ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 1, Issue 10, December 2012

Authentication for Online Voting Using Steganography and Biometrics

Linu Paul, Anilkumar M.N.

Abstract— **In this paper an online voting authentication technique is proposed which provides biometric as well as password security to voter accounts. Voters are first identified by their facial image by using PCA. Second step is the fingerprint recognition. Third one is steganographic method. The basic idea of strganographic method is to merge the secret key and pin number with the cover image which produces a stego image which looks same as the cover image. The cover image is a biometric measure, such as a fingerprint image. The secret key and pin number is extracted from the stego image at the server side to perform the voter authentication function. This system greatly reduces the risks as the hackers have to find the secret key, pin number, fingerprint and facial image, which makes the election procedure to be secure against a variety of fraudulent behaviors. SHA 256 used for hashing is replaced with MD5 in order to improve the speed**

***Index Terms*—Online Voting, Data hiding, Biometric, Stego image, Steganography**

I. INTRODUCTION

ELECTION enables every citizen of the country to participate in the process of government formation. The Constitution of India provides for an Election Commission of India which is responsible for superintendence direction and control of all elections. Integrity of election process will determine the integrity of democracy itself. So the election system must be secure against a variety of fraudulent behaviors and should be transparent and comprehensible that voters can accept the results of an election [3]. But, now- a -days it has become common for some forces to indulge in rigging which may eventually lead to a result contrary to the actual verdict given by the people. 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. Compared to existing voting system the Electronic voting has several advantages [3] like: Electronic voting system is capable of saving considerable printing stationery and transport of large volumes of electoral material. It is easy to transport, store, and maintain. It completely rules out the chance of invalid votes. 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. As online voting is risky, it is difficult to come up with a system which is perfect in all senses.

Least significant bit insertion is a common approach to embed information in a cover file given by [6]. Unfortunately, this process of LSB modification changes the statistical properties of the cover image, so eavesdroppers can detect the distortions in the resulting stego image. So a novel technique for Image steganography based on DWT [8], where DWT is used to transform original image (cover image) from spatial domain to frequency domain is used. It is useful to achieve confidential transmission over a public network. Proper user identification/authentication is a crucial part of the access control that makes the major building block of any system's security for which fingerprint which is a biometric measure is used. Our aim is to present a new online voting system employing biometrics in order to avoid rigging and to enhance the accuracy and speed of the process so that one can cast his vote irrespective of his location.

Biometrics is the automated recognition of individuals based on their behavioral and biological characteristics. Biometric recognition means by measuring an individual's suitable behavioral and biological characteristics in a recognition inquiry and comparing these data with the biometric reference data which had been stored during a learning procedure, the identity of a specific user is determined. Because biometric identifiers cannot be easily misplaced, forged, or shared, they are considered more reliable for person recognition than traditional token or knowledge based methods. The objectives of biometric recognition are user convenience, better security and higher efficiency. Fingerprints are unique for each finger of a person including identical twins. Face Recognition is the process of identification of a person by their facial image. These techniques makes it possible to use the fingerprint and facial images of a person to authenticate him into a secure system, So the Electronic voting system has to be improved based on the current technologies viz., biometric system. A pre requisite for authentication is enrollment, in which the biometric features are saved.

II. RELATED WORK

Electronic voting is a great improvement over paper systems. Flaws in any of these aspects of a voting system, however,

Linu Paul, *ECE Department, M.G University,, FISAT,. Angamaly , India, Mobile No:9496462843*
Anilkumar.M.N., *ECE Department, M.G University,, FISAT,. Angamaly India, Mobile No:* 9656927612

can lead to indecisive or incorrect election results. Some of the existing solutions of computerized voting systems highlighted their vulnerabilities in [5]. They include Punch Card Systems, Global Election Management System (GEMS) and Direct Recording Electronic (DRE). All these systems are standalone systems, they lack in ability of voting from anywhere. That is why the actual notion of online voting is missing in those systems.

