Evidence based Access Control over Web Services using Multi Security

E. S. Shameem Sulthana
Research Scholar, Bharathiar University
Coimbatore, Tamilnadu, India.

Dr.S.Kanmani
Professor & Head in Dept. of IT
PEC, Pondicherry, India.

ABSTRACT
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.

Keywords - E-voting, Steganography, Evidence, Security, Web Services.

1. INTRODUCTION
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 are residing outside of their native places during the election process, it has been necessary to have new methods to collect, remotely and in a secure manner, the information of such voters.

In our previous research we have implemented the concept of cryptography. The voter has to register first. 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. The latest is used in its MAC (Media Access Control) implementation. This combination is conceived with the aim of preventing collisions between the digest messages. There are many security problems arises in this concept. So, in this paper we have proposed a system for voting can be done through internet with the concept of Steganography and biometrics. Steganography is the idea of hiding private or sensitive data or information within something that appears to be nothing out of the normal [1]. Steganography and cryptology are similar in the way that they both are used to protect important information. The difference between the two is that Steganography involves hiding information so it appears that no information is hidden at all. If a person views the digital object that the information is hidden inside, he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information, this is the main objective behind Steganography. Steganography comes from the Greek words Steganós (Covered) and Graptos (Writing), these days the sense of the word "Steganography" usually refers to information or a file that has been concealed inside a digital Picture, Video or Audio file [2]. What Steganography technically does is to make use of human awareness; human senses are not trained to look for files that have information hidden inside of them. An Automatic key is also generated by using cryptographic algorithm and efficient key management in critical wireless networks. Research in information hiding has tremendous increased during the past decade with commercial interests driving the field. An Automatic key is also generated by using cryptographic RSA algorithm with efficient key management in critical wireless networks. Depending on the application context, a biometric system may operate either in verification mode or identification mode.

Voter registration is the process of collecting the voters' data in order to constitute an electoral roll. Most of the proposals have been focused in voting and tallying stages, giving least interest to voter registration stage. In this paper we propose a remote voter registration scheme, in which biometric systems play an important role to protect the accuracy of the electoral roll. Biometric systems have been already considered in electronic voting in the voting phase, e.g. [3].

2. PROBLEMS IDENTIFIED IN CURRENT REMOTE VOTING SYSTEMS.

The contents of the registration form can be altered after the voter has sent this form. The problem identified in handwritten signature is that, it is not bound to the contents of the register. Therefore, the following problems may occur in the current remote voting system.

- Accuracy in validating the voter identity
- Prevention of multiple registers by voters
- Integrity of voter registration information

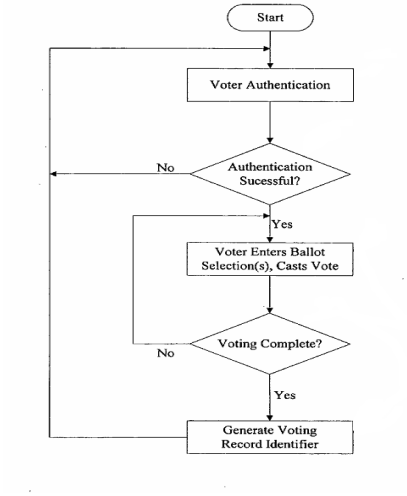


Figure-1 Existing Voting Process Using Biometric System

Figure-1 shows the existing voting process using biometric. To increase the accuracy of remote registration process, we propose the combination of biometric systems and steganographic functions. In our proposed system the section 4 will describe the proposed model, section 5 will describe how to implement the proposed work of steganography, section 6 shows the implementation part proposed work of biometric, section7 results & discussions, and section 8 gives the conclusion and future work.

3. GENERAL STEGANOGRAPHY FRAMEWORK

A general Steganography framework is shown in Figure-2. It is assumed that the sender wishes to send via Steganographic transmission, a message to a receiver. The sender starts with a cover message, which is an input to the steago-system, in which the embedded message will be hidden. The hidden message is called the embedded message. A Steganographic algorithm combines the cover massage with the embedded message, which is something to be hidden in the cover. The algorithm may, or may not, use a Steganographic key (stego key), which is additional secret data that may be needed in the hidden process. The same key (or related one) is usually needed to extract the embedded massage again.

