IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 4, Issue 7, July 2016

STEGANOGRAPHY BASED AUTHENTICATED VOTING SYSTEM

Shyam Manohar Agrawal[1], Prof. Vaishali S.Jabade[2]

M.Tech Student, Electronics and Telecommunication, Vishwakarma Institute of Technology, Pune, India [1]

Asst.Professor, Electronics and Telecommunication, Vishwakarma Institute of Technology, Pune, India [2]

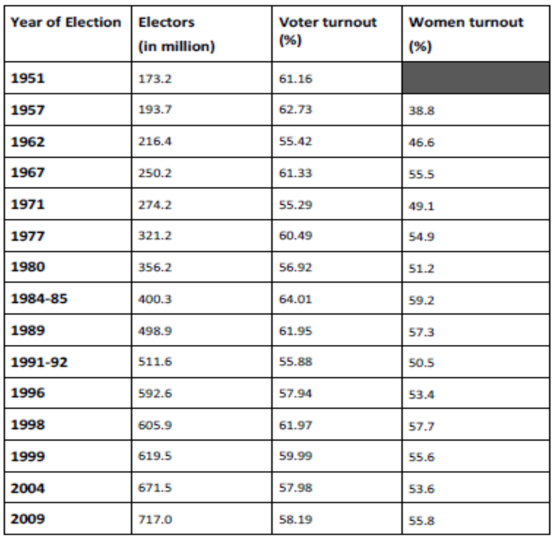
Abstract: Steganography Based Authenticated Voting System, is a system that will help a person to cast his vote even when he is away from his constituency. This will reduce his effort and save his travelling time. This system will enable the ELECTION COMMISSION OF INDIA (ECI) to manage elections easily and securely. This system will use the data which is already present with in the form of Aadhaar unique identification. It contains personal identity along with his biometric information. With the help of steganography we can try to provide a biometric as well as password security to our vote. The system will make a decision whether the voter is the authenticated 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 and stego image but they are not noticeable by human eye. One only be able to extract the embedded key and data only when the fingerprint gets match. Correct use of the procedure will increase the voting percentage in India and help in selecting right leader for the nation.

Keywords: Steganography, ECI, Fingerprint, Aadhaar Card

I. INTRODUCTION

An election is a process by which a person chooses an individual to deal with 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, transparency and safety. 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. The voting system should be fast so the valuable time of voters as well as the voting system conductors will be saved and there should be a provision of Absentee voting. An absentee ballot is a vote cast by someone who is unable or unwilling to attend the official polling station or to which the voter is normally allocated.

Table 1: Voter Turnout in Lok Sabha Election [3]



Year of Election	Electors (in million)	Voter turnout (%)	Women turnout (%)
1951	173.2	61.16	
1957	193.7	62.73	38.8
1962	216.4	55.42	46.6
1967	250.2	61.33	55.5
1971	274.2	55.29	49.1
1977	321.2	60.49	54.9
1980	356.2	56.92	51.2
1984-85	400.3	64.01	59.2
1989	498.9	61.95	57.3
1991-92	511.6	55.88	50.5
1996	592.6	57.94	53.4
1998	605.9	61.97	57.7
1999	619.5	59.99	55.6
2004	671.5	57.98	53.6
2009	717.0	58.19	55.8

Currently, India does not have an absentee ballot system for all citizens except in few exceptions. Because of absence of such system the voting percentage in India has never exceeded 65 precent of total voters since1951 as illustrated in table 1[3].

In Steganography Based Authenticated Voting System main aim is to concentrate the focus on increase in voting percentage and security of votes. 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. The voter ID card provided by ECI in many cases does not have clear photo of the voter this can lead to false voting or identity theft. This limitation in current system can be abolished by providing biometrics security to voting system. If Steganography Based Authenticated Voting System works well then it will be a good progress over the current system.

II. RELATED WORK

The numbers of voting systems have been adopted all over the world with the passage of time starting from paper ballot system to the recently adopted electronic voting system. This evolution of voting system has been discussed by S.M.Agrawal et.al.[1].The recent Voting system face the challenge of security and authencity.Steganography process can be used for overcoming the aforementioned challenges. The steganoghaphy generally falls into two categories, one using spatial domain while other using transform domain.

