Open access Journal International journal of Emerging Trends in Science and Technology

Online Voting System Based On Biometrics Using Adhar Card Data

Authors
Prof. JadhavAbhijit D., Ambavane Pooja R., Patil Mrunalini A.
Shewale Kalyani G., Vishwasrao Shyama P.
Department of Information Technology
Sharadchandra College of Engineering,Otur
Email: *Pooja14592@gmail.com.,Mrunalinipatil73@gmail.com*

Abstract
Literature is the media of teaching and learning authentic language. The language of literature is well organized and wonderful choice of diction. Language generally represents literature. The recent historical positions regarding the use of literature in English language teaching, and the inclusion of literary texts may foster the development of reading, writing, speaking, listening, and critical thinking skills. This is the reason why, this paper argues for the use of literature for language teaching purposes. More important, it claims consistently that the use of literature for language teaching purposes can promote literary understanding and general linguistic awareness among teachers and learners.
Key words: Literature, Language, Skills development, Motivation, Oppositions and Resistanc
Abstract-In every country Election is nothing but the basic ornament of democracy that allows country people to show their opinions by electing their leaders in accordance with their choice.In our country the voting percentage is very poor and it is degrading day by day also during voting there may be chances of cheating like Booth Capturing or people votes can be casted to different candidates other than the one whom they wished to give away their votes. This happens in our regular voting system. To avoid all the drawbacks in all the traditional manual election systems' problems, our aim is to cast Online Voting System employingbiometrics in order to avoid frauds and to enhance the accuracy and speed of the election so that one can cast his vote irrespective of his location, Biometric systems are the system which make identification of people according to their physical characteristics which are unique always. Biometric methods consist of fingerprint, face recognition, hand shape, retina,voice tracking, iris recognition, palm print methods.
We have tried to make a sincere effort to put a stop to all the malicious activities & safeguard the right of voting of each & every individual of country. The software will provide a user friendly GUI using which the voters can cast their votes according to their choice to the corresponding candidates. Different levels of security would be provided in the software which would help in authentication of an individual. Thus we plan to make the voting process friendly, secure & effective one.
Keywords-Online Voting, Steganography, Biometrics, Authentication..

INTRODUCTION

In online voting system people can cast their vote through the internet from anywhere. The ultimate aim of online Voting is to provide voters a good environment so that voters can cast their votes with minimum efforts on the internet. Until now there are many properties have been proposed to make the Online Voting secure, among them some secure processes are describe below must be satisfied.

1. Eligibility: Only eligible voters are permitted to cast their vote.
2. Privacy: There is no association between voter's identification and a marked ballot.
3. Uniqueness: No voter can cast his ballot more than once.
4. Completeness: No one can forge a valid ballot and a voter's ballot cannot be altered, the valid ballots are counted correctly.
5. Fairness: No one can falsity the result of voting.
6. Verifiability: Voters can verify that their ballots are counted correctly.
7. Efficiency: The computations can be performed within a reasonable amount of time.
8. Mobility: The voter can vote anytime and anywhere by using internet.

In this Paper we used following concept for secure Online Voting process.

Steganography:-

Steganography is art or it is a science to hide information during transmission. Essentially, Here in process of a steganography system the information-hiding starts by identifying a cover medium's redundant bits (those that can be modified without changing or destroying that medium's integrity).The embedding process creates a medium by replacing these redundant bits with data from the hidden message is called stego medium.

In our proposed system we are using the steganography concept for transmission of casted vote from voter machine to system machine.

Biometrics:-

A biometrics is a behavioral or physiological characteristic of a human being that can distinguish one person from another and that theoretically can be used for identification or verification of identity.It is much secured than any ID or password. ID or Password can be stolen but biometric features cannot be stolen or can't be duplicated.

In our proposed system biometrics is used to take fingerprint of voter for valid identification of voter.After identification process system proceed further or system can restrict the further processing for unidentified voter.

2. Literature Survey

ShivendraKatiyar, 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.,andJajodia, 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]

3. Proposed Methodology

Using the proposed system voting can be done through internet with the security concept of biometrics and Steganography. Voter's valuable vote transmitted to the

server securely using Steganography. Steganography is the art of hiding private or sensitive data within something that appears to be nothing. The general model of Steganography says that if you want to send some secret message then choose a cover image, find the bits which are redundant and replace the redundant bits with data bits of the message. The hidden message can be easily extracted by performing some operations on the other end.in this way the casted vote of voter will transmit without any interruption.

Fingerprint recognition is used for user authentication because it is the most deployed biometric technique. Here in our proposed system thumb impression of voter in taken, system extract the features from given thumb and compare it with the thumb which is stored into the database previously during registration. As it matches, then voters are permitted to cast their vote otherwise system don't permit them for voting till the thumb impression get match.

Once an individual passes al the security criteria he/she will be logged into his/her voting account. Once a particular voter is authenticated by the system, a secure channel will be established using https and then he/she will be able to cast the vote. The vote will remain secret i.e. it will not be reflected anywhere in the database that which user has voted for whom. The casted vote is added into the candidate's account accordingly finally, the account will be closed if any voter will try to vote again throw his/her account that user will not be able to cast vote by any means again. Here the ID of the voter is nothing but voter's Adhar card ID.This is complete voting process. The working flow of the voting process is shown in figure below.