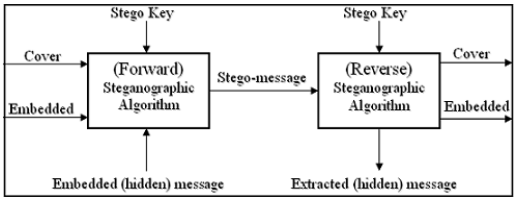


Figure-2 General Steganography Framework

The output of the Steganographic algorithm is the steago message. The cover massage and steago message must be of the same data type, but the embedded message may be of another data type. The receiver reverses the embedding process to extract the embedded message.

4. PROPOSED SYSTEM

In our proposed system we have developed a web site using ASP.NET and in that we have given the registration option to the voter. The voter must fill up the registration form and then automatically the webcam will be switched on and the voters face will be captured. The voter should also put their finger print in registration process itself. The details of the voter are sent to the election commission server.

Figure-3 E-voting system

Here, information hiding is very important. So, we have introduced a concept of Steganography to provide more security to the data. The term hiding here can refer to either making the information undetectable or keeping the existence of the information secret. Information hiding is a technique of hiding secret using redundant cover data such as images, audios, movies, documents, etc. This technique has recently become important in a number of application areas [7]. The biometric concepts are implemented using ASP.NET. The biometric evidence is received through the web cam [4]. The Steganography algorithm is implemented using JAVA programs.

5. IMPLEMENTATION OF THE PROPOSED MODEL

As a result, this paper briefly addresses following problems of substitution techniques of audio Steganography [5, 6]:

- **Transparency-** evaluates the audible distortion due to signal modification like message embedding or attacking.
- **Robustness-** measures the ability of embedded data to withstand against intentional and unintentional attacks.
- **Capacity-** refers to the ability of a cover media to store secret date, and it can be measured by the amount of secret data (bytes) that can be hidden in a byte of a cover media.

Problem 1: Having low robustness against attacks which try to reveal the hidden message. As we know in samples LSBs are more suspicious, thus embedding in the bits other than LSBs could be helpful to increase the robustness.

Problem 2: Having low robustness against distortions with high average power.

The Solution

Accordingly, there are two following solutions for mentioned problems:

1) *The solution for first problem:* Making more difficult discovering which bites are embedded by modifying the bits else than LSBs in samples, and selecting the samples to modify privately-not all samples.

2) *The solution for second problem:* Embedding the message bits in deeper layers and other bits alteration to decrease the amount of the error.

To integrate these two solutions, "embedding the message bits in deeper layers" that is a part of second solution also can satisfy "modifying the bits else than LSBs in samples" of second solution [10]. In addition, when we try to satisfy "other bits alteration to decrease the amount of the error" of second solution, if we ignore the samples which are not adjustable, also "selecting not all samples" of first solution will be satisfied. Thus, intelligent algorithm will try to embed the message bits in the deeper layers of samples and alter other bits to decrease the error and if alteration is not possible for any samples it will ignore them.

5.1. ALGORITHMIC APPROACH

A. Alteration

At the first step, message bits substitute with the target bits of samples. Target bits are those bits which place at the layer that we want to alter. This is done by a simple substitution that does not need adjustability of result be measured.

B. Modification

In fact this step is the most important and essential part of algorithm. All results and achievements that we expect are depending on this step. In this stage algorithm tries to decrease the amount of error and improve the transparency. For doing this World Academy of Science, Engineering and Technology 54 2009 362 stage, two different algorithms will be used.

One of them that are more simple likes to ordinary techniques, but in aspect of perspicacity will be more efficient to modify the bits of samples better. Since transparency is simply the difference between original sample and modified sample, with a more intelligent algorithm, I will try to modify and adjust more bits and samples than some previous algorithms. If we can decrease the difference of them, transparency will be improved.

