Standard Deviation Converges for Random Image Steganography

Rengarajan Amirtharajan, P. Archana , V. Rajesh , G. Devipriya and J.B.B.Rayappan
School of Electrical & Electronics Engineering, SASTRA University

Abstract- **The advent of the internet age has led to the increase of prominent network security issues. Information encryption has long been a method used for information security. With the rapid development of parallel computing capacities of computer hardware, this method alone could not be trusted to ensure security by increasing the key sizes, thus bringing in the information hiding techniques into the scenario. Cryptography scrambles the data to be secured while information hiding embeds the information into files which do not reveal the presence of information. Steganography and water marking are two information hiding techniques. While steganography is used for secretly embedding the sensitive information in files, watermarking is used to implement copyright protection. Steganographic techniques are being widely used these days to increase the security of information. A combination of cryptography and steganography results in very strong cryptosystems. This is a paper of unexampled prosperity, which elicits easy-to-implement, difficult-to-sense proficiency for image steganography enforcing the statistical distribution's profound laws. Bit length for embedding is adjudicated via some delineated conditions and is done so by making use of Least Significant Bit . These conditions are the index for increasing complexity as well as security. Experimental ensues in terms of BPP, embedding capacity, and stego outputs also vindicate this paper. This paper prognosticates the crucial imputes of steganography.**

Keywords: Data hiding, Information hiding, Random Image Steganography (RIS), Modified LSB.

I. INTRODUCTION

With the tremendous advancements in communication, the need for securing the data has also increased manifold [1]. Experts define information security as the security that ascertains prudence, accessibility and veraciousness to whichever data format the communication habituates. Morals, as well as ethics, has weakened and have given way for infringement of information thus allowing the intruders to sabotage, manipulate or even sell this information for a greater profit [2]. This could lead to serious consequences like bankruptcy of a country, tyranny, mayhem, or attacks on a country by terrorists. Thus the need for information hiding algorithm arose [2-4]. The only tool that equips science to protect stored information and secure information transfer is Information Hiding.

The subclasses of information hiding techniques are steganography, cryptography and watermarking techniques [1]. Cryptography is the oldest and it involves coding of the source message in a way that only the sender and receiver can understand [5]. But it has a disadvantage in that, though third people cannot understand the secret code with ease, he still knows that there is a secret code present. Once he gets hold of the key he can access the secret data too. Steganography overcame this defect and it uses a cover object in the form of audio, video or image [6] which is then encoded with the secret data, thus it doesn't attract unwanted attention. Watermarking is intended for copyright protection where the information to be sent is embedded in a digital signal to verify its authenticity [2].

After extensive research it is found that steganography is the best method of data hiding as all the three characteristics of information hiding is effectively utilized. It is robust with high payload and also highly imperceptible. Several steganographic methods [7-18] have been proposed in image steganography and they are classified majorly as spatial [1, 4, 13] and frequency domain techniques [8, 14, 18]. The former widely engages LSB techniques to inscribe covert information in a cover's pixel in addition to pixel value differencing and Pixel Indicator based schemes [11, 16]. The secret data in latter is rooted in the cover's coefficients which are transformed by any of these: DCT [14], IWT [8, 18].

To maintain high quality stego output [19-24](i.e. high imperceptibility) and to share the secret stego key for recovery, an edge pixel finding algorithm is employed, known as Edge Detection [24] based steganography. This is a technique where the edges in an image are found out by using a suitable algorithm. The edge has varying gray levels and is used to define the boundary regions of the image fragments and they are used to analyze the important aspects of the image. The trio of differential embedding, alternating encryption and varying depth of embedding makes a self-sufficient, reliable and robust security system.

After carefully reviewing the available literature, this paper proposes an adaptive random image steganography method by considering the intensity values of the pixels. Section II explains the proposed method followed by result and discussion in Section III. Finally conclusions are drawn in Section IV.

II. PROPOSED METHODOLOGY

This implementation uses the variable bit embedding method. For the whole image, reckon the mean and standard deviation of each pixel in view of only the 4 MSB's.

