Securing Online Voting System Using Multimodal Biometrics and Steganography

Neha Gandhi[1] Dr. Chander Kant Verma[2]
[1]M.Tech. Scholar [2]Assistant Professor

Abstract— with the help of online voting system author can manage election easily and securely. In this paper, we provide security to online voting system with secure user authentication by providing biometric as well as password security to voter accounts. System will decide whether voter is genuine or not. Firstly, system will capture facial image of voter and then take fingerprint impression of voter and after that fuse them. After fusion, we get an image which is taken as cover image and then we embed voter secret data into cover image using Steganography. This method produce stegno image which is quite same as cover image. Extraction of stegno image is take place at server side to perform the voter authentication. Correct use of this procedure decrease threat factor in online voting system the proposed work is to enhance security in online voting system with multimodal biometrics along with steganography concept.

Keywords: Biometrics, Online Voting, Stego image, Steganography.

I. INTRODUCTION

It is a web based that facilities the running of elections and surveys online. Objective behind the development of this system is to simplify the process of organizing elections and make it easy for voters to vote remotely from their home computers. An election is an official process by which person chooses an individual to hold all kind of public issues. So the whole system of election must be secure and robust against a variety of fraudulent behaviors [3]. System should be transparent and comprehensible so that voters and candidates can accept the results of election [9].Integrity of the election process will help in determining the integrity of democracy itself .Furthermore; the traditional way of voting will take a long process and time. So, the novel online voting will become the best solution for the matters; besides provide easier way of voting. When we compared it with existing voting system the Electronic voting has several advantages [9] like: Electronic voting system is capable of saving considerable printing stationery and transport of large volumes of electoral material. It is very easy to transport, Store, and maintain. It completely rules out the chance of votes which are not valid. In a voting system, whether electronic or using traditional paper ballots, the system should meet the certain important criteria such eligibility and authentication, uniqueness, accuracy, integrity, verifiability, reliability, secrecy, flexibility, convenience, transparency, and cost effectiveness. Among these, authentication can be viewed as the most critical issue.

A. Biometrics

Biometric recognition is a common and reliable way to authenticate any human being based on his physiological or behavioral biometrics [11].Biometric recognition means by measuring behavioral and biological characteristics of an individual in a recognition inquiry and comparing these data with the biometric reference data which had been stored during a learning procedure, in this way the identity of a specific user is determined. Because it is difficult to misplaced, forged, or shared biometric identifiers, they all are considered more reliable for recognition of person than traditional token or knowledge based methods. The main objectives of biometric recognition are user convenience, security and higher efficiency.

B. Multibiometrics

Unimodal biometrics uses single source of biometric system for personal identification. It has variety of problems such as noise in sense data, Intra-class variation, Inter-class similarities and spoof attacks. Multibiometrics is a combination of one or more biometrics. In multibiometrics noise in any one of the biometrics will lead to high false reject rate (FRR) while identification .All these problems are addresses by Multimodal biometrics. Multimodal biometrics is combination of two or more biometrics system (e.g. Fingerprint and Face, Face and Iris). Multibiometric systems [1] remove some of the drawbacks of the uni-biometric systems by grouping the multiple sources of information .The main objective is to provide a higher level security to online voting system. These systems utilize more than one physiological or behavioral characteristic for enrollment and verification/identification. Multibiometrics addresses the issue of non-universality or insufficient population coverage. It becomes difficult for an imposter to spoof multiple biometrics traits of a legitimately enrolled individual.

II. PROPOSED METHODOLOGY

Using this proposed system voting can be done through internet with the concept of Steganography and multibiometrics. Steganography is idea of hiding private or sensitive data within something that appears to be nothing out of normal. . If a person sees the digital object, he or she will have no idea that there is any hidden information, and therefore the person will not try to decrypt the information. Basically, there are some types of Steganography like audio, image, video etc. Images are well liked cover media used for Steganography here [2]. The basic model of Steganography says if you want to send some private information then choose a cover image, find its redundant bits and replace these bits with data bits of the information. The information can be easily extracted by doing some operations on the other end. Concept of Steganography is used to achieve these criteria's of a public voting system. Least significant bit insertion is a common approach to embed information in cover file given by [6].But this process of LSB modification changes some properties of cover image, so eavesdroppers can detect distortions in resulting stego image[5].Here we use different technique for image steganography based on DWT [8]. The LSB insertion technique is implemented in spatial domain in which the information is embedded into

the least significant bits of cover image to derive the stego-image whereas DWT technique is implemented in frequency domain in which the stego-image is transformed from spatial domain to the frequency domain and the information is embedded into the frequency components of the cover image. To work with this system each and every individual of country should be provided with a PAN number (Person Authentication Number). System also needs facial image and fingerprint impression of all voters. Here, fused image of face and fingerprint is taken as cover image [7].Finally, at the time of account creation a secret key is given to each voter which voter should hide from every single person.