A. Spatial domain:

In spatial domain, it directly processes the location and luminance of the image pixel directly. Many techniques have been proposed in this domain such as LSB(Lest significant bit) insertion method[4][5],Patchwork method and texture block coding method[6].For the human perception, the small changes in grey values are regarded as noise. The disadvantage of LSB technique is it suffers from random flipping of lower bits.

B. Transform domain:

In transform domain, it processes coefficients in frequency domain for hiding data. There are different techniques present such as the Fourier transform [7][9], discrete cosine transform [8][10] and discrete wavelet transform[2][17].The data is hidden in the low or middle frequency coefficients of the cover image, because the high frequency coefficients are easily suppressed by compression. Therefore, how to select the best frequency portion of the cover image for hiding the data is an important and difficult topic.

After the inverse transformation, the hidden data seems scattered in spatial domain .the transform domain method is more robust than the spatial domain method against compression, cropping and jittering. Although various applications may have different requirements and performance evaluation criteria, generally, the key requirements for steganography are imperceptibility, security, capacity and complexity [2]. To avoid the degradation of image quality and increase the security of hidden information, there are two important requirements that are most needed for a well-designed watermarking scheme and which described as follows.

- Imperceptibility:

The host image or original image should not be visibly degraded by the watermark. In other words, we must ensure that an unauthorized user does not perceive the existence of the watermark. Imperceptibility ensures the excellent perceptual quality of the protected image.

- Security against image manipulation :

Active attackers in the network pose a serious threat to the transmitted image and it may undergo changes as the attackers try to sense the hidden information. The hidden message gets destroyed if some image manipulation, such as cropping or rotating is performed on the image. It is important for Steganographic algorithms to be secure against malicious changes to the image.

III. PROPOSED METHOD

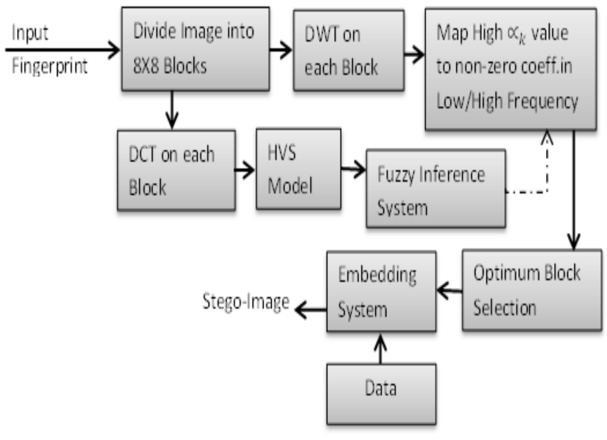


Fig.1 Proposed Method

The methodology includes steganography with the help of biometric security. Fundamentally there are some 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 stenographic 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. The proposed is an adaptive image watermarking algorithm based on a HVS (Human Visual System) model and a FIS (Fuzzy Inference System). The FIS and the HVS combined are used to adjust the watermarking strength and to generate the maximum possible watermark length that can be embedded without noticeably degrading the quality of the image. The watermark is embedded into the low frequency range of the image after being transformed by the Discrete Wavelet Transform (DWT). As a result, the watermark is more Secure and imperceptible.

A. HVS MODEL (Human Visual System) :

In the HVS (Human Visual System) model, Psycho-visual studies have shown that it has a general band pass characteristics. The sensitivity of human vision is different in various spatial frequencies (frequency bands) [11].A number of factors affect noise sensitivity of human vision the following three sensitivity properties can be employed in the proposed Steganographic scheme. Which are used to generate the Fuzzy inference System [16][17].

