ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 5, Issue 2, February 2016

Digital Image Steganography based Security Model using wavelet for Internet voting Environment.

Komal Kapoor[#1]

[#1] BPS Mahilla Polytechnic,Khanpurkalan,Sonipat,Haryana, India

***Abstract*—The growth of internet has increased the attention towards having an internet voting system which will give the facility to voter to vote online. The security and authentication are the major bottleneck in an internet voting system. Biometrics is a convenient, secure and efficient way of authentication. For Personal Identification, fingerprints are the most widely used parameter amongst all biometrics. The security of fingerprints is the major concern in an internet voting system. The paper has proposed the method for securing biometric finger print template which is required for authentication in an internet voting system. The paper has presented a steganographic technique to hide the fingerprint image of a voter behind the voter's face image. The proposed Steganography algorithm works on the daubechies wavelet transform coefficients of the original image to embed the secret fingerprint image. The proposed algorithm has selected the skin area for hiding the secret image. The generated stego image is good in terms of perceptibility and PSNR.**

***Keywords*—Authentication; Biometric; Steganography; Internet Voting system; security; Perceptibility.**

I. INTRODUCTION

Internet Voting System [1][2][5] is an election system in which the voted electronic ballot is transmitted to the election officials via the Internet. It differs from the electronic voting system which do not use internet as the medium to transmit the data. The implementation of Internet voting has advantage of increased participation of those who do not regularly participate in the elections and also for those who cannot be at the polling place for voting. But the security, integrity and secrecy of Information are under technological threat over the internet. The successful implementation of internet voting is totally dependent on the security and authenticity of information. Security should be provided when the data is transmitted to the election official over the Internet and after the voting process when the votes are stored for counting and auditing. The internet voting system suffers from vulnerabilities like Denial of service, voter impersonation, spoofing, Voter coercion and vote buying, Vote transportation, secrecy, security. Using internet as medium for vote casting, the internet voting system should deal with the various security issues like Authentication, confidentiality, Integrity, Vote transmission, Reliable Vote Storage, Multiple Voting, Defence against Attacks on Internet Voting Machines, Defence against Attacks on Election Computer System.

Among the various risk in internet voting, there is one risk that is voter authentication. Voter authentication allows only the eligible voters to vote in an internet voting system. The Biometric data like fingerprint, iris, face, retina etc is widely used for authentication and identification. So in an internet voting environment the voter fingerprint image can be used as the data for authentication. But this fingerprint data is susceptible to various attacks when transmitted via the internet for authentication. To overcome this problem a Steganographic technique is presented in this paper which will protect the fingerprint images required for authentication.

Steganography [10] [13] [14][15] is the word which comes from Greek language means covered writing. Steganography is the art of concealing the information in other message on information which is called as carrier or cover. So the information is not visible to the observer. Steganography is the practice of hiding private or sensitive information within something that appears to be nothing out to the usual. Steganography's ultimate objectives are undetectability, robustness (resistance to various image processing methods and compression) and capacity of the hidden data.

The present paper has proposed the Steganographic technique in transform domain using DWT which will hide the voter's finger print image behind the voter's face image.

II. RELATED WORK

Bo Yang and Beixing Deng[19] proposed a Steganography method which hides the small-size gray image in a large-size gray image. Arnold transformation is first performed on the secret image. Discrete Wavelet Transformation (DWT) is performed both on the cover image (image without secret message) and the transformed secret image (image to be embedded into cover image). DWT coefficients of each component (approximate, horizontal, vertical, diagonal) of secret image are quantized and coded into bit streams. Then, the approximate component of secret image is embedded into the approximate component of cover image using improved Least Significant Bit (LSB) algorithm. Three detailed components (horizontal, vertical, diagonal) are embedded into the relationship between their counterparts and the approximate component of the cover image respectively. The

results showed that the stego image is imperceptible, robust and had better secrecy.