Embedding depends on the pixel intensity value and the value of mean and standard deviation.

Two bits are embedded, when the pixel value is less than (mean–SD/2).

978-1-4673-5758-6/13/$31.00 © 2013 IEEE

Go for 3 bit embedding, if value is less than (mean +SD/2).
For other cases 4 bit has been embedded
In addition, an entrenching secret data random traversing path is generated to get the chaotic effect.

A. Embedding Algorithm

1. Assume cover image as a Matrix A
2. Compute Mod(A,16) and store it as Matrix B
3. Compute the mean and standard deviation of the Matrix B
4. Compute the values U1 and U2 where U1=(mean - SD/2) and U2=(mean + SD/2)
5. Using the Pseudorandom path generator algorithm generates a traversing path.
6. Extract the value of 4MSB's for the current pixel being traversed in the cover image.
7. Check for the following cases and embed appropriately
    a. If value < U1 k=2 else
    b. If value<U2 k=3 else
    c. K=4
8. Embed k bits in the current pixel and jump to next pixel value
9. Repeat steps 6 to 8 till end of image is reached.

B. Extraction Algorithm.

1. Assume stego image as a Matrix A1
2. Compute Mod(A,16) and store it as Matrix B1
3. Compute the mean and standard deviation of the Matrix B1
4. Compute the values U1 and U2 where U1=(mean-SD/2)and U2=(mean+SD/2)
5. Using the traversing path used in embedding algorithm traverse the image
6. Extract the value of 4MSB's for the current pixel being traversed in the cover image.
7. Check for the following cases and embed appropriately
    a. If value < U1 k=2 else
    b. If value<U2 k=3 else
    c. K=4
8. Extract k bits in the current pixel and jump to next pixel value
9. Repeat steps 6 to 8 till end of image is reached.