The current remote voter registration systems face some security problems. These problems are mainly related to the inability to accurately verify the identity of the voter, which can facilitate impersonation or multiple registrations by the same voter with different data. Voter registration is conventionally carried out face to face with the registration authority. Many voters residing outside their native places during the election process are unable to cast their vote, so it has becomes necessary to have new methods to collect the voting information from the remote voters in a secure manner. In previous research only the concept of cryptography was used. Voter has to register first. After submitting the registration form the voter status will be sent to the voter will be verified with election commission server. After submitting the registration form the voter status will be sent to the voter through e-mail. Then based on the given voter information the voter will be verified with election commission server. If it is matching, then the voter will receive the identity proof through e-mail which is generated using cryptography techniques. In order to get the integrity proof it is used as a combination of SHA1 hash function and MD5 hash function. This combination is conceived with the aim of preventing collisions between the digest messages. Still there are many security problems in this concept also like denial of submission of votes due to network issues, alteration of ballots by system admin, authentication documents posed a potential threat, when the voter opens his internet ballot on his /her computer, at that point the ballot is no longer encrypted and would therefore be susceptible to manipulation by a malicious code.

III. PROPOSED METHOD

The steganographic algorithm uses image based steganographic system proposed in [4]. Biometric identity is included to provide added security. Steganography uses fingerprint as cover media because after digitalization images contain the quantization noise which provides space to embed secret data. The general model of Steganography says if you want to send some secret message then choose a cover image, find its redundant bits and replace these bits with data bits of message. The message can be easily extracted by doing the same operations on the other end.

Concept of steganography is used to achieve these criteria's of a public voting system. Image based steganography [2] is a well-known and widely used technique that manipulate information in order to cipher or hide their existence. A steganographic system thus embeds hidden content in a cover media so as not to provoke an eavesdropper's suspicion. Firstly two dimensional Discrete Wavelet Transform (2-D DWT) is performed on a gray level cover image. Image quality is to be improved by preserving the wavelet coefficients in the low frequency sub band. The experimental results show that the algorithm has a high capacity and a good invisibility. Moreover PSNR of cover image with stego-image shows the better results in comparison with other existing steganography approaches.

There are some pre-requirements are needed to support such a system. Firstly, each and every individual in the country should be provided with voter Identification Number or PIN (Personal Identification Number). This is needed for maintenance of voter accounts in the database. Secondly, we need facial images and fingerprints of all the individuals. 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. Voter can cast vote after login which is done after authenticating the voter's facial image, fingerprint, PIN number and secret key. In the database stego image made by embedding secret key and PIN is stored. Voter's fingerprints and facial images are also stored in the database.

To cast a vote, a voter logs in to the system by scanning the face and fingerprint. If authenticated by the face and fingerprint match then the voter is allowed to log in to the voting system by entering PIN number and secret key. The system will create the stego image by embedding the secret key and PIN number. Now this stego image will be sent securely to the server for voter authentication. At the server side**,** the secret key and PIN number from database stego image and voter's stego image is extracted and compared to perform the voter authentication function. Once authentication is complete, the voter will be allowed to vote. Voter can select the desired candidate and finalize the vote. After casting the vote, the account will be closed and in the database the voted bit will be set for that voter. Fig. 1.shows the basic mechanism:

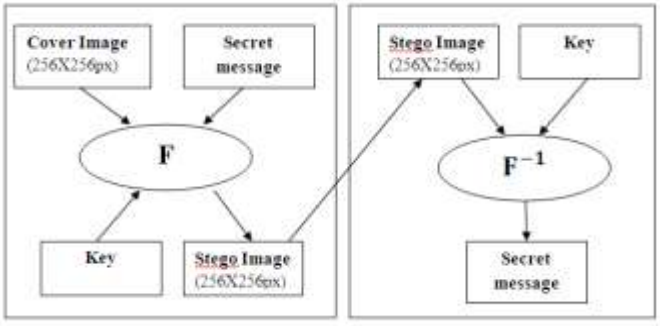

Fig.1.Sego Image creation and extraction

A. Database Creation

During the database creation every individual will be provided with a system generated Secret key and PIN number. The system will create the stego image by embedding the secret key and PIN number. Now this stego image will be stored securely in the database of server for voter authentication.

B. Generation of Secret Message

In this phase, a 192 bit secret message is created from a 16 bit secret key. Firstly, the secret key is concatenated with the 16-digit personal identification number. Now we will apply MD5 algorithm [1] to get a 128 bit hash code for that key. It is again concatenated with the PIN to get the secret

message. As the actual secret key is never embedded in the stego image, there will be no chance of predicting secret key from it. The mechanism is shown in Fig. 2:

C. Key Expansion Using Hashing

The secret key is very important in the case of online voting. It cannot be compromised in any condition. As the system is designed for general public, there is a limitation with the secret key. It should be short enough to be remembered by every voter. This 4-digit PIN can easily be represented using 2 bytes. But 2 byte data looks seems to be vulnerable in terms of length. The eavesdroppers will never be able to deduce that some data is hidden in the image. But if they know that it is a stego image, they can easily extract the PIN. In order to increase the complexity of analysis, the 2 byte secret key is expanded by applying MD5 hashing algorithm [1] to get 192 bits secret message. When the secret message is embedded in the cover image, the stego image will remain more complex to be analyzed .So, even if eavesdroppers know that this is a stego image, it would be more difficult for them to predict the embedded data.

