International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue14
November 2017

Online Voting System Powered By Biometric Security Using Steganography

Annapureddy Gayathri & S. Asif
PG Scholar, Dept of CSE, Asst. Professor, CSE Dept, CMR Institute of Technology,
cooldude.asif@gmail.com, agayathri777@mail.com,

Abstract—*Utilizing Cryptography and Steganography whilst, we attempt to provide Biometric as well as Password protection to voter bills. The scheme makes use of snap shots as duvet objects for Steganography and as keys for Cryptography. The important thing snapshot is a Biometric measure, reminiscent of a fingerprint photo. Appropriate use of Cryptography commonly reduces the dangers in these programs as the hackers must find each secret key and the template. The fundamental concept is to merge the secret key with the quilt image on the groundwork of key photo. The outcomes of this process produces a stego photo which looks particularly much like the quilt photo but not detectable by means of human eye. The system goals the authentication requirement of a vote casting system.*

Keywords- on-lineballoting, Steganography, Biometric.

INTRODUCTION

Integrity of the election process will determine the integrity of democracy itself. So, the election system must be secure and robust against a variety off raudulent 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 votingsystem, whetherelectronic or using traditional paper ballots, the system should meet the following criteria:

1. Anonymity: Anonymity of ballot should be preserved; both to guarantee the voters safety when voting against a malevolent candidate and to guarantee that voter have no proof that proves which candidate received their votes.

2. Tamper-resistant: The voting system must also be tamper-proof to thwart a wide range of attacks, including ballot stuffing by voters and in correct tallying by insiders.

3. Human factors: A voting system must be comprehensible and usable by the entire voting population, regardless of age, infirmity or disability. Other requirements of such a system could be viewed as authentication, scalability,

speed and accuracy. .Among these, authentication can be viewed as the most critical issue. As online voting is risky, it is difficult to come up with a system which is perfect in all senses. Once we are sure that a voter is genuine, we can easily address other issues like anonymity and tamper resistance.

If other security is done well, electronic voting could be a great improvement over paper systems. Flaws in any of these aspects of a voting system, however, can lead to indecisive or in correct election results. Some of the existing solutions of computerized voting systems are explained by Armen and Morelli and highlighted their vulnerabilities. They include Punch Card Systems, Global Election Management System(GEMS)and Direct Recording Electronic (DRE).As these systems are stand alone systems ,they lack inability of voting from anywhere. That is why the actual notion of online voting is missing in those systems.

Steganography:

Steganography manner to hide secret knowledge into innocent knowledge .Digital photos are superb for hiding secret know-how. An picture containing a secret message is called a canopy snapshot. First, the difference of the cover image and the stego photograph must be visually unnoticable. The embedding itself will have to draw no additional concentration to the stego snapshot in order that no hackers would try to extract the hidden message illegally. 2nd, the message hiding method must be riskless. It's not possible for any individual to extract the hidden message if she/he does not have a designated extracting process and a right secret key. 0.33, the highest size of the key message that may be hidden will have to be as long as feasible.

Existing System:

- Paper-based voting systems originated as a system where votes are cast and counted by hand
- With the advent of electronic tabulation came systems where paper cards or sheets could be marked by hand counted electronically.
- These systems included punched card voting, mark sense and later digital pen voting systems.

Disadvantages:

- Tampering of registered votes.
- Hackers and intruders might hack the system and alter the results.
- Not much secure as compared to the latest generation and technology.
-

Proposed System:

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.

The algorithm uses image based steganographic and cryptographic system are proposed. The Steganography part is needed as we want to involve biometric identity to provide added security. Mostly, Steganography uses images as cover media because after digitalization images contain

the quantization noise which provides space to embed data.

Advantages:

- Maintains highest level of security.
- The process of collecting votes was secure, reliable and accountable.
- Ensuring Single Vote for Single Person.Automatic Counting.
- Steganography and cryptography is used for security.

Literature Survey:

2.1. Biometrics & Security: Combining Fingerprints, Smart Cards and Cryptography

Since the beginning of this brand-new century, and especially since the 2001 Sept 11 events in the U.S, several biometric technologies are considered mature enough to be a new tool for security. Generally associated to a personal device for privacy protection, biometric references are stored in secured electronic devices such as smart cards, and systems are using cryptographic tools to communicate with the smart card and securely exchange biometric data. After a general introduction about biometrics, smart cards and cryptography, a second part will introduce our work with fake finger attacks on fingerprint sensors and tests done with different materials. The third part will present our approach for a lightweight fingerprint recognition algorithm for smart cards. The fourth part will detail security protocols used in different applications such as Personal Identity Verification cards. We will discuss our implementation such as the one we developed for the NIST to be used in PIV smart cards. Finally, a fifth part will address Cryptography-Biometrics interaction. We will highlight the antagonism between Cryptography - *determinism, stable data* - and Biometrics - *statistical, error-prone* -. Then we will present our application of challenge-

response protocol to biometric data for easing the fingerprint recognition process.