Fig. 1: Fused image of face and fingerprint as cover image

After collecting all above data from every voter system will work as follows. First of all the voter has to sign in to the account with the help of voter's account identification number. Then voter is asked to give the fingerprint and facial impression. Then the voter is asked to enter the secret key for PAN number decryption from the database embedded fused image. Finally the voter has to enter the PAN number. If PAN number match is found then the voter is an authenticate person & can cast a vote. Then the account will be closed for that person. Once the account will be closed then that account will not be opened again for second time. So the fraudulent cases such as duplicate voting will be avoided in the online voting system.

A. Database Creation

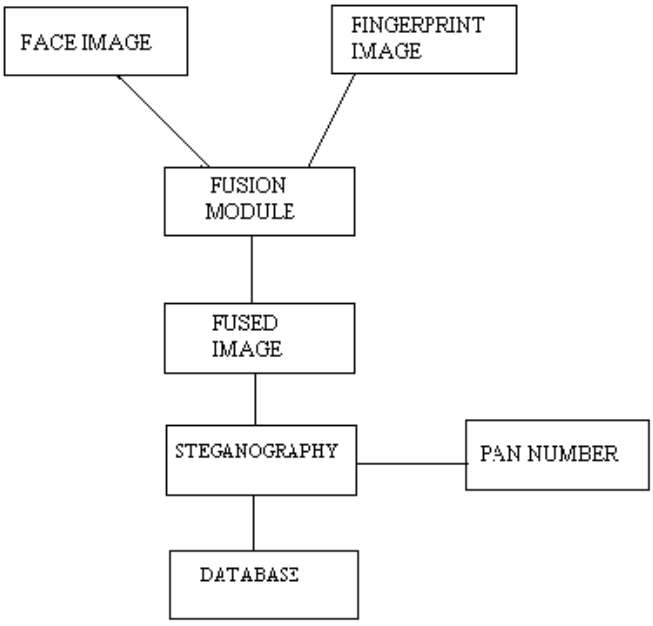

Fig. 2: Block Diagram for Database Creation

Database is created by voter committee. It's duty of committee members to collect the data from each person. Every voter should have an account identification number to maintain the account; PAN number is basically used for authentication of voter & secret key as password or cross verification of database.

As shown in the fig.2 finger print image block takes the fingerprint image of voter as an input. Facial image block takes the facial image of voter as an input. In the fusion module, fusin of fingerprint and face take place. PAN number block accepts the personal authentication number as an input. Steganography block performs steganography on the personal authentication number. Thus a stego image is saved as database image. Different aspects in data hiding systems are of great concern like capacity and security. Capacity means the amount of data that can be hidden in the cover object; security means an eavesdropper's failure to detect hidden information. We have concentrated our focus on security. The cover image for each voter is fused image only which we get after fusion of face and fingerprint. Prior to the least significant bit insertion, system uses discrete wavelet transform. In discrete wavelet transform with the help of HAAR transform the fused image is transformed from spatial domain to frequency domain. For 2-D images, HAAR transform processes the image by 2-D filters in each dimension. The filters divide the input image into four non-overlapping sub bands. The Discrete Wavelet Transform is made up of realization of Low pass Filters and High Pass Filters. It is one of the simplest and basic transformations from the time domain to a frequency domain. First of all HAAR transform convert the fused image into four non overlapping sub bands LL, LH, HL, HH as shown in the fig.3 . Where L stands for low frequency band & LL is shown at left upper most corners. H stands for high frequency band & HH is shown at right lower most corners. With the help of LSB (least significant bit) insertion technique the PAN number is embedded into the LL sub band. The fused image after PAN number embedding is shown in fig.3 as embedded image. If compared to the Fourier transform which only differs in frequency, the Haar function varies in both scale and position.