Ali Al-Ataby and Fawzi Al-Naima[33] proposed method pre-adjusts the original cover image in order to guarantee that the reconstructed pixels from the embedded coefficients would not exceed its maximum value and hence the message will be correctly recovered. Then, it uses Wavelet transform to transform both the cover image and encrypted hidden message. Wavelet transform allows perfect embedding of the hidden message and reconstruction of the original image. It was found that the proposed method allows high payload (capacity) in the cover image with very little effect on the statistical nature of it. This is of course on the expense of reducing PSNR and increasing the MSE (and hence RMSE). The results of the proposed method were compared with the results obtained after applying the same techniques mentioned above but with the transform being FFT. The comparison was in favor of DWT as expected due to the ability of Wavelet transform to compress data and introducing scarcity, hence increasing the capacity or payload of the steganography process. The drawback of the proposed method is the computational overhead. The method requires resources from the computer hardware (mainly processor speed and memory (RAM).

Dr.S.T.Gandhe [20] have used the Steganography and cryptography both for copyright protection of digital images. In this algorithm first the logo is encrypted and then it is inserted in the given image using DWT. The paper has evaluated various performance parameters such as mean square error, PSNR, correlation Coefficient and tested the algorithm on various attacks but the algorithm is not immune to compression technique.

Ahmed A. Abdelwahab and Lobna A. Hassaan[34] proposed a data hiding technique in the DWT domain which decomposed both secret and cover images with 1-level DWT. The author has applied many of image processing operations such as lossy compression, blurring, cropping, median filter, sharpen, and addition of noise and showed that the technique is robust. The disadvantage of this method is that the extracted data is not completely as same as the embedded original version.

Roli Bansal, Priti Sehgal, Punam Bedi [22] has represented an efficient watermarking scheme to watermark host fingerprint images with their corresponding facial images using Particle Swarm Optimization (PSO) in the Discrete Cosine Transform (DCT) domain. The author used PSO to find the best DCT coefficient's in the finger print image where the facial image data can be embedded, so that the distortion produced in the host image is minimum. The Structural Similarity Index (SSIM) and the Orientation Certainty Level Index (OCL) is used as objective function for PSO. The algorithm resulted into better watermarked image quality while retaining the feature set of the original fingerprint. The proposed technique is also robust against image processing attacks. The watermarked fingerprint image and the extracted facial image can be verified for a secure and accurate biometric based personal authentication.

III. MATHEMATICAL BACKGROUND

Discrete Wavelet transform (DWT) [35] is a mathematical tool for decomposing an image on a set of wavelet basis function. The wavelet transform is based on small waves, called wavelets. The wavelets are the mathematical function that represents the scaled and shifted form of finite length waveform called mother wavelet. The wavelet transform gives both the temporal and frequency information of an image for analysis. Wavelet transform analyse the image at different resolution.

The DWT processes the image by dividing it into four non overlapping multi-resolution subbands LL -Low frequency band, LH -Horizontal high frequency band , HL -Vertical high frequency band and HH.-Diagonal high frequency band .The sub band LL represents the coarse-scale DWT coefficients (the approximation) while the subbands LH, HL and HH represent the fine-scale of DWT coefficients (the details).To obtain the next coarser scaled wavelet coefficients, the subband LL is further decomposed and dividing into four non overlapping multi-resolution sub bands is accomplished. This process is repeated several times, which is determined by the application at hand. Each level has various bands information such as low– low, low–high, high–low, and high–high frequency bands. Furthermore, from these DWT coefficients, the original image can be reconstructed. This reconstruction process is called the inverse DWT (IDWT).

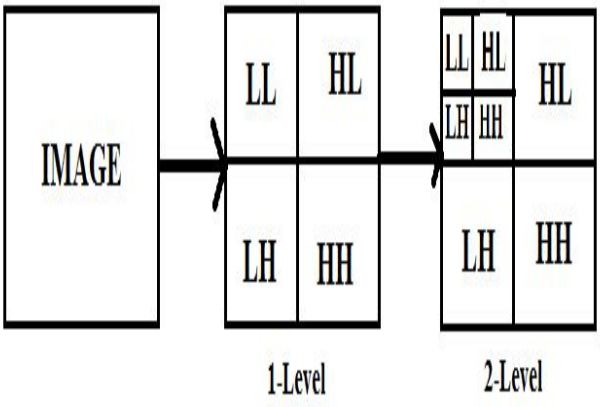

Fig. 1Two dimensional wavelet transform of an image

IV. PERFORMANCE MEASUREMENT PARAMETERS

A. **Peak Signal to Noise Ratio (PSNR)**: PSNR is used as a performance measurement parameter for measuring the imperceptibility of stego image[36] . PSNR is defined as

