Steganography & Biometric Security Based Online Voting System

Shweta A.Tambe[1], Nikita P. Joshi\[1], P.S. Topannavar[1]

[1]Scholar, ICOER, Pune, India

Emai- suchetakedari@gmail.com

ABSTRACT – Online voting system that helps to manage elections easily and securely. With the help of steganography one can try to provide a biometric as well as password security to the voters account. The system will make a conclusion whether the voter is correct person or not. System uses voters fingerprint image as cover image and embed voter's secret data into the image using steganography. This method produces a stego image which is equal to the original fingerprint image only. On the whole there are changes in the original fingerprint image & stego image but they are not visible by human eye.

Keywords – Biometric, Cover, Fingerprint, Online, Password, Steganography, Security

INTRODUCTION

An election is an official process by which person chooses an individual to hold all kind of public issues. The elected person should satisfy all necessary needs of common people so the system of whole country works properly. The main requirements of election system are like authentication, speed, accuracy, and safety. The voting system should be speedy so the valuable time of voters as well as the voting system conductors will be saved. Accuracy means the whole system should be accurate with respect to result. Safety involves the secure environment around the election area so that voters will not be under any force. In online voting system main aim is to concentrate the focus on security of voters account. For any type of voting system following points must be taken into consideration. This can include confusing or misleading voters about how to vote, violation of the secret ballot, ballot stuffing, tampering with voting machines, voter registration fraud, failure to validate voter residency, fraudulent tabulation of results, and use of physical force or verbal intimation at polling places. If online voting system works well then it will be a good progress over the current system. In the next section the proposed methodology, database creation & embedding the secret data, online voting system, recognition of the embedded message, & analysis of the system is explained.

PROPOSED METHODOLOGY

The methodology includes steganography with the help of biometric security. Fundamentally there are various types of steganography like text, audio, image, and video. Images are the well-liked cover media used for steganography. In many applications, the most important requirement for steganography is the security, which means that the stego image should be visually and statistically similar to their corresponding cover image strictly. Now a day's steganographic system uses images as cover object because people often send digital images by email. So using image for steganography is the good choice as all kind of emails contain at least single image. After digitalization, images contain the quantization noise which provides space to hide data.

When images are used as the cover image they are generally manipulated by changing one or more of the bits of an image. With the help of least significant bit (LSB) insertion, system hides the message. As LSB of an image contain less amount of information, individual can easily hide any personal data by replacing those bits by message bits. To work with the system each person should be provided with a PAN number (Personal Authentication Number).This is like a serial number allocated to every person. System also needs the thumb impression of all voters as a cover image. Finally at the time of account creation a secret key is given to each voter which the voter should hide from every single person.

Considering that all above data is collected from every voter the 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 thumb impression. Then the voter is asked to enter the secret key for PAN number decryption from the database embedded fingerprint 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. After giving vote the count will be incremented for that political person.

A. DATABASE CREATION & EMBEDDING PROCESS

For database creation a voter committee should be appointed. Committee member's job is to collect the data from each person. Every voter should have an account identification number to maintain the account, PAN number for voter authentication & a secret key as a password or cross verification of the database. As shown in the fig.1 finger print image block takes the fingerprint image of voter as an input. 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.

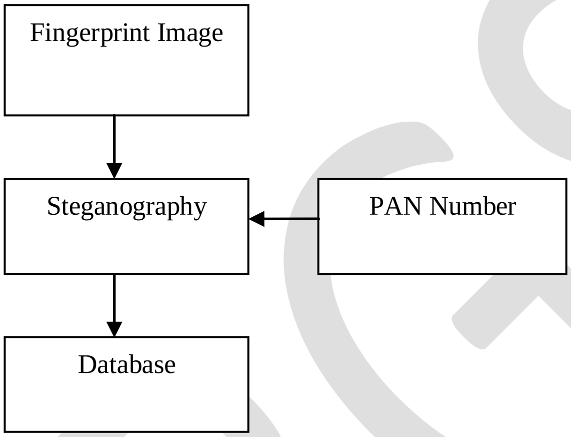

Figure.1 Block Diagram for Database Creation

The fingerprint image should be plain which will act as cover image after data hiding. So the cover image for each voter is its own fingerprint image only. Prior to the least significant bit insertion, system uses discrete wavelet transform. In discrete wavelet transform with the help of HAAR transform the fingerprint 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 fingerprint input image into four non overlapping sub bands LL, LH, HL, HH as shown in the fig.2 (a) . 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 fingerprint image after PAN number embedding is shown in fig.2 (b) as embedded image. If compared to the Fourier transform which only differs in frequency, the Haar function varies in both scale and position.

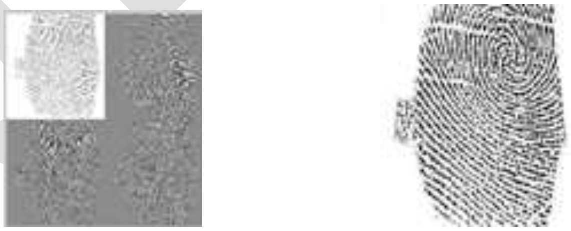

Figure.2

(a) Four Sub bands of DWT (b) 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 fingerprint 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.3 a voter is first asked for voter's account identification number so that voter's election account will be opened. Then voter is asked to give the fingerprint image followed by secret key. If the secret key is correct then the PAN number decryption & recognition is carried out with the help of discrete wavelet transform. Discrete wavelet transform is applied to the embedded fingerprint 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.