i. <u>Luminance sensitivity:</u>

The perceptual ability of the signal on a constant background. If the background is brighter then the visibility of embedded signal is very low hence we can embed larger signal in original image [22].The luminance sensitivity can be estimated by following formula:

$$L_K = \left[\frac{X_{DC,k}}{\overline{X_{DC}}}\right] \qquad (1)$$

Where, $X_{DC,k}$, is the DC coefficient of the DCT of the k^{th}block and $\overline{X_{DC}}$ is the mean value of all block's DC coefficients of a specific image.

ii. <u>Texture sensitivity:</u>

The more chaotic the background is, the larger the embedded signal could be [11]. It can be estimated by quantizing the DCT coefficients of an image (X) using the JPEG quantization table (Q). The latter results are then rounded to the nearest integers. The number of non-zero coefficients is then computed. This method can be estimated by the following formula.

$$T_K = \text{ADD}\{\text{Round}\,\frac{X_K\,(x,y)}{Q(x,y)}\} \qquad (2)$$

Where, Add is an adder that adds the non-zero coefficients and (x,y) represents the location in the k^{th} block.

iii. Frequency sensitivity:

The human perception to the sine wave at difference frequencies. It is the basic visual model that the variance of low frequency is more sensitive and high frequencies are less visible to the human eye, the frequency sensitivity is represented by the JPEG quantization table (luminance). Human vision is less sensitive to noise in high resolution bands and bands having orientation of +45° [12].

We use the DC coefficients of an image as the luminance sensitivity. The texture sensitivity is estimated by quantizing the DCT coefficients of an image using the frequency sensitivity. Then, we compute the non-zero coefficients as the texture sensitivity. The JPEG quantization table is then used as the frequency sensitivity.

B. Fuzzy Inference system:

The FIS has been implemented to adapt the HVS different properties. In the proposed scheme we are considering texture, brightness and Frequency sensitivity. This approach is designed in such a manner to enable the visual sensitivity membership function to fit the properties of an image.[14][15]

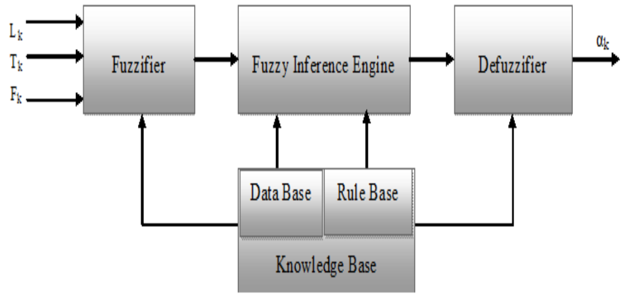


Fig.2 Fuzzy Inference System

I. Fuzzifier:

It transfers the crisp input to fuzzy sets.

- Brightness sensitivity:

The brightness can be categorized as dark, medium or bright. The figure below plots the fuzzy input variable with less, moderate and high brightness values.

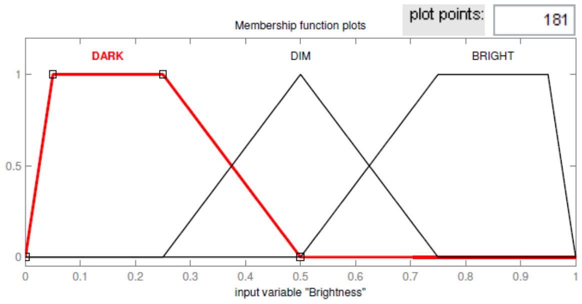


Fig.3 Brightness Sensitivity Membership Function

- Texture sensitivity:

The eye's response to texture is classified into 3 categories - low, medium, and high. Plots below illustrate smooth, medium and rough texture values for this fuzzy input variable.

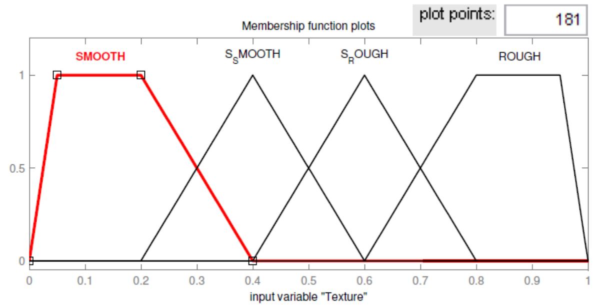


Fig.4 Texture Sensitivity Membership Function

- Edge distance or edge sensitivity

The edge distance can be small, medium, or large as shown in the plots below.