$$\mathbf{PSNR= 10*\log_{10}(I^2_{max} / MSE)}$$

Where MSE represents Mean Square Error which is calculated as

$$\mathbf{MSE}=\frac{1}{M*N}\sum_{i=1}^{M}\sum_{j=1}^{N}[S(i,j)-I(i,j)]^2$$

Here I_{max} indicates the maxi mum value in the image; i and j are the image coordinates; M and N are the dimensions of the image; S (i,j) is the resultant stego image and I(i,j) is the original cover image.

PSNR is measured in decibels (dB). PSNR values below 30 dB indicate low quality (i.e., distortion is visible in embedding). A PSNR of 40 dB, or higher qualifies a high quality image.

B. **Structural Similarity Index (SSIM)**: The quality of the Stego image is calculated using Structural Similarity Index (SSIM)[37] which is defined as

$$\mathbf{SSIM= (2S_{avg}\, I_{avg}+c_1)(2\sigma_{SI}+c_2)/(S^2_{avg}+I^2_{avg}+1)(\sigma_S^2+\sigma_I^2+c_2)}$$

Where, S and I are Stego Image and original cover image. S_{avg} and I_{avg} are the corresponding average of Stego image and original cover image. σ_S and σ_I the corresponding variances of Stego Image and original cover image. σ_{SI} is the covariance of S and I and c_1, c_2 are appropriate constants.

C. **The Normalized Correlation (NC):** The Normalized Correlation is used as a parameter for measuring the robustness of stego image[38].It is used to compare the extracted watermark with the original watermark. Its value lies between [-1,1]. The unity values signify exact similarity between extracted watermark and original watermark.

$$\mathbf{NC}=\frac{\sum_{i=1}^{m}\sum_{j=1}^{n}w(i,j)*w'(i,j)}{\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n}w(i,j)^2}\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n}w'(i,j)^2}}$$

Where, w represents the inserted watermark and w' represents the extracted watermark.

V. PROPOSED METHOD

The biometric template required for confirming the identity of a voter should be protected in an internet voting environment. For the protection of biometric template a steganographic method has been proposed and simulated in Matlab. The proposed method has used the image Steganography to hide the fingerprint image of voter behind the voter's face image which is required for authentication in an internet voting system. The proposed algorithm has used the color face image in JPEG format to secure the gray scale fingerprint image. The technique is based on Adaptive Image Steganography in frequency Domain. The method has selected the skin area for hiding the secret image. The proposed Steganography algorithm works on the discrete wavelet transform coefficients of the original image to embed the secret fingerprint image without affecting the visual quality of the image. The statistical error-based methods dependent on pixels value difference such as mean square error (MSE), root mean square error (RMSE), peak signal-to-noise ratio (PSNR), Structural Similarity Index (SSIM) is used here for the performance measurement of proposed method.