D. Discrete Wavelet Transform (DWT)

DWT applies on the cover image. Generally wavelet domain allows us to hide data in regions that the human visual system (HVS) is less sensitive to, such as the high resolution detail bands (HL, LH and HH), Hiding data in these regions allow us to increase the robustness while maintaining good visual quality. In discrete wavelet transform, the used wavelet filters have floating point coefficients.

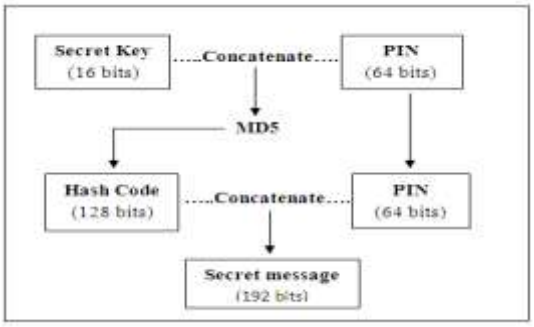

Fig.2. Secret message creation

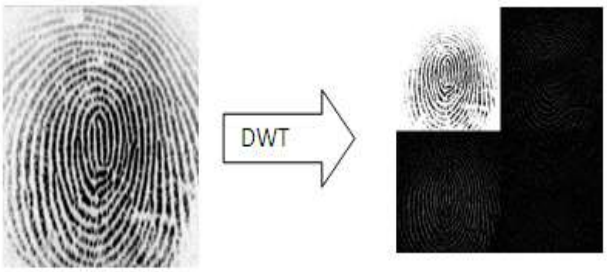

Fig. 3.Conversion of image into 4 frequency sub bands using DWT.

DWT offers better energy compaction than DCT without any blocking artifact. DWT splits component into numerous frequency bands called sub bands known as

LL – Horizontally and vertically low pass
LH – Horizontally low pass and vertically high pass
HL – Horizontally high pass and vertically low pass
HH – Horizontally and vertically high pass

Since Human eyes are much more sensitive to the low frequency part (LL sub band) we can hide secret message in other three parts without making any alteration in LL sub band [8]. As other three sub-bands are high frequency sub-band they contain insignificant data. Hiding secret data in these sub-bands doesn't degrade image quality that much. DWT used in this work is Haar-DWT, the simplest DWT. Fig. 3. shows the four frequency sub bands.

E. Face Recognition

Face recognition is one of the important challenges in appearance-based pattern recognition field [10]. One of the most popular algorithms is principal component analysis (PCA). Each image is treated as one vector. All images of the training set are stored in a single matrix T and each row in the matrix represents an image. The average image has to be calculated and then subtracted from each original image in T. Then calculate the eigenvectors and eigenvalues of the covariance matrix S. These eigenvectors are called eigenfaces.

The eigenfaces is the result of the reduction in dimensions which removes the unuseful information and decomposes the face structure into the uncorrelated components (eigenfaces).Each image may be represented as a weighted sum of the eigenfaces. A probe image is then compared against the gallery by measuring the distance between their represent vectors. Face recognition aims to decompose face images into small set of characteristic feature images called eigenfaces which used to represent both existing and new faces [9]. The training database consists of M images which is same size.The images are normalized by converting each image matrix to equivalent image vector Γi; the training set matrix Γ is the set of image vectors with

$$\text{Training set } \Gamma=[\Gamma_1\ \Gamma_2\ \Gamma_3 \dots\dots\dots \Gamma_M] \quad (1)$$