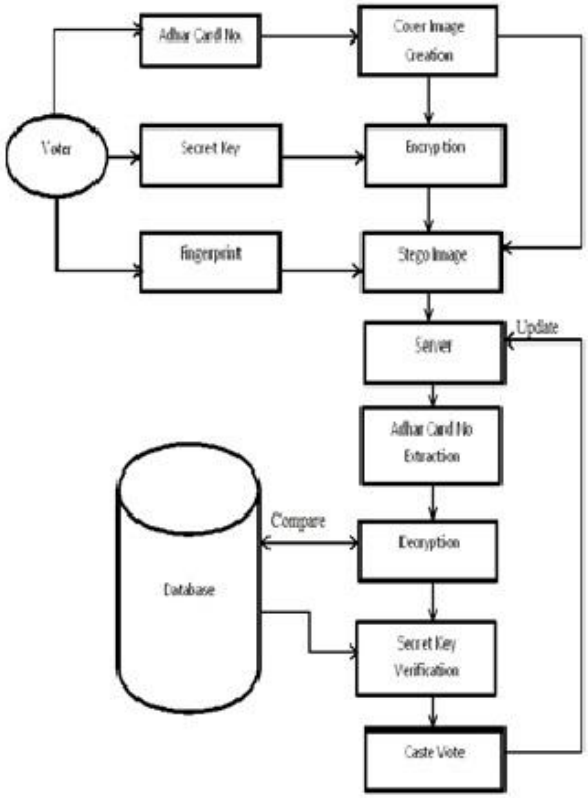

Figure 1: System Implementation

4. System Implementation

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

1. Steganography
2. Biometrics

Algorithm used to implement Steganography described below:-

A. Stego image creation algorithm:-

Input: Cover [], Core [], RM [], SM []
Output: Stego []
Begin
forevery bit of Secret Message SM [i] do
ifSM [i] = 1 then
ifCover[RM[i]] and Core[RM[i]] both odd then
Stego[RM[i]] = Cover[RM[i]] – 1
else if Cover[RM[i]] and CI[RM[i]] both even then
Stego[RM[i]] = Cover[RM[i]] +1
end
else
Stego[RM[i]] = Cover[RM[i]]
end
else if SM[i] = 0 then
ifCover[RM[i]] and Core[RM[i]] both can either even or odd
thenStego[RM[i]] = Cover[RM[i]]
else
Stego[RM[i]] = Cover[RM[i]] + 1
end
end
End

According to the algorithm, if secret message bit is one and both cover image and key image byte values are odd we are making stego image byte value one less than cover image byte value, else one more than that. If secret message bit is zero and both cover image and key image byte values are even or odd we are keeping stego image byte value same as cover image byte value, else one more than that. We should notice that during extraction we have to apply the same random function with the same seed.

B. Decryption algorithm for authentication:-

Input: Stego [], Cover [], RM[], Secret Key
Output: Authorized Voter/ Not an Authorized Voter
Begin
$S[]$, $Date[]$, $SecretKeyDate$, k = 0
fori=0 to 287 do
ifStego[RM[i]] and Core[RM[i]] both either even or odd then
SM[i]= 0
elseSM[i] = 1
end
end
fori = 256 to 287 do
Date [k++] =SM[i]
end
$SecretKeyDate = Concatenate(SecretKey, Date)$
if$Compare(SM[], SHA256(SecretKeyDate))$
thenReturn: Authorized Voter
else
Return: Not an Authorized 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 message and Secret Key we can verify the authenticity.
In biometrics for fingerprint following features are to be considered for unique identification.



LoopArch Whorl

Loop:-
The loop is the common type of fingerprint pattern and accounts for about 65% of all prints.

Arch:-
The arch pattern is a more open curve than the loop. arch patterns having two types: the plain arch and the tented arch.

Whorl:-
Whorl patterns occur in about 30% of all fingerprints and are defined by at least one ridge that makes a complete circle.

Algorithm used to implement Biometrics described below:-

Initially there are two types of biometric algorithms

1. Feature extraction or template generation algorithms:-

The first function of the algorithm is the processing or feature extraction of the sample presented to the system. Template generation then takes place where adigital representation of one's biometric is created and stored for matchingpurposes in the future.

2. Matching algorithms:-

In this algorithm matching is done with the given samples and previously stored samples and generates the resultsof comparison by performing estimation, calculation or measurement.
AES algorithm are used for encryption and decryption process

AES:-
The algorithm starts with an Add round keystage followed by 9 rounds that having four stages
and a tenth round having three stages. These rounds are performed for both encryption and decryption withthe exception that each stage of a round the decryption algorithm which is the inverse of it'scounterpart in the encryption algorithm. The four tages are as follows:

1. Substitute bytes
2. Shift rows
3. Mix Columns
4. Add Round Key

In the tenth one step ofMix Columnsstage in ignored. The first nine rounds of
the decryption algorithm consist of the 4 stages:
1. Inverse Shift rows
2. Inverse Substitute bytes
3. Inverse Add Round Key
4. Inverse Mix Columns

Again, the tenth round simply leaves out the Inverse Mix Columns stage.

Conclusion
In this paper we tried to develop a secure internet voting system based on biometric fingerprint. We have tried to overcome all the drawback occurs in traditional or current voting system. Our proposed system having many strong features like correctness,verifiability, convenience etc. This is the system in which the power is in system's hand rather than any human being so that fraud occurrence can be removed easily.
For this proposed voting system no requirement of election officer, paper ballot or any electronic machine only the internet connection and thumb scanners are required so that one can vote from anywhere securely.

References

1. ShivendraKatiyar, Kullai Reddy Meka, Ferdous A. Barbhuiya, SukumarNandi,"Online Voting System 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 E-voting that is Electronic Voting System Proc. IEEE Symposium on Security and Privacy (May, 2004).