2.2 Evidence based Access Control over Web Services using Multi Security:

In previous research the proposed system has determined the identity proof for the voters using hashing algorithms (MD5 and SHA1) through internet. From those results it founds that the security is not sufficient for the data. To protect the election accuracy, different methods have been proposed for hiding information. In this paper the proposed system embedded the information. The embedding is typically parameterized by a separate key. Without Knowledge about this key, it is difficult for a third party to detect or remove the embedded material. In this paper we are proposing a single text or a binary image is automatically scattered and embedded in video frames with BPCS method, genetic distortion audio tracks and text image with automated dynamic key for every transaction. The Dynamic key is generated by the calculation of the time stamp and efficient key is classified by the RSA cryptographic algorithm and managed in wireless networks. Here a single key is compressed of all the three keys make the user to be more convenient to encrypt and decrypt. According to the third party, a single packet is transfer for every transaction, but it has the fused format. This paper explains on voting through internet, with facial detection integrated with finger print authentication and automated load balancing, fused with data hiding security. A data hiding method, which is applicable through steganography, and the biometric concepts provide full security for data that is passed through the network from different places. The main goal of this work is it supports a remote voter registration scheme that increases the accuracy of the current systems. In this scheme the voter identification is carried out by biometric systems. This work evaluates how to take advantage from the most usable biometrics to carry out the voter registration process in a more effective way. Biometrics is also used to prevent impersonation, detect multiple registrations from the same person and protect from alterations of the registration information. This modification ensures higher payload and security.

The significant improvement in the information and communication Technology (ICT) from last few decades increases various new needs. E-Governance system has also no exception. People are approaching to fulfil their dreams. In the case of M-voting the security is the major issue. Democracy Needs all and only the authorized voters can vote and each eligible voter can vote but not more than once. To achieve these voters, need to be registered properly and

authenticated. This paper presents a novel approach to provide secure mobile voting based on Biometrics in conjunction with elliptic curve cryptography and steganography (ECC-stegno scheme)..

2.3. Secret Key Expansion Using Hashing: The secret key plays very important role in the whole process. It should not be compromised in any case. There is alimitation with the secret key here, as thesystem is designed for general public which is quite negligent in these issues, we can't keep the key too long. It should be short enough to be remembered by everybody. For explanation purpose we are assuming it to be a 4-digit number, similar to ATM PIN. This 4-digit PIN can easily be represented using 2 bytes. But 2 byte data looks very much vulnerable in terms of length. As we have to finally embed it into the image, which is quite big. The cover image is a 24-bit image where every pixel is represented using three bytes. So, we have 3 ∗ 2^16 byte data in total. Now hiding only 2 bytes in this much space will not fully exploit the resources in terms of cryptography. This is because the algorithm we are using provides both cryptography and steganography at the same time. Steganography says its good as the statistical properties of the cover image will remain intact due to under-performed modification As the fingerprint image is of the same dimension, we will be exploiting very less features of the key image. So, to increasethe complexity of analysis, the 2 byte secret key is expanded to 32 byte key by applying MD5 hashing algorithm [2]. Now these 160 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 remain 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.

MODULES:

This project contains two modules

- Admin
- User

1**. Admin**

There are some pre-requisites to support such a system. Firstly, each and every individual in the country should be provided with a Personal Identification Number, such as SSN (Social Security numbers) in some countries. This is needed for maintenance of voter accounts in the database. Secondly, we need Thumb Impressions (fingerprint images) of all the individuals.

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue14
November 2017

Thirdly, during the account creation every individual will be provided with a system generated Secret key which he/she should not disclose to anybody. This will be needed to cast the vote.

2. **User**

To cast a vote, a voter logs in to the system by entering the personal identification number and secret key. Along with this voter has to give the thumb impression on the fingerprint sensor. The system will generate the cover image and embed the secret key into it according to the predefined procedure to generate the stego image. Now this stego image will be sent securely to the server for voter authentication.