The mean face (Ψ) is the arithmetic average vector given by:

$$\Psi = \frac{1}{M}\Sigma_{i=1}^{M}\Gamma_i \quad (2)$$

The deviation vector for each image Φ_i is given by:

$$\Phi_i = \Gamma_i - \Psi \qquad i = 1,2,3\dots..M \quad (3)$$

Consider a difference matrix A= [$\Phi_1, \Phi_2 \dots\dots \Phi_M$] which keeps only the distinguishing features for face images and removes the common features. Then eigenfaces are calculated by find the Covariance matrix C of the training image vectors by:

$$C = A.A^T \quad (4)$$

Due to large dimension of matrix C, we consider matrix L of size (Mt X Mt). The eigenvectors of C (Matrix U) can be obtained by using the eigenvectors of L (Matrix V) as given by:

$$U_i = AV_i \quad (5)$$

The eigenfasecs are:

$$\text{eigenface} = [U1, U2, U3, \ldots\ldots UM] \quad (6)$$

Instead of using M eigenfaces, the highest m' <= M is chosen as the eigenspace. Then the weight of each eigenvector ω_i to represent the image in the eigenface space, as given by:

$$\omega_i = U_i^T(\Gamma - \Psi) \quad i=1,2,3\ldots\ldots m' \quad (7)$$

$$\text{Weight matrix } \Omega = [\omega 1, \omega 2 \ldots. \omega\ m' \ ]^T \quad (8)$$

$$\text{Average class projection } \Omega_\Psi = \frac{1}{x_i}\Sigma_i^{x_i}\Omega_i \quad (9)$$

The Euclidean distance δ_i(8) is used to find out the distance between two face keys vectors and is given by:

$$\delta_i = \| \ \Omega - \ \Omega_{\Psi_i} \| \quad (10)$$

The smallest distance is considered to be the face match score result. Fig.4.shows some faces used in the experiment.

Face Recognition is the process of identification of a person by their facial image. This technique makes it possible to use the facial images of a person to authenticate him into a secure system. Principal Component Analysis (PCA) is a dimensionality reduction technique based on extracting the desired number of principal components of the multi-dimensional data.

In this phase face image of the voter is captured by a good quality camera and sent to the server to get the face recognition.

Steps are

1. Consider a real time face image
2. Calculate the mean
3. Calculate the deviation from the mean (X)
4. Find the covariance matrix, C=X X^T
5. Find the eigenvectors and eigen values of the covariance matrix
6. Calculate eigenvalues greater than the threshold(e-3)
7. Repeat the steps 2 , 3 ,4 , 5 , 6 for a set of images in the Data Base
8. Find the Euclidean distance B/W real time image and each images in the database
9. Arrange the Euclidean distance in the descending order
10. 10.If the 1st value is 0 (anyone image in the database is matched with the real time image)then the face is recognized

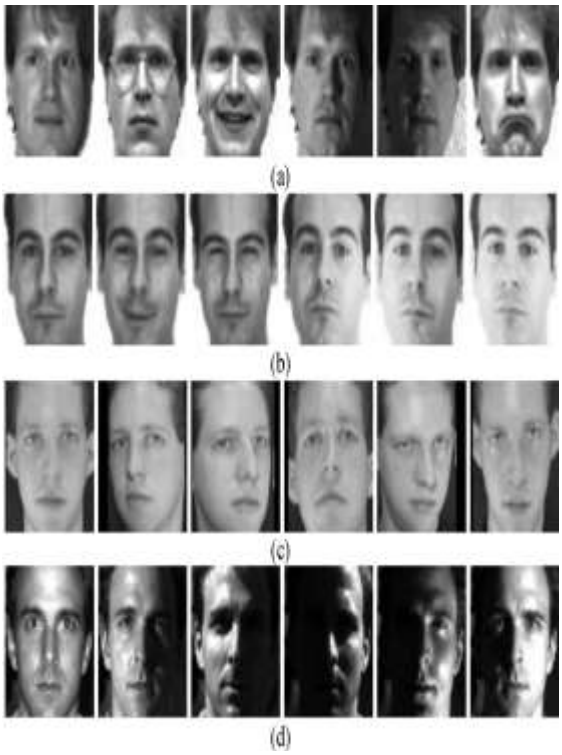

Fig.4. Some cropped faces used: (a) Images from the Yale database; (b) images from the AR database; (c) images from the ORL database and (d) images from the YaleB database.

F. Embedding Process

The block diagram of the embedding procedure is shown in Fig.5.