There are two example of adjusting for expected intelligent algorithm below.

Sample bits are: 001**0**1111 = 47
Target layer is 5, and message bit is 1
Without adjusting: 001**1**1111 = 63 (difference is 16)
After adjusting: 001**1**0000 = 48 (difference will be 1 for 1 bit embedding)
Sample bits are: 001**00**111 = 39
Target layers are 4&5, and message bits are 11
Without adjusting: 001**11**111 = 63 (difference is 24)
After adjusting: 000**11**111 = 31 (difference will be 8 for 2 bits embedding)

It is clear, the most transparent sample pattern should be measured fittest. It must be considered that in *crossover* and *mutation* the place of target bit should not be changed.

C. Verification

In fact this stage is quality controller. What the algorithm could do has been done, and now the outcome must be verified. If the difference between
original sample and new sample is attachable and reasonable, the new sample will be accepted; otherwise it will be rejected and original sample will be used in reconstructing the new audio file instead of that.

D. Reconstruction

The last step is new audio file (steago file) creation. This is done sample by sample. There are two states at the input of this step. Either modified sample is input or the original sample that is the same with host audio file. It is why we can claim the algorithm does not alter all samples or predictable samples. Using the proposed algorithm, message bits could be embedded into multiple, vague and deeper layers to achieve higher capacity and robustness [8].

5.2. PROPOSED ALGORITHM FOR STEGANOGRAPHY

Step1: Read the information from the file and encrypt the message through the public or private key.
Step2: Read the image file and Compress the image by the Quantizing technique.
Step3: Compute the threshold (T), based on average gray value and place the key information in the Image where value>T.
Step4: Send through internet to the Destination and Decompress image and extract key information.

Using this algorithm the data can be hidden in the deeper layers of samples and alter other bits to decrease the error and if alteration is not possible for any samples it will ignore them. The data should not be hidden in LSB bits. The hackers will mostly search the data in LSB bits. So, the Steganography algorithm will help to store the data into the darkest area of the image which is consider as a removal part of the image. Often the storing of data pattern should be changed as image, text, audio or video bit [5, 6].

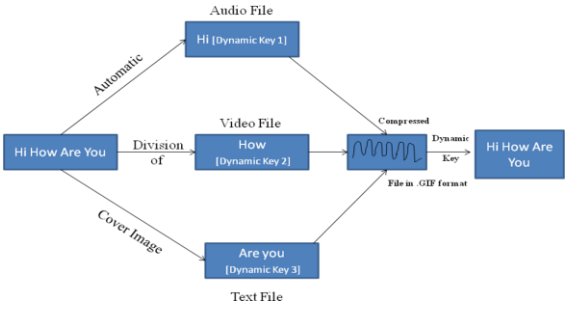
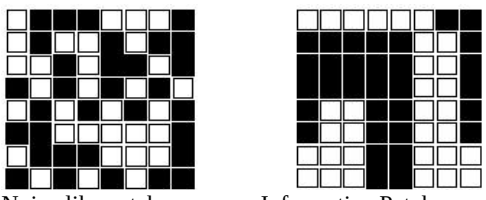


Figure-4 Transmission of Data

There are many number of voters can be registered. So, to accommodate them in our database we have taken only one bit pattern from their face or finger print based on the concept of interoperability. The details of the patterns of the voter can be stored in database. If the voter is already registered the system will shows the message that "Voter is already registered". So, the duplication of the voter information can be avoided. Then based on the given voter information the voter will be verified through our algorithm and with election commission server. If it is matching, then the voter details can be displayed on the screen. In server side system the admin can take care of the verification.

5.3. BIT PLANE COMPLEXITY SEGMENTATION STEGANOGRAPHY

When an image is decomposed into bit-planes, the complexity of each region can be measured. Areas of low complexity such as homogenous color or simple shapes appear as uniform areas with very few changes between one and zero [12, 13].



