World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:2, No:5, 2008

A New Algorithm for Enhanced Robustness of Copyright Mark

Harsh Vikram Singh, S. P. Singh, and Anand Mohan

***Abstract*—**This paper discusses a new heavy tailed distribution based data hiding into discrete cosine transform (DCT) coefficients of image, which provides statistical security as well as robustness against steganalysis attacks. Unlike other data hiding algorithms, the proposed technique does not introduce much effect in the stego-image's DCT coefficient probability plots, thus making the presence of hidden data statistically undetectable. In addition the proposed method does not compromise on hiding capacity. When compared to the generic block DCT based data-hiding scheme, our method found more robust against a variety of image manipulating attacks such as filtering, blurring, JPEG compression etc.

***Keywords*—**Information Security, Robust Steganography, Steganalysis, Pareto Probability Distribution function.

I. INTRODUCTION

ALTHOUGH the developments in image coding standards for image data compression using JPEG, MPEG and JPEG2000 have been widely exploited for multimedia data transfer through World Wide Web but data protection against unauthorized access for copy right violation, manipulation or even deletion have become the challenging concern. Therefore providing effective security solutions to ensure multimedia data integrity and authenticity during open channel transmission has become an interesting field due to obvious advantages of digital document distribution. This is particularly needed to retain benefits of low cost of global data distribution by a document owner while also offering dependability at the receiving end. Recently, digital data hiding using *steganography* [1,2,3] has emerged as an attractive technique for such applications because of facilitating hiding an imperceptible mark in the multimedia data which can be used to identify the genuine document owner, track authorized users and detect illegal document tampering [4]**.** Imperceptible hiding using steganography [5] is achieved by embedding copyright identification data into the multimedia document (image, audio, or text) called "digital cover" or "host media" which is to be transmitted through an open channel.

An effective steganography technique for copyright protection aims at achieving high robustness of the imperceptible copyright mark against deliberate attempts of copyright violation by modifying, altering or even deleting the original identification mark of a document owner.

Harsh Vikram Singh is with Institute of Technology, Banaras Hindu University, India. e-mail: harshvikram.singh.ece04@itbhu.ac.in

In addition it is also required that embedding of copyright mark data into the cover introduces minimum perceptual distortion in the host cover. Based on the processing domain the data hiding schemes can be classified as *spatial domain* and *transform domain* [6, 7] techniques. The spatial domain data hiding is computationally simple and straight forward wherein host media data is directly replaced by identification mark data using substitution techniques. However, these techniques are more fragile to external attacks and thus provide poor robustness of the copyright identification mark. On the other hand the transform domain techniques require more computations but they achieve superior robustness against lossy compressions and other signal processing operations like scaling and rotations or cropping, depending on the invariant properties of a particular transform [8, 9]. Therefore transform domain techniques have proved better choice for achieving enhanced security of copyright mark and thus for greater assurance of originality of a multimedia document at the receiving end. In general digital document distribution may consist of image, audio or text or their permutations distributed through open channel. However, the issue of copyright protection of original paintings, art work, maps, sketches, sceneries, photographs and pictures of an owner is more challenging as well as demanding than other data types due to their high cost. In view of this our present study focuses on copyright protection of still image documents. As an illustrative example we have considered IEEE standard still images as host media in which text data is embedded as copyright mark. Although robust copyright data embedding along with image data compression can be achieved by data hiding into coefficients of Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) or Discrete Wavelet Transform (DWT) [10,11,12] but DCT is frequently preferred because it is widely used in JPEG and MPEG [13,14]; and thus it has merited our attention under the present study.

This paper describes a new algorithm for achieving enhanced robustness of copyright mark data as compared to existing techniques of data hiding using DCT coefficients [15]. Higher robustness of hidden copyright mark has been achieved using Pareto heavy tailed probability distribution function (*pdf*) [16,17] that increases the randomness of selecting DCT blocks as well as its coefficients for hiding copyright data into the medium frequency bands of two-dimensional discrete cosine transform (2D-DCT) coefficients of an IEEE *Lena* image. Embedding of copyright mark data into mid-band DCT coefficients has been carried out to achieve visual imperceptibility [18,19] of the hidden copyright mark which is statistically undetectable and robust against image manipulation attacks. The merits of the developed algorithm are illustrated through simulation studies by hiding textual copyright data into IEEE standard *Lena* image. The qualitative performance evaluation of the suggested algorithm has been carried out through analysis of histogram, JPEG compression and low pass filtering s*teganalysis* techniques [20, 21].