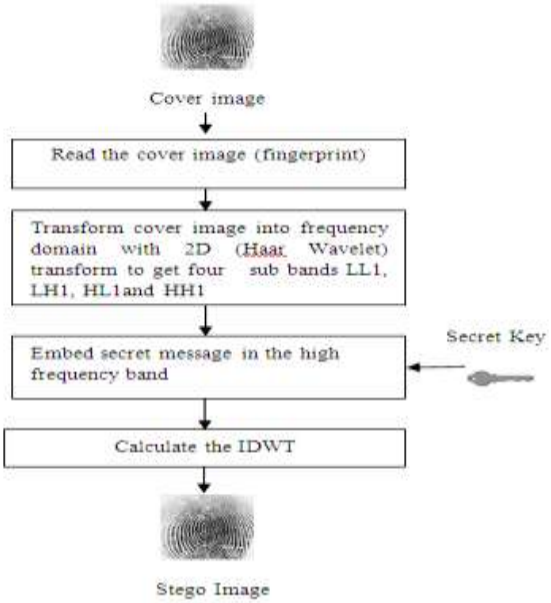

Fig. 5.Blockdiagram of Embedding Process

G. Extraction Process

At the server, uses the extraction algorithm to obtain the secret message. The block diagram of the extraction algorithm is shown in Fig. 6.

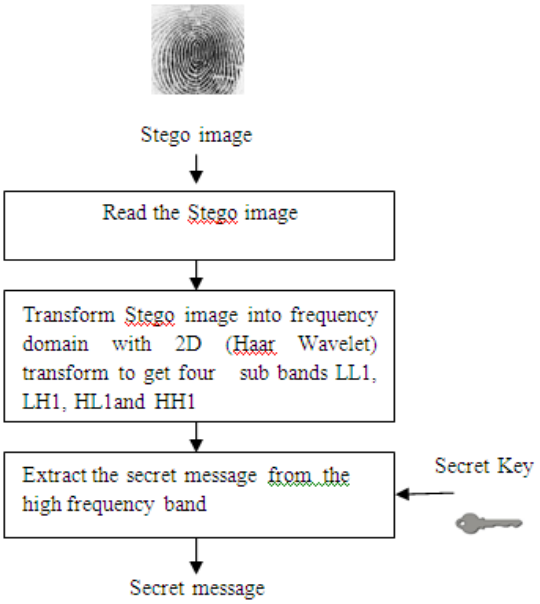

Fig. 6.Blockdiagram of Extraction Process

H. Fingerprint recognition

Fingerprint-based identification [11] is one of the most important biometric technologies which have drawn a substantial amount of attention recently. Humans have used fingerprints for personal identification for centuries and the validity of fingerprint identification has been well established. In fact, fingerprint technology is so common in personal identification that it has almost become the synonym of biometrics. Fingerprints are believed to be unique across individuals and across fingers of same individual. Even identical twins having similar DNA, are believed to have different fingerprints. These observations have led to the increased use of automatic fingerprint based identification in both civilian and law-enforcement applications.

A fingerprint is the pattern of ridges and furrows on the surface of a fingertip. Ridges and valleys are often run in parallel and sometimes they bifurcate and sometimes they terminate. When fingerprint image is analyzed at global level, the fingerprint pattern exhibits one or more regions where ridge lines assume distinctive shapes. These shapes are characterized by high curvature, terminations, bifurcations, cross-over etc. These regions are called singular regions or singularities. These singularities may be classified into three topologies; loop, delta and whorl. At local level, there are other important features known as minutiae can be found in the fingerprint patterns. Minutiae mean small details and this refers to the various ways that the ridges can be discontinuous. A ridge can suddenly come to an end which is called termination or it can divide into two ridges which is called bifurcations which is shown in Fig.7

The system first detects the core point in a fingerprint image. Core point is defined as the north most point of inner-most ridge line. A circular region around the core point is located and tessellated into 128 sectors. The pixel intensities in each sector are normalized to a constant mean and variance. The circular region is filtered using a Gabor filter to produce a filtered image.

Fig.7. Ridge ending, core point and ridge bifurcation

Gabor filter is a well known technique to capture useful information in specific band pass channels. The average absolute deviation with in a sector quantifies the underlying ridge structure and is used as a feature. The feature vector is the collection of all the features, computed from all the 128 sectors, in every filtered image. The feature vector captures the local information and the ordered enumeration of the tessellation captures the invariant global relationships among the local patterns. The matching stage computes the Euclidean distance between the two corresponding feature vectors.