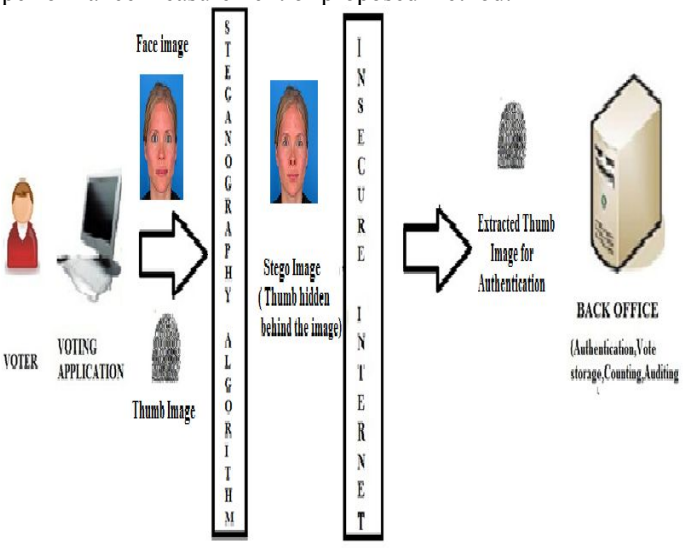

Fig. 2 Proposed Method

A. Proposed Fingerprint Embedding Algorithm

- Maintain the image database (face and thumb) of voters to represent the identity of the voters.
- Convert the face image which is in RGB color model to YCbCr color model.
- Thresholding is applied to Cr image to get the face area pixels which is needed for embedding.
- The pixel information which is required for cropping the original image is extracted from the Face area in Cr image.
- From the Cr image the first and last, row and column is searched which has the face pixel. From that rows and columns information, the original image is cropped.
- At last this cropped image is resized to 512*512.
- From the cropped image only the Blue Image Plane is selected to hide the data.
- The Blue Image Plane is decomposed into first level coefficients LL1, LH1, HL1, HH1 using the discrete wavelet Transform. The first level Approximation coefficient LL1 is further decomposed using DWT for getting the second level coefficients LL2, LH2, HL2 and HH2.
- The Gray scale Finger Print Image of Size 256*256 is taken. This finger Print image is then decomposed using DWT into first level coefficients. This result

into the first level coefficients which is stored as LL, LH, HL, HH.

- The HH2 coefficient of cover image is exchanged pixel by pixel with the One tenth value of LL approximation level coefficient of Finger print image.
- Two Level Inverse Wavelet Transform is applied to get host Image.
- This Host Image is then resized to cropped image size.
- This way only the cropped portion of original image has the finger print information.
- Final steganographic image is received which contains the biometric information for transmission over internet.

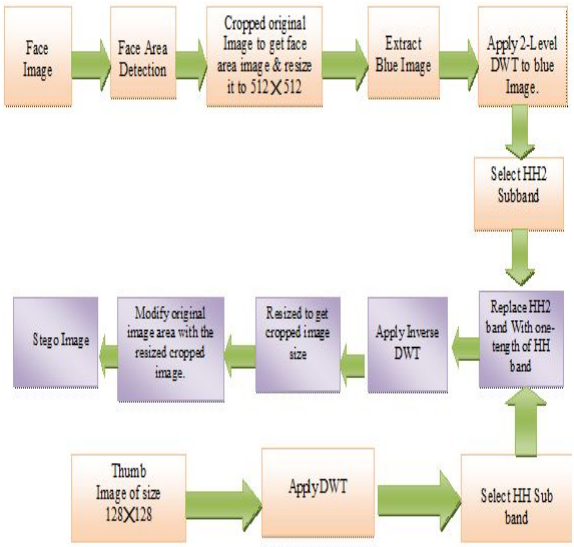

Fig. 3 Block diagram of Embedding Algorithm

B. Proposed Fingerprint Extraction Algorithm:

- Convert the Stego Image which is in RGB color model to YCbCr color model.
- Thresholding is applied to Cr image to get the face area which is needed for embedding.
- The pixel information which is required for cropping the Stego image is extracted from the Face area in Cr image.
- From the Cr image the first and last , row and column is searched which has the face pixel. From that rows and columns information the Stego image is cropped.
- This cropped Stego image is resized to 512*512.
- From the Cropped stego image only the Blue Image Plane is selected.
- The Blue Image Plane is decomposed into first level coefficients LL1, LH1, HL1, HH1 using the discrete wavelet Transform. The first level Approximation coefficient LL1 is further decomposed using DWT for getting the second level coefficients LL2, LH2, HL2 and HH2.
- The second level HH2 coefficient has the stored information.
- The first level Approximation coefficient of fingerprint image is ten times the second level HH2 coefficient and termed as LL.
- Three zero matrix of size equal to extracted first level approximation coefficient of fingerprint image is generated which act as first level LH, HL, HH of fingerprint image.
- Inverse Discrete Transform is applied to LL, LH, HL, HH coefficient to get the finger print Image.

