SHA256(SecretKeyDate)) then

Return: Authentic Voter else

Return: Not an Authentic Voter End

End

In the above algorithm, we are checking bytes of stego image and key image, if both are odd or even we are taking the secret message as one otherwise zero. Using the Date value contained in the secret messag0e and Secret Key we can verify the authenticity. In biometrics for fingerprint following features are to be considered for unique identification.


Loop Whorl Arch

Loop:-

The loop is the common type of fingerprint pattern.

Arch:-

The arch pattern is a more open curve compare to the loop.Two types of arch patterns: plain arch and tented arch.

Whorl:-

Whorl patterns occur in about 30% of all fingerprints

Algorithm used to implement Biometrics described below:-

Initially there are two types of biometric algorithms

1) Feature extraction/template generation algorithms:-

first function of the algorithm is the feature extraction of the sample which presented to the system. Template generation then takes place where a digital representation of biometrics and stored for matching purposes in the future.

2) Matching algorithms:-

In this algorithm matching of the given samples and previously stored samples is done and it will generates the results of comparison by performing estimation, calculation or measurement.

AES algorithm are used for encryption and decryption process AES:- The algorithm starts with a Add round key stage and followed by nine rounds of the 4 stages and a 10th round of the 3 stages. This get for both encryption and decryption with the exception that each stage of a round the counterpart in the encryption algorithm.

The four stages are as follows:

- Substitute bytes
- Shift rows
- Mix Columns
- Add Round Key

In the tenth one step of Mix Columns stage in ignored. The first nine round of a decryption algorithm contains the following:

- Inverse Shift rows
- Inverse Substitute bytes
- Inverse Add Round Key
- Inverse Mix Columns

Also then the tenth round is leaves out the Inverse Mix Columns stage.

V. FUTURE SCOPE

Currently we have considered fingerprint recognition for this online system, however the data which will be retrived from Adhar Card is having Retinal scan and image data stored and the future scope as below:

- If the voter is having scratches on finger or physically disabled and unable to use fingerprints then we can use Retinal scan as 2nd authentication method.
- Image can be used with face recognition as 2nd authentication where finger recognition deice is not available.
- As currently as part of KYC we connect mobile number to Aadhar Card, this can be also utilised as notification after voting to voter.

VI. CONCLUSION

In the paper we create a reliable online voting system based on biometric fingerprint.

We tried to overcome all the difficulties occurs in current voting system. In Our system we have many strong features like correctness, verifiability ,convenience etc. The fraud occurrence can be removed easily in this system because all is handled by systems rather than human being.

So there is no requirement of election officer, paper ballot or any electronic machine in this proposed voting system only the internet connection and thumb scanners are required then the voters can vote from anywhere secure.

VII. REFERENCES

[1] Shivendra Katiyar, Kullai Reddy Meka, Ferdous A. Barbhuiya, Sukumar Nandi,"Online Voting Sys- tem Powered By Biometric Security Using Steganography",2011 Second International Conference on Emerging Applications of Information Technology.

[2] Johnson, N. F. and Jajodia, S., Exploring steganography: Seeing the unseen, IEEE Computer Magazine, pp. 26-34, February 1998.

[3] Tadayoshi Kohno, Adam Stubble_eld, Aviel D. Rubin, and Dan S. Wallach, Analysis of an Elec-tronic Voting System, Proc. IEEE Symposium on Security and Privacy (May, 2004), found at http://avirubin.com/vote/analysis/index.html