Gabor filters optimally capture both local orientation and frequency information from a fingerprint image. By tuning a Gabor filter to specific frequency and direction, the local frequency and orientation information can be obtained. Thus; they are suited for extracting texture information from images. An even symmetric Gabor filter has the following general form in the spatial domain:

$$G(x, y; f, \theta) = exp\left\{-1\left|2\left[\frac{x'^2}{\delta_{x'}^2} + \frac{y'^2}{\delta_{y'}^2}\right]\right\}\cos(2\pi f x')$$

$$x' = x\sin\theta + y\cos\theta$$
$$y' = x\cos\theta - y\sin\theta$$

Where f is the frequency of the sinusoidal plane wave along the direction θ from the x-axis, and δx and δy are the space constants of the Gaussian envelope along x and y axes, respectively. The filtering is performed in the spatial domain. The frequency f is the average ridge frequency (1/K), where K is the average inter ridge distance. The average inter ridge distance is approximately 10 pixels in a 500 dpi fingerprint image. Hence, f = 1/10. Sixteen different orientations are examined. These correspond to θ values of 0, 11.25, 22.5, 33.75, 45, 56.25, 67.5, 78.75, 90, 101.25, 112.5, 123.75, 135, 146.25, 157.5 and 168.75 degrees. The values for x' δ and y' δ

were empirically determined and each is set to 4 (about half the average inter ridge distance).

The steps are

1. Consider a real time fingerprint image
2. Find the central point
3. Crop the fingerprint image
4. Normalize the cropped print
5. Apply Gabor filtering
6. Find the mean value of the image
7. Repeat the steps 2,3,4,5 for each images stored in the Database.
8. Find the Euclidean distance B/W mean value of real time image and each images in the database
9. Arrange the Euclidean distance in the descending order.
10. If the 1st value is 0 (anyone image in the database is matched with the real time image) then the fingerprint is recognized.

I. *Voter Account Maintenance*

Once a voter passes the authenticity criteria, he/she will be logged into his/her voting account. Voters are restricted from logging into his/her voting account more than once during elections. Once a particular voter is authenticated by the system, a secure channel will be established using https and then he/she will be allowed to casting the vote. The vote will remain secret in every sense, i.e., it will not be reflected anywhere in the database that which user has voted for whom. Finally, the account will be closed and that user will not be able to log back in by any means again. This completes the voting process. The authentication mechanism makes use of both, biometric measures as well as secret key. If any of these properties are tempered by any individual, it can be easily detected and the request will be rejected from the server side.

ANALYSIS

A. *Steganographic Performance*

The main aim of steganography is to hide secret message into a cover, so that the presence of hidden data cannot be identified. Here we have used DWT based steganography, in which the secret data is embedded in the high frequency band. Because the eye cannot detect the very small perturbations it introduces into an image and simple to implement. In this algorithm, the secret message is fewer bits in length than the number of pixels in the cover. More is the number of bits modified; more will be the change in the statistical properties of any image [7]. Database stego creation of each voter needs 6-7 sec.

Any processing applied to an image may cause an important loss of information or quality. Image quality evaluation methods can be subdivided into objective and subjective methods. Subjective methods are based on human judgment and operate without reference to explicit criteria. Objective methods are based on comparisons using explicit numerical criteria, and several references are possible such as the ground truth or prior knowledge expressed in terms of statistical parameters and tests. Stego-image quality measures how much difference (distortion) was caused by data hiding in the original cover, where the higher the stego-image quality, the more invisible the hidden message. We can judge the stego-image quality by using Peak Signal to Noise Ratio (PSNR). The PSNR for an image of size MxN is calculated by (11)

$$PSNR = 10\ log_{10}\left(\frac{255^2}{MSE}\right) \quad (11)$$

and

$$MSE = \left(\frac{1}{M \times N}\right) \Sigma_{x=1}^{M} \Sigma_{y=1}^{N} (p(x,y) - p'(x,y))^2 \quad (12)$$

The MSE is the Mean Square Error, P(x, y) stands for the image pixel value in the cover image and P'(x, y) is for the pixel value at position (x, in the image after inserting secret message. A high value of PSNR means better image quality (less distortion), it is recorded that in grayscale images that the human visual system (HVS) cannot detect any distortions in stego-images having PSNR that goes beyond 36 dB. The proposed system has PSNR that goes beyond 180 dB. The PSNR value approaches infinity as the MSE approaches zero; this shows that a higher PSNR value provides a higher image quality.