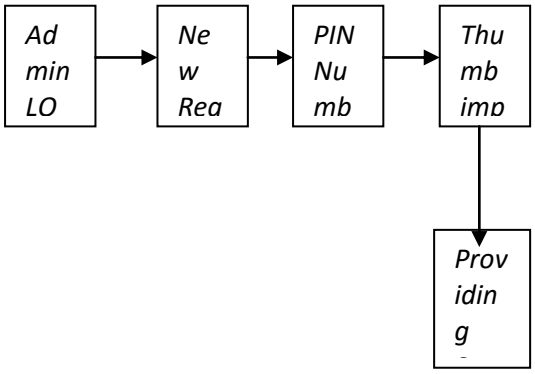


Fig.No: 4.2.6. Admin

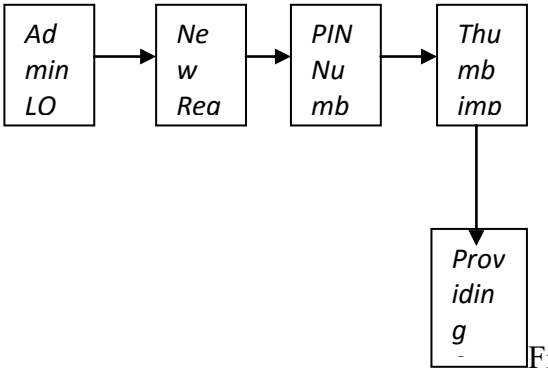


Fig. No: 4.2.6. User

Block Diagrams:

CoverImageCreation

Steganography manner to hide secret knowledge into innocent knowledge.Digital photos are superb for hiding secret know-how.A picture containing a secret message is called a canopy snapshot. First, the difference of the cover image and the stego photograph must be visually unnoticable. The embedding itself will have to

Draw no additional concentration to the stego snapshot in order that no hackers would try

to extract the hidden message illegally. 2nd, the message hiding method must be riskless. It's not possible for any individual to extract the hidden message if she/he does not have a designated extracting process and a right secret key. 0.33, the highest size of the key message that may be hidden will have to be as long as feasible. Everyvotershouldhavea16digitpersonalidentificati on number. This number will be automatically written over abase image in predefined font style &size. Let ususe256*256 PIXELS BIT MAP COVER IMAGE. The base image should be clear so that the text written over it is machine red able. This image will be finally modified into a stego-image and sent over in secure channel. The base image is a default image for the system, same for all. Cover image is a simple inscription of personal identification number over the base image. So, the cover image for every voter will be same except he digits written over its shown in the figure.

Secret key expansionus in ghashing:

The secret key plays very important role in the whole process. It should not become promised in any case. Here is a limitation with the secret key here, as the system is signed for general public which is quite negligent in these issues, we can't keep the key too long.Itshouldbeshortenoughtoarea assumingittobea4 digit number, similar to ATM pin. This 4 digit pin can easily be represented using 2 bytes. But 2 byte data looks very much vulnerable in terms of length. As we have to finally embed it into the image, which is quite big. The coverimage isa24-bit image where every pixel is represented using three bytes. so, we have 3∗ 216 byte data in total. Now hiding only 2BYTES IN THIS much space will not fully exploit the resources in terms of cryptography. This is Because the algorithm we are using provides both cryptography and steganography at the same time. Steganography says its good as the statistical properties of the cover image will remain intact due to underperformed modification. The eaves droppers will never be able to deduce that some data is hidden in the image. But if somehow they know that it is a stego image, they can easily extract the pin.

From the cryptography point of view,the key image will remain under-utilized as well. As the fingerprint image is also of the same dimension, we will be exploiting very less features of the key image. So,to increasethe complexity of analysis,

the2byte secret key is expanded to32 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 remains a e. The stegoimage will remain more complex to be analyzed because more features of the keyimae are utilized in this case. so, even ifcleaves droppers know that this is a stegoimage, it would be more difficult for them top predict the embedded data.

Embedding Algorithm:

The embedding algorithm makes use of a stego- cryptographic model. The model easily unifies cryptographic and steganographic models. It basically results as a steganographic one with the addition of a new element as the key image. It finally delivers cryptographic functionality while preserving its steganographic nature.

The output of this embedding process is a stego image S and the inputs are expanded secret key concatenated with time-stamp, i.e. secret message, a cover image and the key image. In this embedding process we are going to modify the 256*256 pixels cover image given by the array CI[] of $3 * 216$ size. In terms of cryptography, performing permutations on input data increases the level of confusion More is the level of confusion, more it will become unpredictable. In this phase wedistribute the bits of secret message throughout the image in a random manner.

As we need to embed 288 bits of secret message into cover image by encryption, we need to determine the bytes of cover image which we are going to modify. These are determined by random function with secret key as seed. Here, we have array Random[] of size 288 with values ranging from 1 to $3 * 216$. Initially stego image array SI[] is same as that of cover image array CI[]. We have a key image array KI [] of $3 * 216$ bytes. So, in order to yield stego image S we are going to modify the array SI[] by the following embedding algorithm.