It is shown that BER level of 0.0288 for medium quality (Q-80) JPEG compression and 0.0716 for low quality (Q-30) JPEG compression is achievable. As more than 92% of the hidden data was recovered without any error for low quality (Q-30) JPEG compression. The corresponding PSNR between original and stego image obtained by proposed method is 39.84 dB which is well above the acceptable level for perceptual analysis. Therefore the suggested algorithm can be potentially useful in achieving enhanced copyright protection.

II. Data Modeling of DCT Coefficients

The mid-band region is a popular choice for data embedding in order to limit the distortion and enables the algorithm to be robust against a multitude of image manipulating attacks. It is often mentioned in the literature that the Gaussian model is not appropriate for the mid-frequency DCT coefficients [22]. Reininger and Gibson [23] used the Kolmogorov-Smimov (*KS*) goodness-of-fit tests in order to conclude that these coefficients can be better modeled as Laplacian rather than as Gaussian, Rayleigh, or gamma distribution. Laplacian PDF is given by

$$f_X(x) = \frac{\beta}{2}\exp\left(-\beta\left| \ x-\mu\right|\right) \quad (1)$$

where $\mu = mean(x)$, and $\beta^2 = 2/\mathrm{var}(x)$. However, it is shown in [24] that the Laplacian distribution is inadequate for heavier tailed samples, because its tail decays at a fast exponential rate. Tanabe and Farvardin [25] modeled the DCT coefficients using the generalized Gaussian Density (GGD), as its tail decays at a slower rate than the Gaussian distribution [26], which has the following PDF

$$f_X(x) = A\exp\left(-\beta\left| \ x-\mu\right|^c\right) \quad (2)$$

The parameters A and β can be expressed in terms of parameter c and standard deviation σ as follows:

$$\beta = \frac{1}{\sigma}\left(\frac{\Gamma\left(\frac{3}{c}\right)}{\Gamma\left(\frac{1}{c}\right)}\right)^{1/2}, \ A = \frac{\beta c}{2\Gamma\left(\frac{1}{c}\right)} \quad (3)$$

for $c = 1$, the generalized Gaussian distribution reduces to Laplacian, while the Gaussian PDF can be obtained for $c = 2$. However, even the GGD does not always sufficiently characterize the low- and mid-frequency DCT coefficients. Hernandez et. al. [27] observed that some samples in the tails of the empirical distributions have relatively high amplitudes and consequently cannot be adequately modeled by the exponentially decaying tails of the GGD.

A more systematic and efficient approach to this problem is to consider a better model for the DCT coefficients, which can capture their heavy tailed nature, i.e., the high-magnitude samples in the tails. Recently the Symmetric alpha- stable $(S\alpha S)$ family has been successfully applied to model heavy tailed data in various applications [28, 29].

The $S\alpha S$ distribution can be described by its characteristic function

$$\varphi(\omega) = \exp\left(j\delta\omega - \gamma\left|\omega\right|^\alpha\right) \quad (4)$$

$\varphi(\omega)$ is parameterized by the location parameter $\delta\,(-\infty < \delta < \infty)$, the scale parameter $\gamma\,(\gamma > 0)$, and the characteristic exponent $\alpha\,(0 < \alpha < 2)$. The location parameter δ gives the mean of the distribution for $1 < \alpha < 2$, while for $0 < \alpha \le 1$ it gives the median. The characteristic exponent or stability index, α is the most important parameter as it determines the shape of the distribution. The shape of the $S\alpha S$ PDF resembles that of the Gaussian density as it is bell shaped. However, it has much heavier tails, which asymptotically follow an algebraic rate of decay. For an $S\alpha S$ random variable X, as $x \to 0$, the tails satisfy

$$P\left(X > x\right) \sim c_\alpha x^{-\alpha} \quad (5)$$

where $c_\alpha = \Gamma(\alpha)\sin(\alpha\pi/2)\big/\pi$, $\Gamma(x) = \int_0^\infty t^{x-1}e^{-t}dt$ is the Gamma function. Hence, the tail probabilities of the $S\alpha S$ random variable follow inverse power law, which coincide with the tail properties of the Pareto distribution [16]. The Pareto distribution provides a rich and flexible modeling tool for heavy tailed non-Gaussian data [17], therefore it can be used for adequate modeling of the mid-frequency DCT coefficients. The PDF of Pareto distribution is given by

$$f\left(x : \alpha, \beta\right) = ak^a / xa^{a+1} \quad (6)$$

where $(a > 0)$ is shape parameter and $(k > 0)$ is the location parameter. Pareto heavy tailed distribution based random numbers have been used in the proposed technique for hiding as well as retrieval of messages in mid-band DCT components.