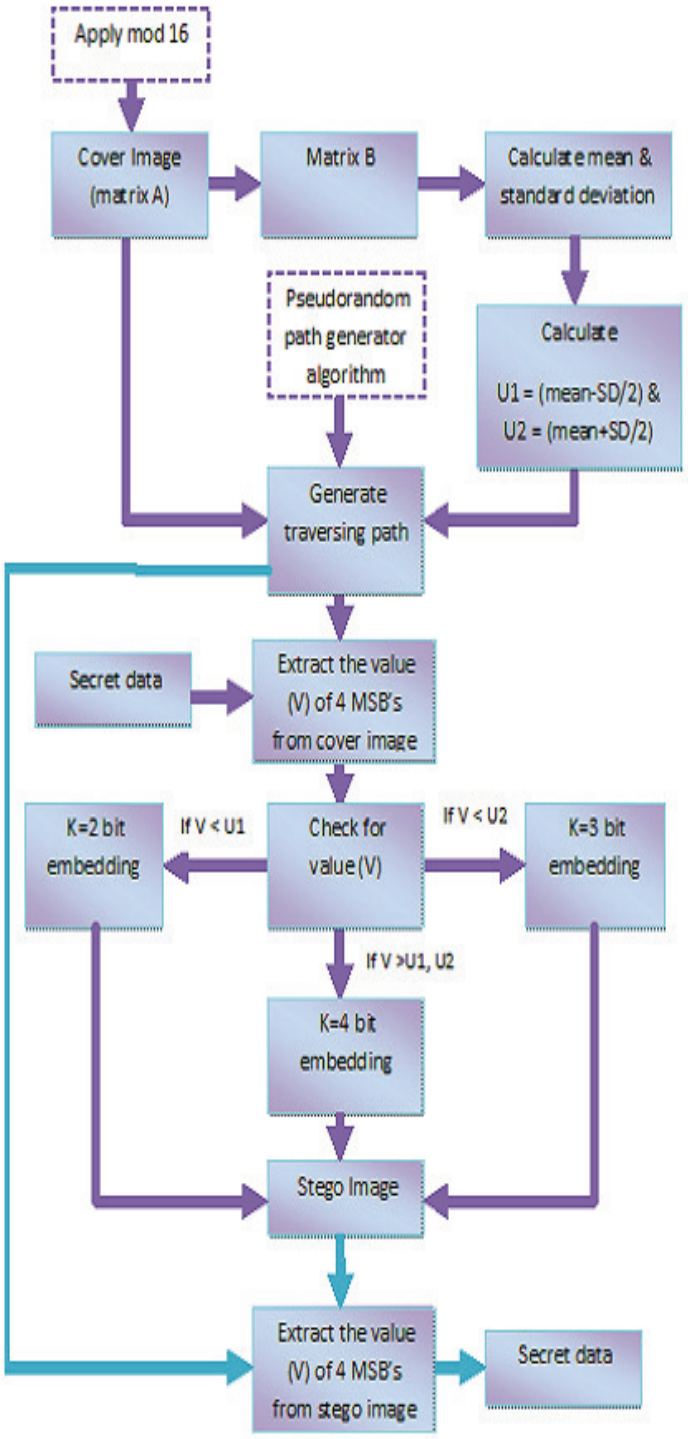

Fig. 1. Block diagram for the proposed method

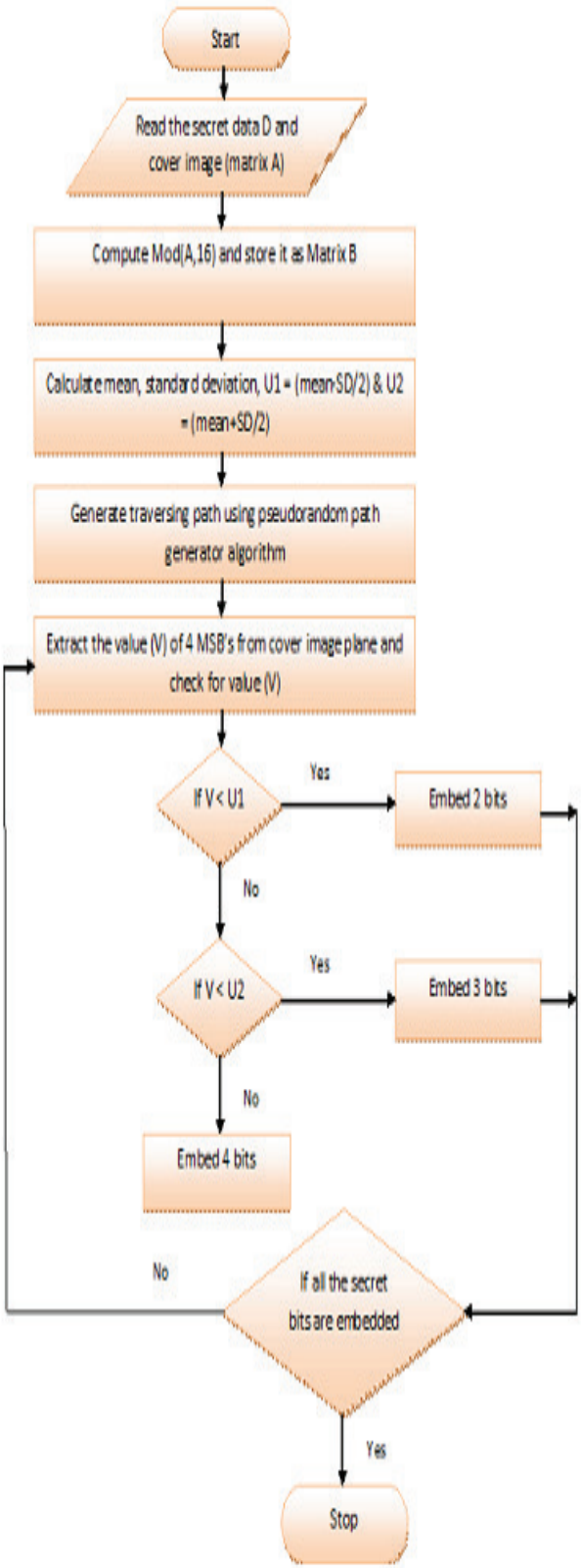

Fig. 2. Flowchart for Embedding

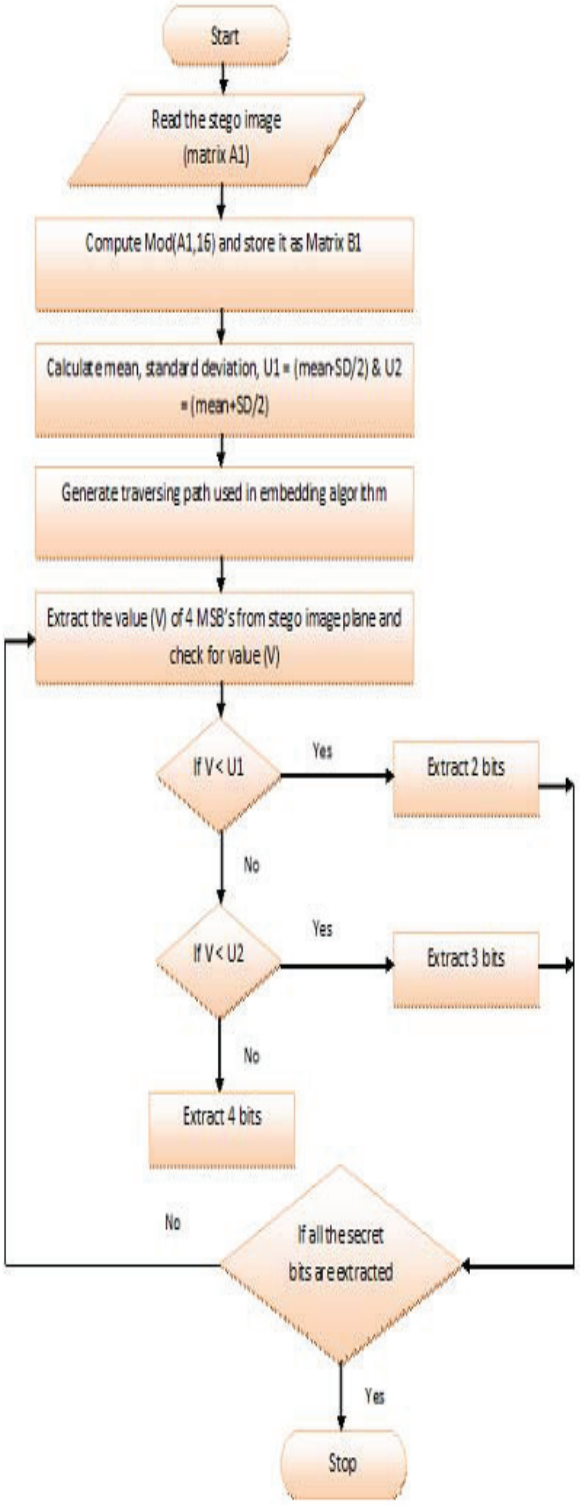

Fig. 3. Flowchart for Extraction

III. Result and Discussion

In view of the fact that this paper addresses the thought of engaging mean and standard deviation is sound and simple, it habituates random jumbling while stocking the covert message in carrier color images. Here, the process is so splendid that we can sense no confidential data infixed within. The cover images taken here are Temple, Mahatma Gandhi, Lena and Baboon of size 256×256; Algorithm is simulated on these images in MATLAB 7.1and the upshots are represented in Figures 4 & 5. The incurred readings are tabled.