Noise-like patch Informative Patch

Figure-5 BPCS Patterns of Data

Complex areas would appear as noise-like regions with many changes between one and zero. These random seeming regions in each bit-plane can then be replaced with hidden data, which is ideally also noise-like. Because it is difficult for the human eye to distinguish differences between the two noise-like areas, we are able to disguise the changes to the image. In BPCS Steganography, a complexity measure is introduced to decide whether a binary image is noise-like or not. The complexity measure currently used is defined based on the length of non-edge border between zero and one.

The main goal of our proposed system is to build a system program that is able to hide data in digital video files, more specifically in the images or frames extracted from the digital video file MPEG [11, 16]. The main function of the proposed approach is:

--Read Frames.
--Select Frame.
--Hidden the Data.
--Read Frames Sequence.
--Extract the Data

5.4. SECURE TRANFERRING OF INFORMATION OF IMPLEMENTATION APPROACH

The compressed method of embedding the data into various cover media plays a major role in transferring the data in the network. The users need not to choose the cover media in which the data is to be hidden [9]. Choice of cover media is automatically done with dynamic allocation. Each and every transaction the cover media changes according to the data.

1) First the information's are sub divided into either by row are column in three different parts.

2) Then verify the pervious allocation process and maintain a clear path that the same cover media will not be chosen in the same order.

3) After this process Dynamic will be generated for each and every cover media.

4) This key is based upon the Cryptographic method of assignment. According to this three key will be generated, but these keys are compressed into single by using efficient key allocation in the critical networks.

5) This key will placed as a header for the packet of compressed information of audio, video and text files.

6) These files may save in the format .gif extension. After this packet reached to the receiver the

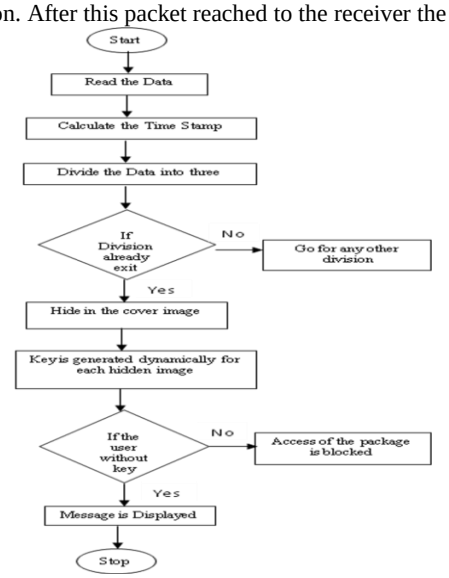


Figure-6 Implementation Approach

header check with the dynamic key if it matches, then efficient private key is generated at the moment to the receiver to decrypt the encrypted information.

6. IMPLEMENTATION OF PROPOSED MODEL FOR BIOMTERIC SYSTEM

6.1. Biometric System Design

The voter registration systems may use biometrics system. Registration module verifies some physical characteristics that uniquely identify the voter. In our proposed system the biometric system is used to help registration officers to improve the accuracy of voter identification [14]. Biometric systems are electronic systems specialized on identifying a user by means of processing unique physiological or behavioral characteristic of the user.

6.2. Face Detection System

In our proposal the biometric characteristics will fulfill all the biometric requirements. The proposed system is implemented based on the following steps to detect the face of the voter.

(i). Capture the image of the voter.
(ii). Load the face image of the voter in the system.
(iii). Read and resize the image.
(iv).Obtaining RGB and height and width of the image.

By using the geometry approach algorithm the voter face has been detected based on various factors.

(a). Lighting Compensation and Standardization.
(b). Extract Skin
(c).Setting up a threshold value skin value
(d). Skin with noise removal
(e). Find skin color blocks
(f). Check face criterions & (g). Face Detected

In our analysis, we considered an additional requirement for remote voter registration when the biometric system must be remotely available for most of the voters.