III. Proposed Algorithm

The proposed algorithm relies on n distinct heavy tailed Pareto based pseudo- random (PN) sequences, where n is the number of bits to be hidden. In addition, selections of blocks for hiding are also taken randomly with heavy tailed Pareto distribution. Properties of Pareto distribution (location and shape parameters) are used as a key with a threshold correlation factor for extracting messages at the receiver end. This key is available at both encoder and decoder locations, and it can be communicated through secure channel prior to sending stego images over open channel. The performance of the proposed steganography algorithm has been evaluated by embedding 512 *ASCII* characters in *IEEE* standard grayscale Lena $(512 * 512)$ image. The simulation was carried out using *MATLAB*.

A. The Encoder

In the proposed algorithm, 8×8 pixel blocks of the image are first transformed using the DCT. The mid-frequency regions of the DCT coefficient blocks are used to embed the hidden data as shown in Fig. 1, where shaded blocks represent the mid-frequency bands [30].

The working of the encoder is as follows:

1. Read the host image $I(M,N)$ of size $M \times N$ and the n-bit data $D_{i\,(i=1\ to\ n)}$ to be hidden.
2. Generate n Pareto random numbers $P_{R(R=1\,to\,n)}$ with location parameter k and shape parameter a.
3. Again generate n different heavy tailed Pareto distribution based PN-sequences $P_{Ni(Ni=1\,to\,n)}$ of length 22 (for 22 mid-band DCT coefficients) using a secret key (location parameter $k1$ and shape parameter $a1$) to reset the random number generator.

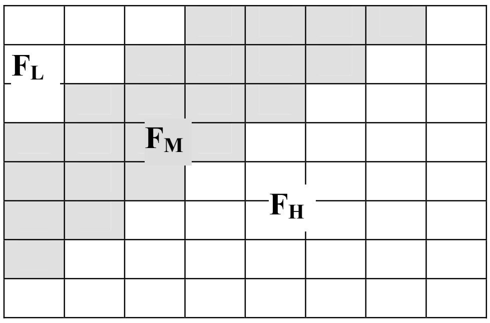


Fig. 1 Mid-frequency DCT region used to embed the hidden data

4. Transform the host image using the 8x8 block 2D-DCT and generate blocks $m_{p(p=1\,to\,m)}$, where $m = \frac{M \times N}{8 \times 8} \leq n$.
5. For $P_R = 1$ to n, select corresponding m_p.
6. For $D_i = 1$ to n,

   hide the i^{th} bit and modulate the ${m_p}^{th}$ DCT block of the host using eqs-1 and 2 respectively for a '0' or a '1' bit [30].

$$\begin{cases} I_W(u,v) = I_W(u,v) + K * W_i(u,v), & \text{if } u,v \in F_M \\ I_W(u,v) = I_W(u,v) & \text{if } u,v \notin F_M \end{cases} \quad (7)$$

$$\begin{cases} I_W(u,v) = I_W(u,v) - K * W_i(u,v), & \text{if } u,v \in F_M \\ I_W(u,v) = I_W(u,v) & \text{if } u,v \notin F_M \end{cases} \quad (8)$$

where K is the gain factor (in the present simulation $K = 10$) used to specify the strength of the embedded data; W_i is the appropriate pseudo random noise sequence based on the i^{th} hidden bit; $I(u,v)$ represents the 8x8 DCT block of the host image; and $I_w(u,v)$ represents the corresponding marked DCT block.

7. Inverse transform each of the marked DCT blocks, $I_w(u,v)$, using 8x8 block inverse 2D-DCT to get the final stego image $I_w(M,N)$.

The original and stego images are shown in Figs. 2 and 3 respectively. The peak signal to noise ratio (PSNR) between these two is found to be 39.84dB. As seen from these figures, the visual distortion induced in the stego image due to embedding is negligible.

Fig. 2 The original image

Fig. 3 The stego image

B. The Decoder

The hidden-bit extraction procedure is based on correlation between the mid-band coefficients of the image and the corresponding PN-sequences [30].