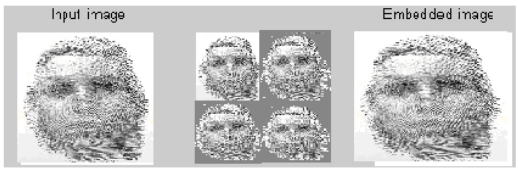

Fig. 3: Input Fused Image, Four Sub bands of HAAR Transform & Embedded Image

Applying a discrete wavelet transform to images, much of the signal energy lies at low frequencies and they appear in the upper left corner of the discrete wavelet transform. This property of energy compaction is made use of in this embedding procedure. Embedding is achieved by inserting the secret data into a set of discrete wavelet transform coefficients, thus ensuring the personal authentication number (PAN) invisibility. The combination of fused image & PAN number is nothing but a stego image is produced with the help of LSB insertion technique. It is assumed that, embedding message in this way is not going

to destroy the information of the original image to a great extent. A secret key is separately provided to each voter along with the PAN number. Voter should remember that in order to use it at the time of online voting. After completion of all the steps thus the database creation of the voter is complete. This task will be performed for each person.

B. Online Voting System

At the time of online voting as shown in the fig.4 a voter is first asked for voter's account identification number so that voter's election account will be opened[4]hen voter is asked to give the fingerprint image and facial image followed by secret key. PAN number is embedded in fused image of face and fingerprint. If the secret key is correct then the PAN number decryption & recognition is carried out with the help of reverse discrete wavelet transform. Reverse discrete wavelet transform is applied to the embedded fused image in order to get the embedded PAN number. Then the voter is asked to enter the PAN number. After comparing both the PAN numbers, if the match is found then the voter is an authenticate person & can cast a vote.

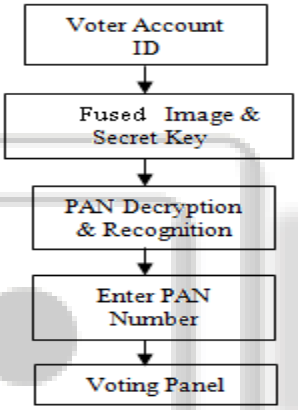

Fig. 4: Online Voting System

C. Embedding Process

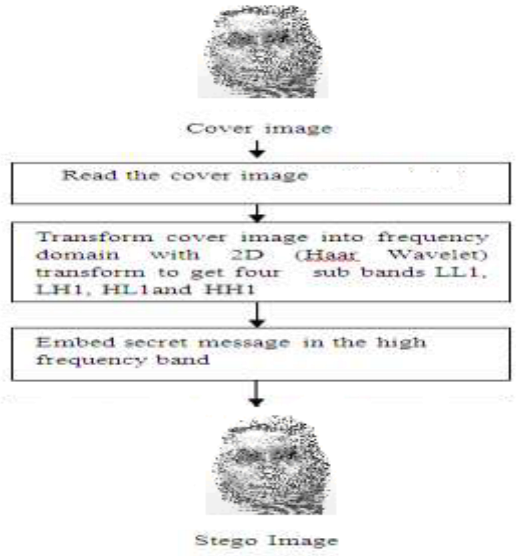

Fig. 5: Block diagram of Embedding Process

D. Extraction of embedded message

The result of embedded process is a stego image. Recognition process includes extraction of the PAN number from the stego image. For recognition purpose reverse discrete wavelet transform is applied to embedded fused database image as shown in fig. 6.

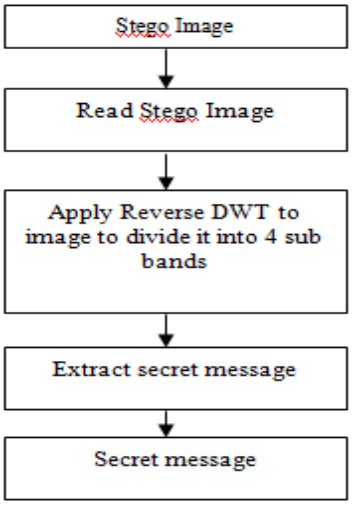

Fig. 6: Block Diagram for Extraction Process

III. Result & Analysis

This system uses account identification number to maintain the voters account, fused image of fingerprint and face as biometric security, PAN number for authentication &secret key for cross verification of the database. Thus the system provides a multilevel security which is the advantage over the earlier election system

A. Steganography Performance

Basically the least significant bit insertion technique is the method of data hiding by direct replacement i.e. spatial domain technique. But there are disadvantages like low robustness to modifications made to stego image & low imperceptibility. Hiding data with the help of transform domain is the great benefit which appeared to overcome the robustness and imperceptibility problems found in the LSB substitution techniques [10].