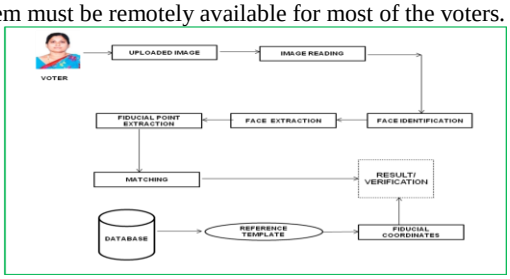


Figure-7 Biometric System Design

This reduces the number of potential candidates to face biometrics, since these allow biometric information to be acquired by means of capturing the face and combine it with the steganography. Face detection system provides non-intrusive way of authentication.

7. RESULTS AND DISCUSSIONS

From our previous research we found that the hashing algorithm is providing low security to the web services. And also the content binding is time consumption. So, we have focused our research direction towards steganography [15].

7.1. Accuracy on Biometric System

Biometrics systems are classified based on the unique characteristic of the user that is used for the identification. Using pre-existing biometric systems comparative analysis and taking finger print biometrics as reference, the proposed biometrics systems fulfill the requirements. However, as we explained in the definition of our proposal, fingerprints do not give any advantage over the current solutions on remote voter registration.

Figure-8 Registration Process

The values for face have been obtained by using a capturing and storing the images in database [17, 18]. This proposed system will protect from alterations the contents of the voter registration information by binding such information to the voter information.

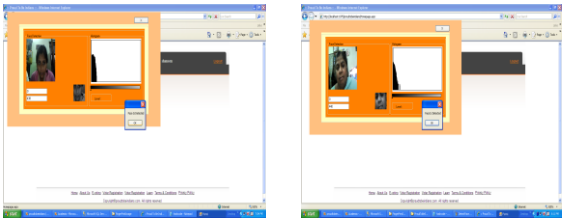


Figure - 9 Face Detection of Approved Voter

The proposed biometric system will provide the highest level of accuracy in remote voting system.

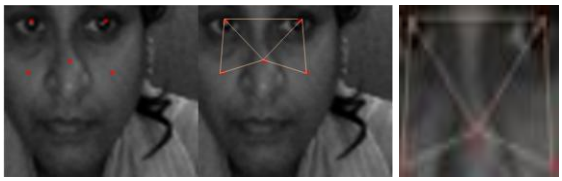


Figure-10 Fiducial Point Extraction

That means a biometric characteristic that can give at the same time both authentication and integrity to the contents.

Figure-11 Detected images with Fiducial Extraction

The figure-11 shows the detected images which is fiducially extracted.

7.2. Generation and Validation of a Registration Proof

Based on the previous analysis, we use a face biometric system. Table-1 shows the comparison between biometric characteristics. The voter carries out a communication with the Validation Module. This communication is done by means of Web camera. Then the voter is asked to give their evidence.

Biometrics	Univers	Unique	Perman	Collect	Perfor	Accepta	Robust	Content Binding
Fingerprint	H	H	H	M	H	M	M	NO
Signature off-line	M	M	L	H	L	H	L	NO
Handwriting	M	M	L	H	L	H	L	NO
Voice	H	M	M	H	M	H	L	NO
Face	H	H	M	H	H	M	H	NO
Face and Cryptography	H	H	M	M	L	L	H	YES
Face and Steganography	H	H	H	M	H	H	H	YES

Table-1 Comparison between biometric characteristics.

The registration proof is then stored by the Validation Module. The validation process facilitates the detection of people who attempt to create more than one record. Therefore, the probability of impersonation is low in our proposed system. Every biometric system will face the FRR (False Reject Rate) and FAR (False Accept Rate).

	False Reject Rate	False Accept Rate
Fingerprint[1]	0.20%	0.20%
Voice[2]	10-20%	2-5%
Face[3]	10%	1%
Face & Cryptography[4]	**10%**	**2%**
Face & Steganography[5]	**20%**	**5%**

Table-2 Comparison of different biometric system

The table-2 shows the comparison of FRR and FAR of different and proposed biometric system [17].

False Reject Rate (FRR). One of the problems that can occur are so called false rejects. A false reject is the situation where a valid user tries to authenticate and is falsely rejected by the system (see Table 2).