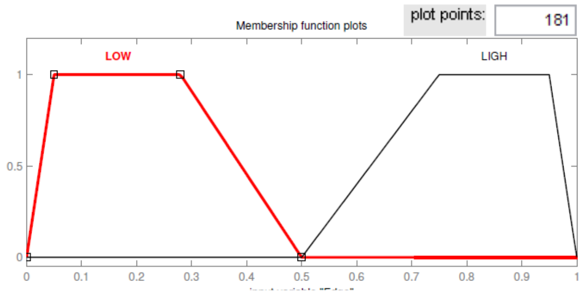


Fig.5 Edge Sensitivity Membership Function

II. Fuzzy Inference Engine:

It is a general control mechanism that exploits the fuzzy rules and the fuzzy sets defined in the Knowledge Base and rule base in order to reach certain conclusion.

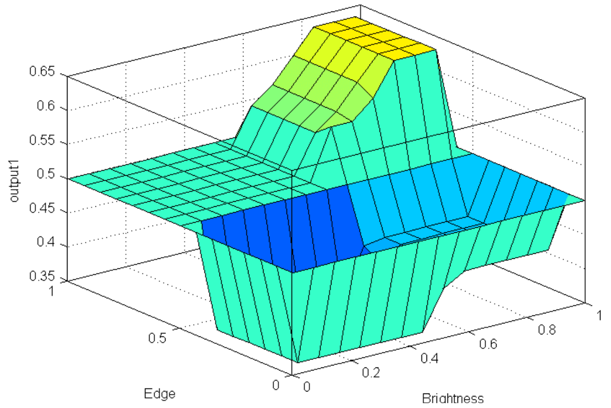


Fig.6 Fuzzy Inference Rule Base (Surface View)

The fuzzy rules are derived are based on the following facts:

The eye is less sensitive to noise in those areas of the image where brightness is high or low.

The eye is less sensitive to noise in highly textured areas but, amongst these, more sensitive near the edges.

The eye is less sensitive in the regions with high brightness and changes in very dark regions.

III. Defuzzifier:

It transfers the fuzzy sets into crisp outputs.

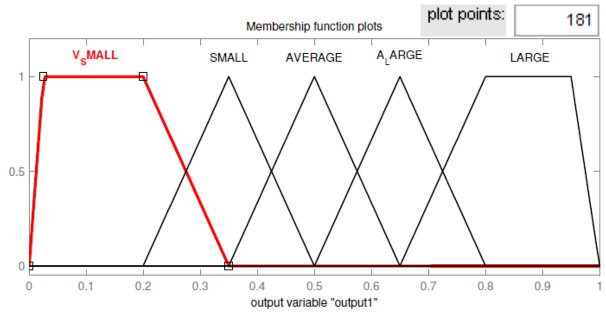


Fig.7 Output Membership Function

IV. Algorithm

A. Data Embedding System:
1. Start
2. Consider the 8 X 8 matrix containing 1's and 0's as the reference matrix
3. Get the voter finger print from aadhaar card database
4. Resize the figure print image into 256 X 256 Pixels
5. Divide the resized finger print image into 8 X 8 blocks
6. Apply Discrete wavelet transform on the on each block
7. Apply Discrete Cosine transform on image
8. Calculate the HVS parameter using DCT coefficient obtained in step 6
9. Calculate the membership function value using fuzzy inference model

$$\propto_{i,j,k} = F_K * L_K * T_K \qquad (3)$$

10. Check for the of membership function for each and every block obtained in step 5
11. If the value is greater than threshold embed the data into that particular block for only those pixel for which reference matrix has value of 1. If not then leave the block and go for next

$$I_{i,j,k} = I_{i,j,k}(1 + \propto_{i,j,k} * W) \qquad (4)$$

12. Apply the inverse DWT on Embedded image to get the stego-image
13. Repeat the steps 3 to 12 for the entire aadhaar card database
14. Stop