The working of the decoder is as follows:

1. Read the stego image.
2. Generate *n* different heavy tailed Pareto distribution based PN-sequences of length 22 using same secret key used during encoding (location parameter $k1$ and shape parameter $a1$) to reset the random number generator.
3. Transform the stego image using the 8x8 block 2D-DCT.
4. Generate one dimensional Pareto array of size *n* with location parameter *k* and shape parameter *a*, denoted as $corr(n)$
5. For $i = 1$ to n
   calculate the correlation between the mid-band coefficients of the i^{th} block and the i^{th} PN-sequence and store this value in $corr(i)$.
6. Calculate the average of all the values stored in the array, $corr(n)$.
7. Extract the j^{th} hidden bit, b_j, using the relationship given below.

$$b_j = \begin{cases} 0, \text{ if } \ corr(j) > average(corr(n)) \\ 1, \text{ if } \ corr(j) < average(corr(n)) \end{cases} \qquad (9)$$

IV. PERFORMANCE EVALUATION

Performance evaluation of the data hiding algorithm has been carried out using three different methods of steganalysis namely: *(i)* analysis of histogram, *(ii)* low pass filtering and *(iii)* JPEG compression analysis.

*(i)*Relative frequency approach has been used in the present case for studying distribution of mid-band DCT coefficients (histogram). If total number of mid-band DCT coefficients is represented by n and their values by x, then for an small interval Δx the relative frequency can be calculated as $R(x_j) = \frac{n_x}{n}$ where n_x represents number of coefficients in interval Δx. $R(x_j)$ depends upon the size of Δx. Smaller interval Δx accommodates less number of coefficients. For large enough data this mid-band DCT coefficient distributions at a particular height and interval Δx cab be represented by a rectangle area $\frac{n_x}{n}$. Therefore height of this rectangle will be $\left(1/\Delta x\right)\left(n_x/n\right)$ and width will be Δx. The plot of $\frac{n_x/\Delta x}{n}$ vs x provides relative frequency histogram curve for mid-band DCT coefficients [31]. When $\Delta x \rightarrow 0$ this relative frequency histogram approaches a smooth curve and gives probability density function of mid-band DCT coefficients [31]. In the proposed algorithm $\Delta x = 0.1$ The relative frequency histogram curves of the original host image, the stego image for the proposed algorithm, and the stego image with the generic spread spectrum based algorithm [27] are shown in Figs. 4, 5 and 6 respectively. The generic spread spectrum based algorithm distorts the histogram curve of the stego image, since it introduces two smaller peaks in the histogram curve as can be seen in Fig. 6. However, the histogram curve of the stego image in Fig. 5 that is generated by the proposed embedding algorithm does not have the additional peaks.

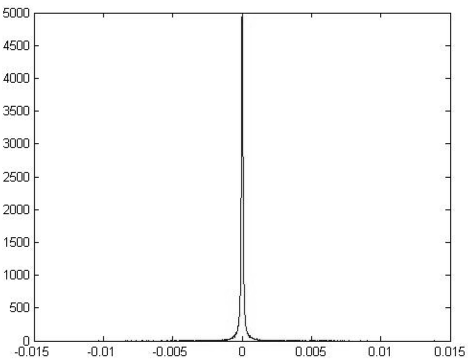
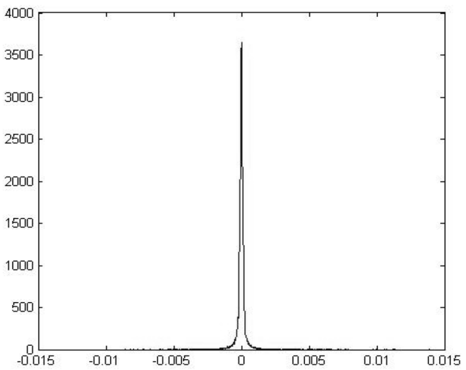