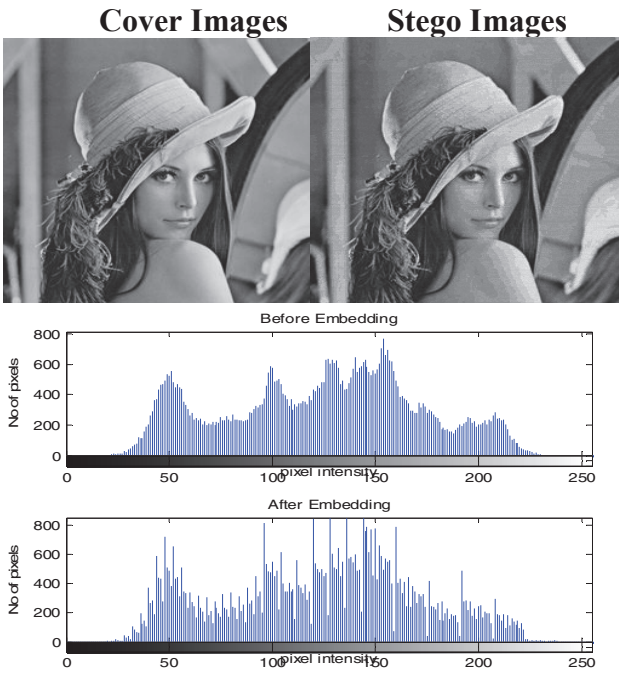

Fig. 4.Lena cover and stego images & their corresponding histograms

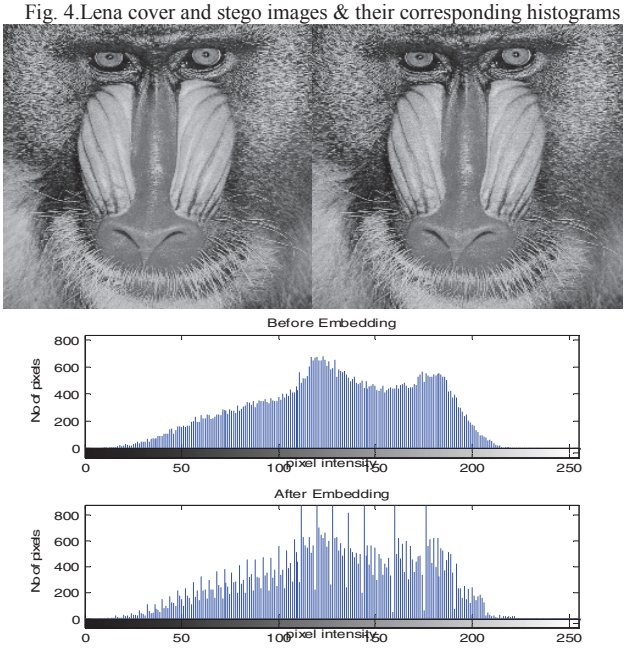

Fig. 5. Baboon cover & stego images and their corresponding histograms

Here the data is not rooted in LSBs of pixels sequentially but in random manner. This paper boasts about its imperceptibility as its PSNR values are very much above 38dB. In simple words to put it, it escapes naked eye intuition which is what needed the most in every steganographic routine. The illustrated table is nothing more than a paradigm which can be molded to any craved echelon of the user. Thus, this construct is much more conciliatory and pliable in addition to enhanced stochasticity. It is so because the carrier files reconcile themselves to revision via matrix transition and modulo. Pseudo randomly generated traversing path adds ramification which indeed turns the attack abominable.