B. Data Validation and Voting System
1. Start
2. Consider the reference matrix from Data embedding system
3. Take the fingerprint image of voter through fingerprint scanner
4. Extract the fingerprint features form the fingerprint image
5. Check if these features match with any of the features from the stego-image database
6. If the matched then fetch that stego-image
7. Divide the stego-image into 8 X 8 blocks
8. Apply Discrete wavelet transform on the on each block
9. Apply Discrete Cosine transform on stego- image
10. Calculate the HVS parameter using DCT coefficient obtained in step 9
11. Calculate the membership function value using fuzzy inference model
12. Check for the of membership function for each and every block obtained in step 8
13. If the value is greater than threshold extract the data from that particular block for only those pixel for which reference matrix has value of 1. If not then leave the block and go for next
14. Confirm the details, give voter the key and allow him to proceed for voting
15. If the fingerprint features don't match then display the message that voter is invalid
16. Stop

V. Results

In our experiments, the original image I is a 256 X 256 Fingerprint image with 8 bits/pixel resolution used. The secret message is embedded in the decomposed sub-band of 8X8 block of original image obtained through single-level wavelet transformation.

We evaluate the quality between the original image and the attacked image using the peak signal-to-noise ratio (PSNR), which is defined as follows:

$$PSNR = 10\, log_{10} \frac{255}{MSE} \qquad (5)$$

Where, the mean square error (MSE) is defined as follows:

$$MSE = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N}\left[I(x,y) - I'(x,y)\right]^2}{M*N} \qquad (6)$$

Where, $I_{(x,y)}$ is Original image and $I'_{(x,y)}$ is Stego image with size (M,N).

- Speckle noise:

$$g(n,m) = \{f(n,m) * u(n,m) + \xi(n,m)\} \qquad (7)$$

Where, g(n,m) is the observed image, u(n,m) is the multiplicative component and ξ(n,m) is the additive component of the speckle noise. Here n and m denotes the axial and lateral indices of the image samples

- Gaussian Noise:

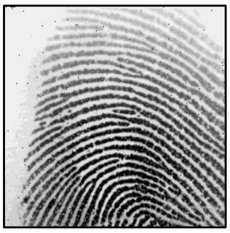
$$P_G(z) = \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{-(z-\mu)^2}{2\sigma^2}} \qquad (8)$$

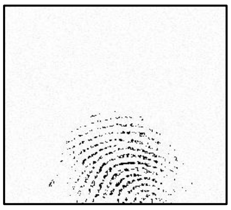
Where, μ is the mean value, σ is variance of the Gaussian noise. z is the component in which the Gaussian noise is added.

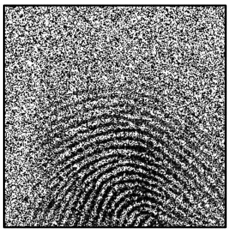
DOI 10.17148/IJIREEICE.2016.4715

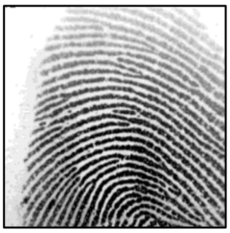
Table 2: Results for Various Attacks

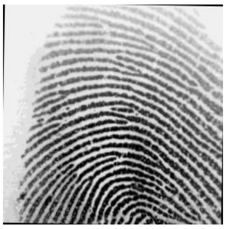
Type of Attack	Stego Image After Attack	PSNR (P) & MSE (M) Values