Fig. 4 Relative Frequency Histogram of Original Image



Fig, 5 Relative Frequency Histogram for Pareto *pdf* Embedding

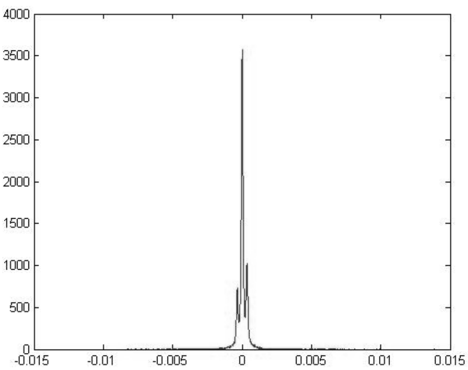


Fig. 6 Relative Frequency Histogram for Generic Spread Spectrum Embedding

(ii) Harmsen et. al. method [32] of low-pass filtering of the histogram is widely used for detection of hidden messages which states that data embedding in a cover corresponds to low pass filtering of histogram of the host and this effect is quantified by a decrease in the histogram center of mass. Therefore, if a noticeable number of high frequency DCT components of the host image have low power, the hidden data can be detected. Applying this principle to the relative frequency histogram of Fig. 5 for Stego-image generated by embedding copyright mark textual data using Pareto *pdf* it is clear that the histogram does not have any noticeable change due to low pass filtering. However, the low pass filtering effect can be prominently observed on the corresponding histogram of Fig. 6 which is generated using generic spread spectrum data hiding. Therefore comparing Figs. 5 and 6 it is evident that Pareto *pdf* based embedding offers much higher robustness of copyright mark against low pass filtering. Thus the proposed method offers much less vulnerability to Harmsen detection method.

(iii) Bit error rate (BER) is calculated by subjecting the stego image to JPEG compression [33] with quality factors 80, 50 and 30, to test the robustness of the proposed algorithm and generic spread spectrum method, shown in Table 1. For medium quality compression (Q 80) BER was 0.0288 whereas for low quality compression (Q 50) BER was found 0.0312, i.e. more than 96% of the hidden data was recovered without any errors. Even for very low quality compression (Q-30) BER was 0.0716 more than 92% of the hidden data was recovered without any error. However BER obtained for generic spread spectrum based stego image subjecting to same quality JPEG compression was much higher. Therefore our proposed algorithm is more robust than generic spread spectrum data hiding.

TABLE I BER AFTER SUBJECTING THE TEST DATA JPEG COMPRESSION

Quality factors for JPEG compression	**BER**	
	Proposed Pareto spread spectrum based hiding	**Generic spread spectrum algorithm based hiding**
(Q-80)	0.0288	0.0337
(Q-50)	0.0312	0.0464
(Q-30)	0.0716	0.0803

V. CONCLUSION

Digital data-hiding algorithm in the DCT domain has been proposed which provides statistical security and robustness against a multitude of image manipulating attacks. In the case of robustness tests, the proposed algorithm outperformed the generic DCT algorithm JPEG compression attacks considered. While providing significant robustness and capacity, this algorithm also induces low distortion in the host image with *PSNR* of more than 39 dB.