False Accept Rate (FAR). The second type of error a biometric system is doomed to make is false accept. In contrast to false rejects, a false accepts means that a user is successfully accepted (authenticated) even though he/she should have been rejected. In an e-Voting system there are actually two scenarios where we have to talk about false accepts (Table 2).

(i) An unauthorized user is erroneously accepted for a vote.

(ii) An authorized user is confounded with another valid user.

If a biometric device is used as an access control mechanism, a false reject may be acceptable, as it may only require the user to use a different means of authentication. In the context of e-Voting, a false reject means to deny an individual of the possibility to execute his/her right as a citizen. From our proposed system it is proven that the e-voting process is very easy to access and it provides the highest level of security.

8. CONCLUSION

In our previous research we determine the algorithm with hash key to do the content binding with the biometric. But, the security level for web services is very low. So, in this paper

we proposed the use of steganography with biometrics systems to increase the voter identification accuracy of voters that make a remote registration. Previous work on Steganography capacity was based on information and communication theoretic consideration, which are also very valid when considering an active warden to manipulate the image. In this paper we implemented an embedded method of scattering the data randomly to the audio files, video files and text files. This embedding method can be well achieved by the dynamic allocation of key by using cryptographic algorithm. If third party tries to hack the compressed stego-packets they have to compute three type of tracking technology. Even the user cannot be determining in which cover image the data is hidden. Since the key is dynamically generated at the spot by using the time stamp the sender and receiver even cannot guess their key to open their package. The biometrics systems can automate the detection of multi registrations made by the same person. Finally, we identified and proposed face biometrics method, which can also bind the registration information to the steganography algorithm we also provided a way to protect the integrity of voter registration information that can be suitable to implement in current environments. In future we can focus on multi biometric concepts to implement in e-voting system.

9. REFERNCES

[1]. Shashikala Channalli, Ajay Jadhav, Steganography An Art of Hiding Data, International Journal on Computer Science and Engineering, Sinhgad College of Engineering, Pune. Vol.1(3), 2009, 137-141 137

[2]. Stanislaw Badura, Slawomir Rymaszewski, Transform domain steganography in DVD video and audio content, IEEE International Workshop on Imaging Systems and Techniques - IST 2007 Krakow, Poland, May 4-5, 2007, Information Technology and Electronics Department, Warsaw University of Technology.

[3]. Mohammed Khasawneh , Mohammad Malkawi , A Biometric-Secure e-Voting System for Election Processes, Proceeding of the 5th International Symposium on Mechatronics and its Applications (ISMA08), Amman, Jordan, May 27-29, 2008.

[4]. F.Song, H.Liu,David Zhang,J.Yang , A Highly scalable incremental facial feature extraction method, Neurocomputing, Proceedings of International Conference in Biometric and Neurocomputing Technology, vol:71(2008) pg:1883-1888.

[5]. Qingzhong Liu , Andrew H. Sung, Mengyu Qiao, Detecting Information-Hiding in WAV Audios, Computer Science Department and Institute for Complex Additive Systems Analysis, New Mexico Tech IEEE 978-1-4244-2175-6/08/, 2008.

[6]. X. Ru, Y. Zhang and F. Wu., Audio Steganalysis Based on "Negative Resonance Phenomenon" Caused by Steganographic Tools. Journal of Zhejiang University SCIENCE A, 7(4):577-583, 2006.

[7]. W. Mazurczyk, J. Lubacz, *LACK - a VoIP Steganographic Method***,** In: Telecommunication Systems: Modelling, Analysis, Design and Management, Vol. 45, Numbers 2-3, 2010, ISSN: 1018-4864 (print version), ISSN: 1572-9451 (electronic version), Springer US, Journal no. 1123,

[8]. K. Szczypiorski, W. Mazurczyk, and et al., Steganographic Routing in Multi Agent System Environment, Special Issue "Secured Information Systems" of Journal of Information Assurance and Security (JIAS), Dynamic Publishers Inc., Atlanta, GA 30362, USA, Volume 2, Issue 3, September 2007, pp. 235-243, ISSN 1554-1010.also in: Computing Research Repository (CoRR), abs/0806.0576, arXiv.org E-print Archive, Cornell University, Ithaca, NY (USA), submitted on 3 June 2008, published on 4 June 2008.