The number of bits that can be hidden in cover image is known as the data-hiding capacity. Here modifying only 0.0366 percent of bits available in the cover image making it difficult to be detected as steganographic one. So, from the steganographic perspective, the whole system is having better security.

The SHA algorithm previously used is replaced with MD5 algorithm in order to improve the speed as well as security of the existing system.

B. *Biometric Performance*

Principal component analysis (PCA), also known as Karhunen- Loeve expansion, is a classical feature extraction and data representation technique widely used in the areas of pattern recognition and computer vision. PCA efficiently represent pictures of human faces. Any face image could be reconstructed approximately as a weighted sum of a small collection of images that define a facial basis (eigenimages), and a mean image of the face. PCA has been widely investigated and has become one of the most successful approaches in face recognition. The proposed face recognition method was used three well-known face image databases (ORL, AR, and Yale).Database contains images from 8 individuals, each providing 10 different images.Face recognition of each voter needs 10-13 sec

Fingerprint matching is based on finding the Euclidean distance between the corresponding feature vectors. This minimum score corresponds to the best alignment of the two fingerprints being matched. If the Euclidean distance between two feature vectors is less than a threshold, then the decision that "the two images come from the same finger" is made, otherwise a decision that "the two images come from different fingers" is made. Since the template generation for storage in the database is an off-line process, the verification time still depends on the time taken to generate a single template. Database of fingerprint images contains 10 images. Fingerprint recognition of each voter needs 8-9 sec

CONCLUSION

Considering the complexity of elections here provided sufficient proof of authenticity of an individual in form of both biometric measures and secret key. Facial image and fingerprint has been used to gain a higher level of authenticity for security systems with high degree of accuracy and reliability. Hence such a system can be designed to protect the high security systems against hacking and cracking. MD5 algorithm enhances the performance and security aspect of the system. This strategy does not give any opportunity to steganalytic tools of searching for a predictable set of modifications. Voting time for each voter is more, so a large population needs more time to complete the voting. As future work, we will be trying to improve considerable aspects of the algorithm which is speed. As a future work, multi-biometrics measure can also be used to implement online voting system.

REFERENCES

[1] William Stallings, *"Cryptography and Network Security, Principles and Practices"*, Third Edition, pp. 67-68 and 317-375,Prentice Hall 2003
[2] Kharrazi, M., Sencar, H. T., and Memon, N., "*Image steganography:Concepts and practice*", In WSPC Lecture Notes Series,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.html
[4] Bloisi, D. and Iocchi, L., "*Image based Steganography and Cryptography*", In Proc. of 2nd Int. Conf. on Computer VisionTheory and Applications (VISAPP), pp. 127-134, 2007.
[5] Armen, C. and Morelli, R., "*E-Voting and Computer Science: Teaching About the Risks of Electronic Voting Technology"*, ACM ITiCSE, 2005.
[6] Sutaone, M.S. and Khandare, M.V., *"Image based steganography using LSB insertion technique"*, IEEE WMMN, pp.146-151, January 2008
[7] Provos, N. and Honeyman, P., "*Hide and seek: An introduction to steganography*", IEEE Security and Privacy, 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] M. Turk, A. Pentland, Eigenfaces for Recognition, Journal of Cognitive Neurosicence, Vol. 3, No. 1,1991, pp. 71-86
[10] Ibrahim, R.; Zin, Z.M., "Study of automated face recognition system for office door access control application," *Communication Software and Networks (ICCSN), 2011 IEEE 3rd InternationalConference*, vol., no., pp.132-136, 27-29 May 2011
[11] A. K. Jain, A. Ross, and S. Prabhakar, "Fingerprint Matching Using Minutiae and Texture Features", *Proc International Conference on Image Processing (ICIP)*, pp. 282-285, Greece, October 7-10, 2001.

.

Linu Paul is an M.tech final year student of Communication Engineering in Federal Institute of Science and Technology, Ernakulam affiliated to Mahathma Gandhi University. Her current research interest is Steganography and Cryptography. She received her B.Tech in Electronics and Communication Engineering from MET'S School of Engineering,Thrissur affiliated to calicut university.

Anilkumar M.N is an Assistant Professor at Department of electronics and Communication Engineering, in Federal Institute of Science and Technology,Ernakulam affiliated to Mahatma Gandhi University. He has teaching experience of more than 15 years to graduate and postgraduates. His research areas include Cryptography, Steganography and Digital Watermarking.