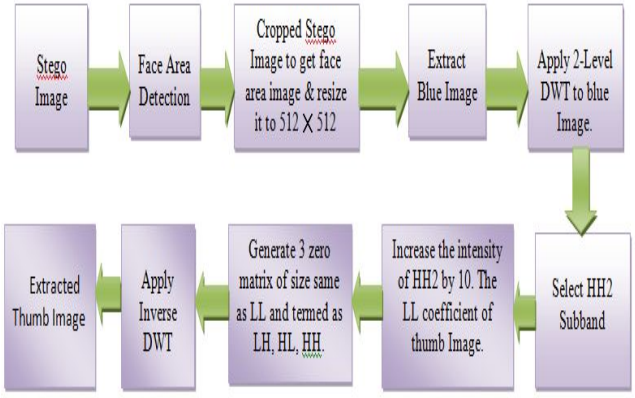

Fig. 4 Block Diagram of Extracting Algorithm

VI. Simulation Results

The proposed Steganography technique is implemented in MATLAB R2008b. The proposed method has used the color Face Image of size 900 ╳ 1200 to hide the gray scale Thumb image of size 256 ╳ 256. . The experiment was performed on various fingerprint images and the face images. The performance of the proposed technique has been evaluated. The results in the form of stego images and extracted thumb images have been shown for the different face and thumb images. The results have also been tabulated for four different face images and fingerprint images in terms of their PSNR, SSIM, NC values.The fingerprint images has been chosen randomly for the implementation.

.

Fig. 5 Results on face image1 and Thumb image1

Fig. 6 Results on face image 2 and Thumb image 2

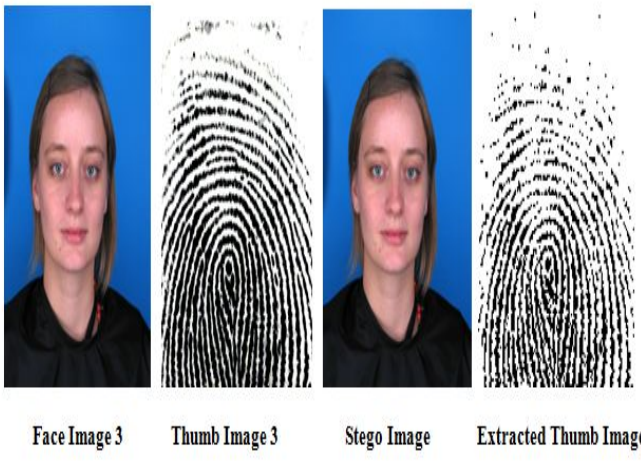

Fig. 7 Results on face image 3 and Thumb image 3

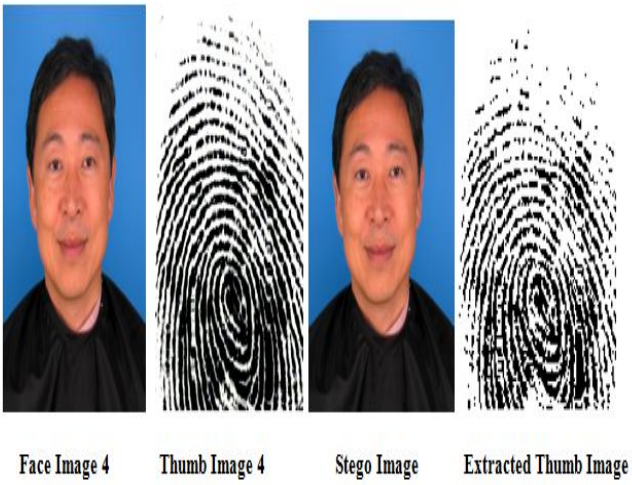

Fig. 8 Results on face image 4 and Thumb image 4

TABLE I
VALUE OF PERFORMANCE MEASUREMENT PSNR, SSIM,NC PARAMETERS

Input image	Thumb Image	PSNR(db)	SSIM	NC
Face 1	Thumb1	41.9221	0.9977	.9872
Face2	Thumb2	41.8842	0.9993	.9854
Face3	Thumb3	42.3927	0.9996	.9996
Face4	Thumb4	42.2937	0.9992	.9992