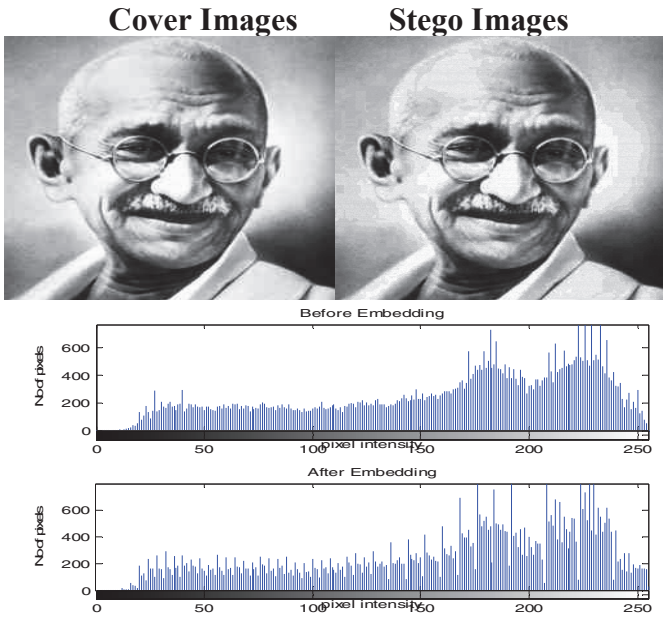

Fig. 6.Gandhi cover and stego images & their corresponding histograms

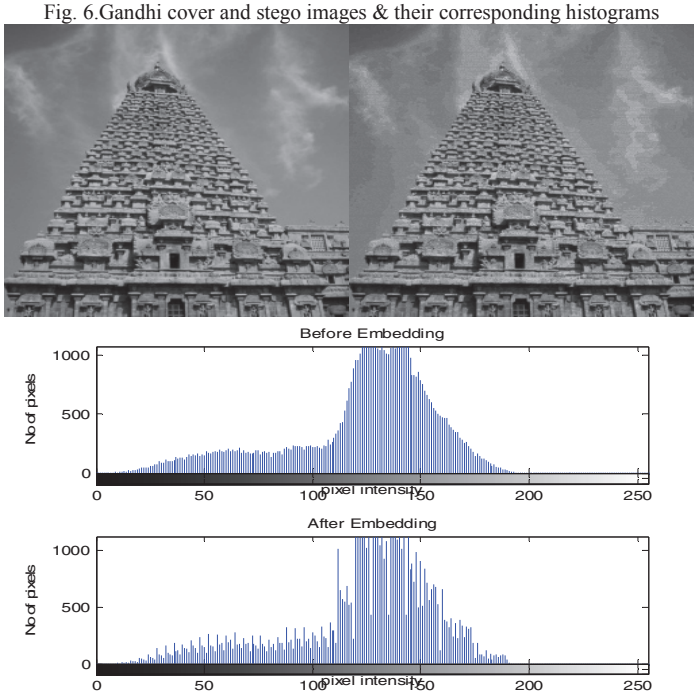

Fig. 7. Big Temple cover & stego images and their corresponding histograms

TABLE I
MSE, PSNR FOR PROPOSED METHOD

COVER IMAGE	MSE	PSNR	Total No. of bits Embedded
Lena	20.5553	35.0016	147464
Baboon	20.7396	34.9628	147658
Mahatma Gandhi	20.8176	34.9465	148971
Temple	16.9788	35.8317	147994

TABLE 2: COMPARATIVE ANALYSIS

No. of bits to be embedded	Worst case [7]	Average case [4,7,13]	Proposed Method	
	MSE	MSE	MSE	Bits Per Pixel
K=1	1	0.125	**20.5553**	**2.2501**
K=2	9	2.5		
K=3	49	42		

From the tabled results, it is pretty clear that despite lower cum varying embedding capacity for the covers, PSNR values indicate that this algorithm is too good to be attacked. Moreover the added advantage here is that the lower the embedding capacity the lower is the error and higher is the security.

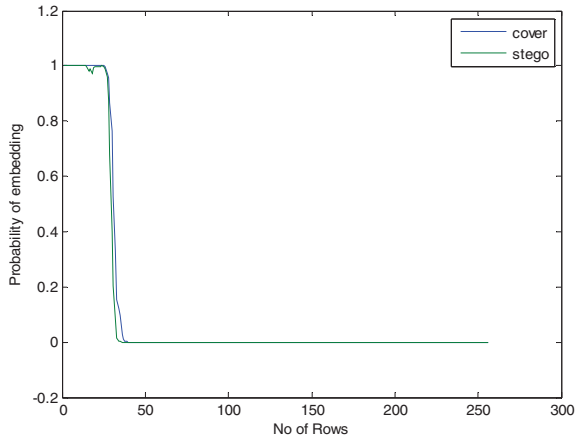

Fig. 8. Graphical results against chi- square attack

In due course, the graphical results reveal that there is only trifling divergence between original covers and their resultant stego outputs. This is the result of testing the paper against Chi-square snipe. No. of rows and embedding probability are platted in opposition to each other signifying the above mentioned. If entire rows are embedded, the probability is one else zero for no embedding. This test can disclose the clandestine information for embedding of 4 bits for the whole cover with the probability 1. Therefore, the proposed routine oeuvres and satisfies the purpose of its creation and hence extremely vigorous to chi-square run.