Salt And Piper Noise (0.041)		P= 29.68019
		M= 69.99408

Gaussian Noise (0.001,0)		P= 7.134315
		M= 12579.08

Speckle Noise (2)		P= 6.859297
		M= 13401.42

Bicubic (4)		P= 37.17563
		M= 11.78529

Bilinear (-1)		P= 14.04892
		M= 2324.452

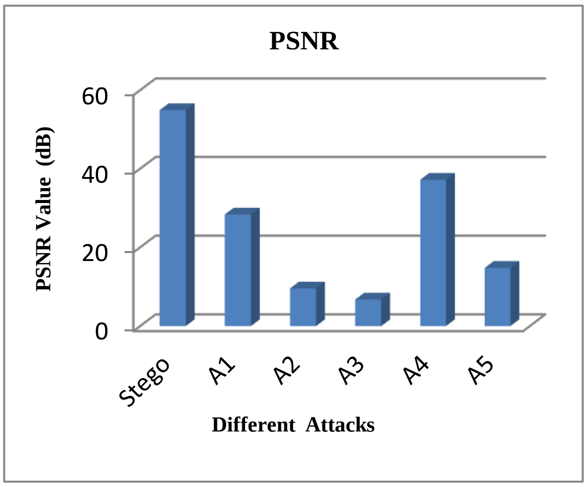


Fig.8 PSNR values of Various Attacks

Fig.8 represents graph of various attacks depicted A1 as Salt and Piper Noise (0.041), A2 as Gaussian Noise(0.001,0), A3 as Speckle Noise(2), A4 as Bicubic interpolation, A5 as Bilinear interpolation.

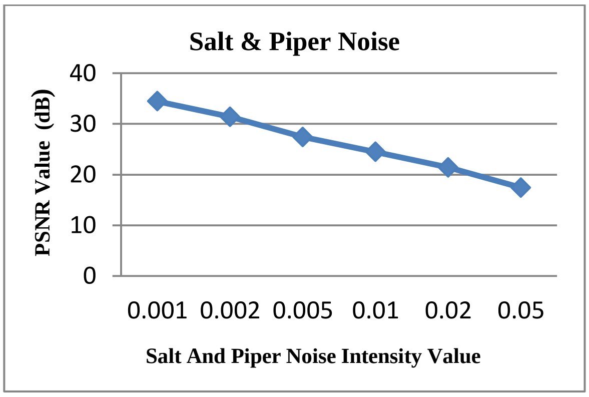


Fig.9 PSNR value for Salt & Piper Noise at different intensity

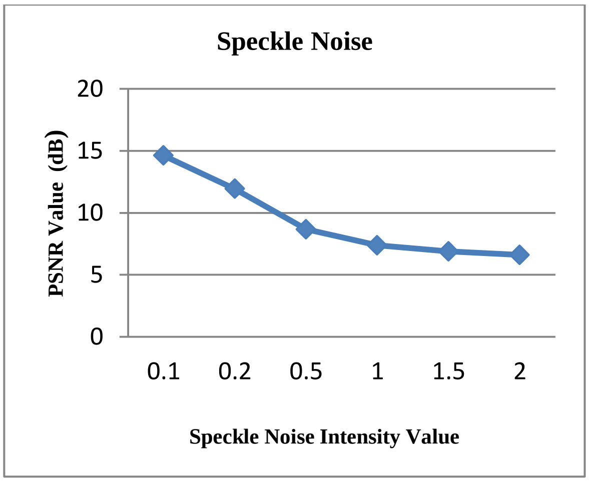


Fig.10 PSNR value for Speckle Noise at different intensity

DOI 10.17148/IJIREEICE.2016.4715

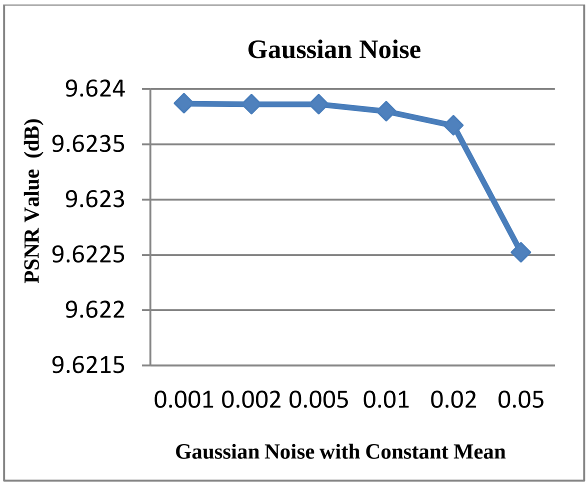


Fig.11 PSNR value for Gaussian Noise at different intensity

As the intensity level of the attacks increases, the PSNR value of attack stego image decrease drastically this showing that the embedded message cannot be retained back if it is manipulated. This shows that the algorithm will useful to increase the security and authenticity. Which is represented in fig.9, fig.10, fig.11