The proposed system was applied to fused images at each time & it achieved satisfactory results. The performance of the proposed technique can be evaluated in terms of comparison between quality of the stego image & original image. The comparison was done on the basis of imperceptibility. Imperceptibility measures how much distortion was caused after data hiding in the cover image that is the quality of the image.. We can evaluate the stego-image quality by using Peak Signal to Noise Ratio (PSNR). The PSNR ratio is used as a quality measurement between the cover image & stego image. The higher the values of PSNR better the quality of the stego image. Typical values for the PSNR are between 30 and 50 dB, with the bit depth of 8 Bit. The PSNR for size M x N image I and ts noisy approximation K is calculated

$$PSNR = 10 \log_{10} \{255^2 / MSE\}$$

And

$$MSE = 1/MN \Sigma^{M}_{x-1} \Sigma^{N}_{y-1} [p(x, y) - p(x, y)]^2$$

The PSNR was calculated for each stego image &PSNR ranges from 30 to 50 which give reasonable visual quality of the stego image.

In General, any steganography technique is done either in spatial or frequency domain. Spatial domain techniques are easy to create and design. They give an ideal reconstruction in the lack of noise. There are several techniques put forward in spatial domain like embedding utilizing the luminance components, manipulating the Least Significant Bits for embedding, Image Differencing. But using the spatial domain is not that much safe as it hide the secret data directly. On the other hand, in Frequency Domain, the cover image is subjected to a transformation into the frequency domain where detail manipulations of the coefficients with perceptible degradation to the cover image is possible. Thus the system supports two stages to hide data. First is transformation of fused image to frequency domain & then manipulation of least significant bit. Thus frequency domain technique is better approach for hiding data.

Table. 1: Parameter analysis of steganography methods

Features	LSB	DWT
Invisibility	Low	High
Payload capacity	High	Low
Robustness against Image manipulation	Low	High
PSNR	Medium	Low
MSE	Medium	High

IV. Conclusion

In this online voting system, author used the concept of multi modal biometrics. Unibiometrics has several disadvantages which are removed by using multibiometrics. In this proposed system, we take facial and fingerprint impression of voter and then fused them. After that author take fused image as cover image for embedding the PAN number. Fused image and PAN number has been used to obtain high degree of authenticity. The security level of system is very much enhanced by the idea of taking fused image as cover image for each user. This proposed system is enhancement over earlier online voting system.

References

[1] *A. K. Jain and A. Ross, "Multibiometric systems", Communications of the ACM, 47 (1), pp. 34-40, 2004.*

[2] Kharrazi, M., Sencar, H. T., and Memon,N."*Imagesteganography:Concepts and practice*", In WSPC Lecture NotesSeries,2004.

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

[4] Shivendra Katiyar, Kullai Reddy Meka, Ferdous A.Barbhuiya, Sukumar Nandi, "Online Voting System owered By Biometric Security Using Steganography" Second International Connference on Emerging pplications of Information Technology 2011

[5] Mohit Kr. Srivastava, Sharad Kr. Gupta, Sushil Kushwaha,Brishket S. Trip athi "Steganalysis of LSB Insertion methodin Uncompressed Images Using Matlab"

[6] Staone, M.S. and Khandare, M.V., *"Image based Steganography using LSB insertion technique",* IEEE WMMN, pp.146-151, January 2008.

[7] A. Ross and A.K. Jain, "Information Fusion in Biometrics", Pattern Recognition Letters, 24, pp. 2115-2125, 2003.

[8] P. Chen, and H. Lin, "*A DWT Approach for Image Steganography",*International Journal of Applied Science and Engineering 2006. 4, 3:275:290

[9] Tdayoshi Kohno,Adam Stubblefield,Aviel D.Rubin, and Dan S.Wallach. *"Analysis of an Electronic Voting System",* Proc. IEEE Symposium on Security and Privacy (May, 2004), found at http://avirubin.com/vote/analysis/index.html

[10] Ali Al-Ataby and Fawzi Al-Naima, "A Modified High Capacity Image Steganography Technique Based on Wavelet Transform" The International Arab Journal of Information Technology, Vol. 7, No. 4, October 2010.

[11] Jain, A.K., Bolle, R. and Pankanti, S., Biometrics: Personal Identification in a networked Society, Kluwer Academic Publishers, p.37, (2000).