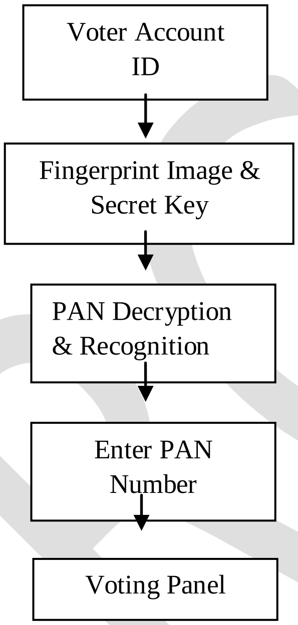

Figure.3 Online Voting System

C. RECOGNITION 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 discrete wavelet transform is applied to extract the hidden message from database image as shown in fig. 4. Principle Component Analysis is used for fingerprint recognition. Principle component analysis is a way of identifying the patterns of fingerprint image in order to highlight their similarities & differences. PCA is a useful method having use in face recognition and image compression, and for finding patterns. Thus system uses PCA for finding fingerprint patterns. PCA representation is explained by eigen values & eigen vectors. This system finds variance, covariance matrix & eigen values. To find out the above parameters one should know about the standard deviation, covariance, eigenvectors and eigen values. Variance is nothing but the amount of data extends in a data set. It is equal to the standard deviation. One can measure the covariance always between two dimensions. When we get a set of data points, we divide it into eigenvectors and eigen values. Every eigenvector has a corresponding eigen value.

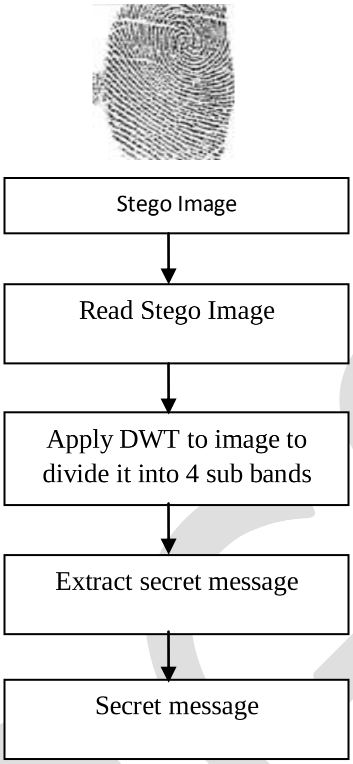

Figure.4 Block Diagram for Extraction Process

Eigen vector with the highest eigen value is therefore the principal component. Finally comparison is done to find out the match using euclidean distance. If match is found between database image & test image then the voter is authorized person.

RESULT & ANALYSIS

This system uses account identification number to maintain the voters account, fingerprint image 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. Hence no fraudulent cases such as duplicate voting.

Steganographic 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 the 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. The proposed system was applied to fingerprint 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. Where, high quality stego image reflects more invisible the hidden message. 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 its noisy approximation *K* is calculated by

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

And

$$MSE = 1/MN \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} [I(i, j) - K(i, j)]^2$$

Where MSE - Mean Square Error

The PSNR was calculated for each stego image & PSNR ranges from 30 to 50 which give reasonable visual quality of the stego image. After applying above formula one can comparatively find out the PSNR of the fingerprint images. Actual PSNR observed for fingerprint image-1 is 40.92 dB. For figure-2 its 41.45 dB, Likewise PSNR of all fingerprint images can be calculated. 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 fingerprint image from time domain to frequency domain & then manipulation of least significant bit with the help of least significant bit insertion technique. Thus frequency domain technique is better approach for hiding data.

CONCLUSION

Considering the difficulty of elections the system provides adequate proof of authenticity in terms of biometric protection as well as multilevel security. The security level of system is very much enhanced by the idea of individuals fingerprint image as cover image for each user. Fingerprint image and PAN number has been used to obtain high degree of authenticity. This methodology does not give any idea for searching predictable modifications in the cover image. Countries with large population have to invest large amount of money, time as well as man power for voting set up. But because of online voting system all the mentioned problems will be reduced to great extent.

REFERENCES:

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

[29] William Stallings, "Cryptography and Network Security Principle and Practices", Third Edition, pp. 67-68 and 317-375, Prentice Hall, 2003

[30] Sutaone, M.S. and Khandare, M.V., "Image based steanography Using LSB insertion technique", IEEE WMMN, pp. 146-151, January 2008.

[31] J.Samuel Manoharan,Dr.Kezi C.Vijila, A.Sathesh, "Performance Analysis of Spatial & Frequency Domain" (4); Issue (3)

[32] Lindsay I Smith "A tutorial on Principal Component Analysis" February 26, 2002

[33] R. EI Safy, H. H. Zayed, and A.EI Dessouki "An Adaptive Steganographic Technique Based on Integer Wavelet Transform"

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

[35] T. Morkel 1, J.H.P. Eloff 2, M.S. Olivier 3 "An Overview of Image Steganography"

[36] Yeuan-Kuen Lee and Ling-Hwei Chen "An Adaptive Image Steganographic Model Based on Minimum-Error LSB Replacement"

[37] Mehdi Kharrazi, Husrev T. Sencar, and Nasir Memon "Image Steganography: Concepts and Practice"

[38] Linu Paul, Anilkumar M.N. "Authentication for Online Voting Using Steganography and Biometrics" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 1, Issue 10, December 2012

[39] M. Sifuzzaman, M.R. Islam1 and M.Z. Ali "Application of Wavelet Transform and its Advantages
Compared to Fourier Transform"