Embedding Algorithm:

Input: CI[],KI[],Random[],SecretMsg[]**Output:**SI[]

Begin

SI[]=CI[]

for*EverybitofSecretMessage SecretMsg[i]* **do**

if*SecretMsg[i] =1***then**

if*CI[Random[i]] andKI[Random[i]] botheither evenorodd***then**

if*odd***then**

SI[Random[i]] =CI[Random[i]] -1

else

SI[Random[i]] =CI[Random[i]] +1

end

else

SI[Random[i]] =CI[Random[i]]

end

else

if*CI[Random[i]] andKI[Random[i]] botheither evenorodd***then**

SI[Random[i]] =CI[Random[i]]

else

SI[Random[i]] =CI[Random[i]] +1

end

end

end

End

Authentication Algorithm:

In the extraction process, firstly the personal identification number from the Stego image is read using OCR. Now, from the matching entry in the voter database, we read the key Image and Secret key of that individual. The keytosuccessful comparisonisthe time-stamp value. The time- stamp (e.g. Date)delivers the security from replay attacks, so that the same stego image cannot be used again in future. Using this secret key as seed we are generating the array Random []of size288. From the stego image we are forming the array SI [].Also, we have array KI []given by key image. Using these we can extract the Secret Msg [] by applying the algorithm given below.

Authentication Algorithm:

Input:SI [], KI [], Random [], Secret Key

Output: AuthenticPerson/NotanAuthenticPerson

Begin

SecretM[],*Da* [32],*SecretKeyDate,j*=0

for*i=0to287***do**

if*SI[Random[i]] andKI[Random[i]] botheitherevenor odd***then**

SecretMsg[i]=0

else

SecretMsg[i]=1

end

end

for*i=256to287***do**

Date[j++]=SecretMsg[i]

end

SecretKeyDate=Concatenate(*SecretKey,Date*)

if*Compare* (*SecretMsg* [],*A*256(*SecretKeyDate*))

then

Return:Authentic Person

else

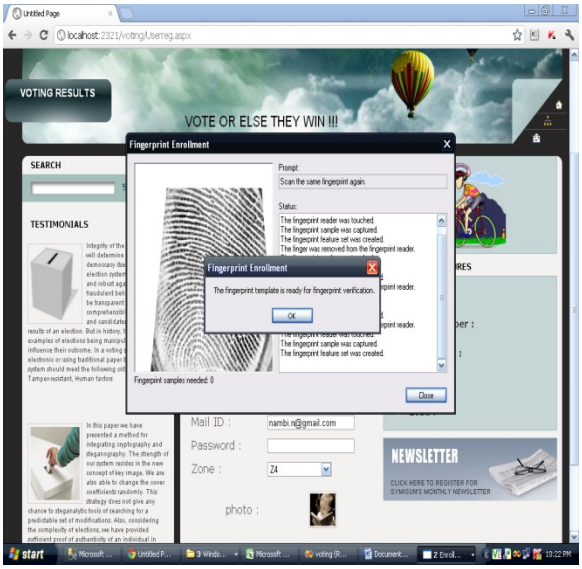
Return:NotanAuthentic Person

end

End

Screen Shot:

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue14
November 2017



Conclusion and Future Enhancement:

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.

To improve two considerable aspects of the algorithm, namely, speed and dependence on pseudo random function.

References:

1.William Stallings, Cryptography and Network Security Principles and Practices, Prentice Hall, pp. 67-68, 2003.
2.Bruce Schneier, "Applied Cryptography" in Protocols Algorithms and Source Code in C, John Wiley and Sons, 1996.
3.Tadayoshi Kohno, Adam Stubblefield, D. Rubin Aviel, Dan S. Wallach, "Analysis of an Electronic Voting System", *Proc. IEEE Symposium on Security and Privacy*, May, 2004.
4.N. F. Johnson, S. Jajodia, "Exploring steganography: Seeing the unseen", *IEEE Computer Magazine*, pp. 26-34, February 1998.
5.N. Provos, P. Honeyman, "Hide and seek: An introduction to steganography", *IEEE Security and Privacy*, 2003.
6.M.S. Sutaone, M.V. Khandare, "Image based steganography using LSB insertion technique", *IEEE WMMN*, pp. 146-151, January 2008.
7.D. Bloisi, L. Iocchi, "Image based Steganography and Cryptography", *Proc. of 2nd Int. Conf. on Computer Vision Theory and Applications (VISAPP)*, pp. 127-134, 2007.
8.M. Kharrazi, H. T. Sencar, N. Memon, "Image steganography: Concepts and practice", *WSPC Lecture Notes Series*, 2004.
9.C. Armen, R. Morelli, "E-Voting and Computer Science: Teaching About the Risks of Electronic Voting Technology", *ACM ITiCSE*, 2005.