REFERENCES

[1] Petitcolas F. A. P., Anderson R. J. and Kuhn M. G., "Information hiding - A survey", *Proceedings of the IEEE*, pp. 1062-1078, vol. 87, no. 7, July 1999.
[2] Anderson R., "Information hiding", *Lecture Notes in Computer Science*, vol. 1174, Springer -Verlag, 1996.
[3] Hopper N. J., Langford J., and Ahn L., "Provably secure steganography," *Advances in Cryptology: CRYPTO 2002,* August, 2002.
[4] Maity, S.P., and Kundu, M.K., "An image watermarking scheme using HVS characteristics and spread transform," *Proceedings of the 17th International Conference on Pattern Recognition*, pp. 23-26, vol. 4, 2004.
[5] Delp, E.J., and Wolfgang, R.B., "A watermark for digital images," *International Conference on Image Processing*, pp. 219-222, 1996.
[6] Bruyndockx, J., Quisquater, J., and Macq, B., "Spatial method for copyright labeling," *IEEE Workshop on Image Processing*, pp. 456-459, 1995.
[7] Wolfgang, R.B., and Delp, E.J., "A watermarking technique for digital imagery: Further studies," *International Conference on Imaging Science*, pp. 279-287, 1997.
[8] Schyndel V.R.G., Tirkel A.Z., and Osborne C.F., "A digital watermark," *IEEE International Conference on Image Processing*, pp. 86-89, 1994.
[9] Westfeld A., and Pfitzmann A., "Attacks on steganographic systems," *Lecture Notes in Computer Science*, pp. 61-75, vol. 1768, Springer-Verlag, 2000.
[10] Ruanaidh J. J. K. ´O, Dowling W. J., and Boland F. M., "Phase watermarking of digital images," *Proceeding. International Conference on Image Processing (ICIP)*, pp. 239-242, vol. 3, 1996.
[11] Koch E. and Zhao J., "Toward robust and hidden image copyright labeling," *Proceedings Workshop Nonlinear Signal and Image Processing*, Marmaros, Greece, June 1995.
[12] Hsieh M.S., Tseng D.C. and Huang Y.H., "Hiding digital watermarks using multiresolution wavelet transform," *IEEE Transactions on Industrial Electronics*, pp.875 - 882, vol. 48, Issue 5, 2001.
[13] Podilchuk C. and Zeng W., "Watermarking of the JPEG bitstream," in *Proceedings of International Conference on Imaging Science, Systems, and Applications (CISST '97)*, pp. 253-260, Las Vegas, June 1997.
[14] Guan Y.L. and Jin J., "An objective comparison between spatial and DCT watermarking schemes for MPEG video," *Proceedings International Conference on Information Technology: Coding and Computing*, pp.207- 211, 2001.
[15] Tao B. and Dickinson B., "Adaptive watermarking in the DCT domain," *Proceedings of International Conference Image Processing*, Lausanne, Switzerland, Sept. 1996.
[16] Briassouli A and Tsakalides P, "Hidden Messages in heavy-tails: DCT-domain watermark detection using alpha-stable models," *IEEE Transactions on Multimedia*, pp. 700-716, vol. 7, August 2005
[17] Adler R., Feldman R., and Taqqu M. S., *A Guide to Heavy Tails: Statistical Techniques and Applications*. Boston, MA: Birkhauser, 1998.
[18] Podilchuk C. I., "Digital image watermarking using visual models," *Proceedings of Electronic Imaging*, vol. 3016, San Jose, CA, 1996.
[19] Podilchuk C. I. and Zeng W., "Perceptual watermarking of still images," *Proceedings of Workshop Multimedia Signal Processing*, Princeton, NJ, June 1997.
[20] Wang, H., and Wang, S., "Cyber warfare: steganography vs. steganalysis,*" Communications of the ACM*, pp. 76-82, vol. 47, 2004.
[21] Fridrich, J., and Goljan, M., "Practical steganalysis of digital images-state of the art," *In Proceedings of SPIE Photonics West*, pp. 1-13, vol. 4675, 2002.
[22] Tescher A. *G.*, "Transform image coding," *Advances in Electronics and Electron Physics.* Suppl. 12. New York: Academic, pp. 113-115, 1979.
[23] Reininger R. C. and. Gibson J. D, "Distributions of the two-dimensional DCT coefficients for images," *IEEE Transactions* on *Communications,* pp. 835-839, vol. -31, June 1983.
[24] Clarke R. J., *Transform Coding of Images*, New York: Academic, 1985.
[25] Tanabe N. and Farvardin N., "Subband image coding using entropy coded quantization over noisy channels," *Computer Science Technical Report Series,* University of Maryland, College Park, MD, 1989.
[26] Birney K. A. and. Fischer T. R, "On the modeling of DCT and subband image data for compression," *IEEE Transaction on Image Processing,* pp. 186–193, vol. 4, 1995.
[27] Hernandez J.R., Amado M., and Perez Gonzalez F., "DCT-domain watermarking techniques for still images: Detector performance analysis

and a new structure," *IEEE Transaction on Image Processing*, pp. 55-68, vol. 9, 2000.

[28] Achim A., Bezerianos A. and Tsakalides P., "Novel bayesian multiscale method for speckle removal in medical ultrasound images," *IEEE Transaction on Medical Image*, pp. 772–783, vol. 20, 2001.

[29] Georgiou P., Tsakalides P. and Kyriakakis C., "Alpha-stable modeling of noise and robust time-delay estimation in the presence of impulsive noise," *IEEE Transaction on Multimedia*, pp. 291–301, vol. 1, no. 3, 1999.

[30] Amin P.K., Liu N. and. Subbalakshmi K.P, "Statistically secure digital **i**mage data hiding," *IEEE 7th Workshop on Multimedia Signal Processing*, pp. 1- 4, 2005.

[31] Schwartz M., *Information Transmission, Modulation, and Noise.* McGRAW-HILL Book Company, 1985.

[32] Harmsen J.J., and Pearlman W.A. "Steganalysis of additive noise modelable information hiding." *Proceedings of SPIE Electronic Imaging*, Santa Clara, CA, vol. 5020, 2003.

[33] Gonzalez R.C. and Woods R.E., *Digital Image Processing Using MATLAB.* PEARSON EDUCATION, 2004.