VII. CONCLUSION

For the purpose of security and authentication in internet voting system, an efficient steganographic technique has been presented in this paper. The proposed method is used for hiding the fingerprint image of a voter in his facial image. The advantage of the proposed technique is as follow

- The facial image used here is a color image of jpeg format whereas most of the other technique has used the gray scale image.
- The size of the hidden fingerprint image is 256 ×256 which means the proposed method is designed for the capacity of hiding 65536 pixels.
- The proposed technique has used the face area information for hiding the fingerprint image.
- The Quality metrics PSNR and SSIM values has revealed that the stego image is imperceptible.
- Only the stego image is needed at the time of recovery. There is no need of original face image at the time of extraction.

REFERENCES

[1] Aggelos Kiayias, Michael Korman and David Walluck, "An Internet Voting System Supporting User Privacy" in proceedings of 22nd annual Computer Security Application Conference, 2006, pp 165-174.

[2] Scott Wolchok, Eric Wustrow, Dawn Isabel, and J. Alex Halderman ,"Attacking the Washington, D.C. Internet Voting System," *in Proc. CFCDS'12*, Feb. 2012
[3] D. Jefferson, A. Rubin, B. Simmons and D. Wagner, "A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)," Tech. Rep., 2004.
[4] Abhishek Roy and Sunil Karforma, "Risk and Remedies of E-governance Systems," *Oriental Journal Of Computer Science & Technology*, vol 4, pp. 329-339, Dec. 2011.
[5] Jordi Puiggalí, Jesús Chóliz, Sandra Guasch, "Best Practices in Internet Voting Nist," Workshop on UOCAVA Remote Voting Systems. Washington DC, August 2010.
[6] R. Michael Alvarez, Thad E. Hall, Alexander H. Trechsel , "Internet Voting in Estonia," *VTP Working Paper*,2008.
[7] http://www.edmonton.ca/city_government/documents/Internet_Voting _Issues_Guide_December_21_2012.pdf/.
[8] www.elections.bc.ca/docs/Internet-Voting-Discussion-Paper.pdf/.
[9] verifiedvoting.org/downloads/InternetVotingStatement.pdf/.
[10] Chin-Chen Chang, Min-Hui Lin and Yu-Chen Hu, "A Fast and Secure Image Hiding Scheme Based On Lsb Substitution," *International Journal of Pattern Recognition and Artificial Intelligence*, vol. 16,2002,pp 399-416.
[11] Andreas Westfeld and Andreas Pfitzmann, "Attacks on Steganographic Systems Breaking the Steganographic Utilities EzStego, Jsteg,Steganos, and S-Tools," *In Proc. IHW'99*,1999.
[12] Andrew Westfeld, "F5-a steganographic algorithm: high capacity despite better steganalysis," *In Proc. IHW'01*, 2001,pp 289-302.
[13] Chi-Kwong Chan and L.M. Cheng, "Hiding data in images by simple LSB substitution," International Journal of Pattern Recognition and Artificial Intelligence vol. 16, pp 399-416.
[14] Ahmad T, Al-Taani and Abdullah M. AL-Issa, "A Novel Steganographic Method for Gray-Level Images".
[15] Michiharu Niimi, Hideki Node, and Eiji Kawaguchi, "A Study on the Steganography using Bit-Plane Complexity Based Region Segmentation Method," *in Proc. IVCNZ'98*, 1998.
[16] Y.K.Lee and L.H.Chen,"High capacity image steganographic model," *IEE Proc.-Vision, Image and Signal Processing*, vol. 147,pp. 288–294, 2000.
[17] J. Fridrich, M. Goljan, and D. Hogea, "Steganalysis of JPEG Images: Breaking the F5 Algorithm," *Proc. 5th Int'l Workshop Information Hiding*, Springer-Verlag, 2002,pp 7-9.