[9]. Rengarajan Amirtharajan, R Jithamanyu, An Invisible Communication for Secret Sharing against Transmission Error ,A Steganographic Perspective Universal Journal of Computer Science and Engineering Technology, 117-121, Nov. 2010. UniCSE, ISSN: 2219-2158.

[10]. Saurabh Singh, Gaurav Agarwal, Use of image to secure text message with the help of LSB replacement, international journal of applied engineering research, Volume 1, No1, 2010, research article, ISSN-0976-4259

[11]. Sujay Narayana and Gaurav Prasad, Two new approaches for secured image steganography using cryptographic techniques and type conversions, Signal & Image Processing : An International Journal(SIPIJ) Vol.1, No.2, December 2010, DOI : 10.5121/sipij.2010.1206 60

[12]. Walaa Abu-Marie, Adnan Gutub, Hussein Abu-Mansour , Image Based Steganography Using Truth Table Based and Determinate Array on RGB Indicator, International Journal of Signal and Image Processing (Vol.1-2010/Iss.3).

[13]. Prosanta Gope, Anil Kumar and Gaurav Luthra, An Enhanced JPEG Steganography Scheme with Encryption Technique International Journal of Computer and Electrical Engineering, Vol. 2, No. 5, October, 2010 1793-8163.

[14]. Victor Morales-Rocha1, Jordi Puiggalí1 and Miguel Soriano, Secure Remote Voter Registration -. Proceeding of 3rd international Conference on Electronic Voting 2008, GI-Edition Lecture Notes in Informatics August 6th- 9th, 2008 in Castle Hofen, Bregenz, Austria. pg 95-108.

[15]. Hamid.A.Jalab, A.A.Zaidan, B.B.Zaidan, New Design for Information Hiding with in Steganography Using Distortion Techniques IACSIT International Journal of Engineering and Technology Vol. 2, No.1, February, 2010 ISSN: 1793-8236.

[16]. Seunglim Yong, MPEG Video Content protection based on Fingerprinting Scheme, IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.10, October 2007 161, Manuscript received October 5, 2007, Manuscript revised October 20, 2007

[17]. VenkataSubbaReddy Poli Nagaraja Arcot Jyothsna Charapanamjeri, Evaluation of Biometrics, IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.9, September 2009 261, Manuscript received September 5, 2009, Manuscript revised September 20, 2009

[18]. Yousra BEN JEMAA, Sana KHANFIR, Automatic local Gabor features extraction for face recognition, (IJCSIS) International Journal of Computer Science and Information Security, Vol. 3, No. 1, 2009.

10. AUTHORS PROFILE

E.S.Shameem Sulthana, Assistant Professor, received her MCA from Bharathidasan University, Trichy (May'2000) and she has completed M.Phil. (Comp. Science) from Mother Teresa Women's University, Kodaikannal. (June'2005). Now, She is pursuing her Ph.D. in Bharathiar University, Coimbatore.

She worked as a lecturer in Bharathidasan Arts & Science College. After that she served as a Senior lecturer in MCA department in Vivekananda Engineering College. At present she is working as a Assistant Professor in Dept. of Computer Science, Achariya Arts & Science College, Pondicherry.

Her research interests are in Web Technology, Network Security, Web Security and Biometrics. She is a Life member of computer society of India, ISTE and institute of engineers India. She has published many papers in international conferences and journals.

S.Kanmani received her B.E and M.E in Computer Science and Engineering from Bharathiar University and Ph.D. from Anna University, Chennai.

She has been the faculty of department of Computer Science and Engineering, Pondicherry Engineering College from 1992. Presently she is heading the department of in Information Technology. Her research interests are in software engineering, software testing and object oriented systems. She is a member of computer society of India, ISTE and institute of engineers India. She has published about 50 papers in international conferences and journals.