IV. Conclusion

The proposed technique uses steganography for security and authenticity of voting system and thus can help in achieving significant growth in the voting percentage in India. The use of FIS model accurately approximates the relationship between different parameters of HVS model. This results in better performance of this system than its previous counterparts.

.

.

References

[1] S. M. Agrawal and V.S. Jabade ,"Intelligent Voting System-A survey",IJIREEICE,Vol.4,Issue 6,June2016.

[2] V.S.Jabade and S.R.Gengaje,"Literature Review of Wavelet Based Digital Image Watermarking Techniques", International Journal of Computer Applications(0975-8887), Vol.31,pp.28-35,Oct 2011.

[3] The Economic Times. Retrieved 23 November 2014.

[4] C.I.Podilchuk and W. Zeng,"Image –adaptive watermarking using virtual models,"IEEE Journal on Selected Areas in Communications, Vol.16, No.4, pp.525-539, May 1998.

[5] S.Saha and R.Vemuri,"How do image statistics impact lossy coding performance",Information Technology ,pp.42-47,2000.

[6] R.C.Gonzalez and R.E.Woods,Digital Image Processing,Addision Wesley,NewYork ,USA 1981.

[7] P.L.Lin, "Robust transparent Image Watermarking System with Spatial Mechanisms", The Journal of Systems and Software, pp.107-116, 2000.

[8] C. T. Hsu and J. L. Wu, "DCT-Based Watermarking For Video," IEEE Transactions on Consumer Electronics, Vol.44, No.1, pp.206-216, Feb.1998.

[9] Xiao Jun Kang Li Jun Dong, "Study of the Robustness of Watermarking Based on Image Segmentation and DFT", *IEEE International Conference on Information Engineering and Computer Science, ICIECS*, 2009, pp1-4.

[10] Chien Chang Chen and De-Sheng Kao, "DCT Based Reversible Image Watermarking Approach", Third IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2007, pp 1-5.

[11] Yusnita Yusof, Othman Khalifa, "Imperceptibility and Robustness Analysis of DWT- Based Digital Image Wateramrking", Proceedings of the International Conference on Computer and Communication Engineering, 2008, pp. 1325-1330.

[12] A. Nikolaidis, and 1. Pitas, "Region-based image watermarking," IEEE Transaction on image processing Vol. 10, No. 11 , pp. 1726-1740, Nov. 2001.

[13] V. S.Jabade and S.R.Gengaje," Logo based Image Copyright Protection using Discrete Wavelet Transform and Fuzzy Inference System",International Journal of Computer Applications(0975-8887), Vol.58-No.10,pp.23-28, Nov 2012.

[14] Santi P. Maity and Seba Maity, "Multistage Spread Spectrum Watermark Detection Technique using Fuzzy Logic", IEEE Signal Processing Letters, Vol.16, No.4, 2009, pp. 245-248.

[15] Ming-shing Hsieh, "Image Watermarking based on Fuzzy Inference Filter", IEEE Proceedings of the International Conference on Machine Learning and Cybernetics, Baoding, 2009, pp.3058-3063.

[16] Barni M, Bartolini F, Piva, "An Improved Wavelet Based Watermarking Through Pixelwise Masking", IEEE transactions on image processing, Vol. 10, 2001 pp.783-791.

[17] V. S.Jabade and S.R.Gengaje "Performance Evaluation of DWT and FIS Based Image Copyright Protection" International Journal of Innovative Research in Computer and Communication Engineering.Vol.4, Issue 1,pp.892-900, Jan 2016

DOI 10.17148/IJIREEICE.2016.4715