[18] N. Provos,"Defending against statistical Steganalysis." *in Proc. of the 10th USENIX Security Symposium*, pp. 323-325,2001.
[19] Bo Yang and Beixing Deng,"Steganography in gray images using wavelet". *In Proc. of ISCCSP'06*, 2006, pp 275-290.
[20] Dr.S.T.Gandhe, K.T.Talele and Dr.A.G.Keskar, "Steganography security for copyright protection of digital images using dwt," *(IJCNS) International Journal of Computer and Network Security*, vol.2, pp.21–26, 2010.
[21] Linu Paul, Anilkumar, "Authentication for Online Voting Using Steganography and Biometrics," *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*,Vol 1, Dec.2012, pp 26-32.
[22] Roli Bansal, Priti Sehgal, Punam Bedi, "Securing Fingerprint Images Through PSO Based Robust Facial Watermarking," *International Journal of Information Security and Privacy*, vol. 6, pp.34-52, Jun 2012.
[23] Olaniyi, O.M, Arulogun O. T. and Omidiora E.O,"Towards an Improved Stegano-Cryptographic Model for Secured Electronic Voting," *African Journal of Computing & ICT* ,Vol 5, Dec 2012,pp 10-16.
[24] Roli Bansal,Priti Sehgal,Punam Bedi," Securing Fingerprint Images using a Hybrid Technique," *In proc.ICACCI'12*, 2012,pp 557-565.
[25] Prabha Susy Mammen and S. Ramamoorthy. "A Novel Data Hiding Technique based Bio-Secure Online Voting System," *in proc. ICCCE'12*,2012
[26] Shobha lokhande, Dipali,sawant, Nazneen Sayyad, amata Yengu and ,D.D.Pukale, "E-Voting through Biometrics and Cryptography-Steganography Technique with conjunction of GSM Modem," in proc. *ETCSIT'12,* 2012
[27] B. Swaminathan, J. Cross Datson Dinesh, "Highly Secure Online Voting System with Multi Security using Biometric and Steganography,"*International Journal Of Advanced Scientific Research And Technology,*vol 2,2012
[28] Rura, Lauretha, Issac Biju, Haldar, Manas Kumar, "Analysis of image steganography techniques in secure online voting," *ICCSN'11,* 2011.
[29] ShivendraKatiyar, Kullai Reddy Meka, Ferdous A. Barbhuiya, Sukumar Nandi ,"Online Voting System Powered By Biometric Security Using Steganography,"*in Proc. EAIT'11*,2011.
[30] Okediran O. O. , Olabiyisi S. O. ,Omidiora E. O. and Ganiyu R. A., "A Survey of Remote Internet Voting Vulnerabilities," *World of Computer Science and Information Technology Journal,* vol.1 ,pp 297-301, 2011.
[31] Rubin A., "Security Considerations for Remote Electronic Voting over the Internet" Available at http://avirubin.com/e-voting.security.html.
[32] Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt, "Digital Image Steganography: Survey and Analysis of Current Methods," *signal processing,* vol. 90, pp. 727-752, mar. 2010.
[33] Ali Al-Ataby, Fawzi Al-Naima "A modified high capacity image steganography technique based on wavelet transform" *The International Arab Journal of Information Technology*, vol 7,pp 358–364, 2010.
[34] Ahmed A. Abdelwahab, Lobna A. Hassaan "A Discrete Wavelet Transform Based Technique For Image Data Hiding" *25th National Radio Science Conference*, 2008.
[35] R.C. Gonzalez and R.E. Woods, Digital Image Processing 2/E. Upper saddle River, NJ: Prentice-Hall.
[36] http://en.wikipedia.org/wiki/Peak_signal-to-noise_ratio.
[37] https://ece.uwaterloo.ca/~z70wang/research/ssim/.
[38] https://en.wikipedia.org/wiki/Cross-correlation.