The proposed methodology (best case) is compared with that of worst case [7] and average case. All these results are for Lena image of 256 x256. As we see, MSE for k = 1, 2 and 3 bit embedding for both the cases are depicted. In this case, where we adopt variable bit embedding the MSE value is 20.5553 which is below half of that of the other two cases. Thus comparatively higher PSNR value is obtained. Also, in this method the BPP is 2.2501 which is fairly decent since this method embed 2, 3 or 4 bit embedding.

IV. CONCLUSION

Steganography is all about concealing the subsistence of a secret message. There is a pool of steganographic techniques available to do the above mentioned notion. In this paper projected a fresh proposal apt for image steganography to embed and retrieve Arcanum in an ergodic and adaptive manner. The algorithm has the building blocks Mean and Standard Deviation which are nothing but the basic metrics of statistical distribution. Variable bit embedding is espoused here which makes the security attack an unimaginable task. This routine has philosophical applications. Commercially it is a good stuff for the reason that it provides high embedding capability and security. Tentative results, without doubt, go hand-in-hand with this conclusion.

978-1-4673-5758-6/13/$31.00 © 2013 IEEE

ACKNOWLEDGMENT

Authors wish to thank G. Revathi, P. Shanmuga priya and A. Kingsly infant M.Tech ACS students ECE Department, School of Electrical & Electronics Engineering

REFERENCES

[1] Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt, Digital image steganography: Survey and analysis of current methods 90 (2010) 727-752.

[2] S. Katzenbeisser, F.A.P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Norwood, MA, 2000.

[3] F.A.P. Petitcolas, R.J. Anderson, M.G. Kuhn, Information hiding—a survey, Proc. IEEE 87 (7) (1999) 1062–1078.

[4] Amirtharajan, R. and J.B.B. Rayappan, 2012. An intelligent chaotic embedding approach to enhance stego-image quality. Inform. Sci., Vol. 193 (2012)115-124.

[5] Bruice Schneier, Applied Cryptography Protocols, Algorithm and Source Code in C. Second edition. Wiley India edition 2007

[6] W. Bender, D. Gruhl, N. Morimoto, A. Lu, ―Techniques for data hiding IBM Syst. J. 35 (3&4) (1996) 313–336.

[7] C.K. Chan, L.M. Chen, Hiding data in images by simple LSB substitution, Pattern Recognition. 37 (3) (2004) 469–474.

[8] Rengarajan Amirtharajan and John Bosco Balaguru Rayappan, 2012. Inverted Pattern in Inverted Time Domain for Icon Steganography.Information Technology Journal, 11: 587-595.

[9] Amirtharajan, R., Jiaohua Qin and John Bosco Balaguru Rayappan, 2012. Random Image Steganography and Steganalysis: Present Status and Future Directions. Inform. Technol. J., 11: 566-576.

[10] Sundararaman Rajagopalan, Rengarajan Amirtharajan, Har Narayan Upadhyay and John Bosco Balaguru Rayappan, 2012. Survey and Analysis of Hardware Cryptographic and Steganographic Systems on FPGA. Journal of Applied Sciences, 12: 201-210.

[11] Siva Janakiraman, Rengarajan Amirtharajan, K. Thenmozhi and John Bosco Balaguru Rayappan, 2012. Pixel Forefinger for Gray in Color: A Layer by Layer Stego. Information Technology Journal, 11: 9-19

[12] Siva Janakiraman, Rengarajan Amirtharajan, K. Thenmozhi and John Bosco Balaguru Rayappan, 2012. Firmware for Data Security: A Review. Research Journal of Information Technology, 4: 61-72.

[13] C.C. Thien, J.C. Lin, A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function, Pattern Recognition 36 (11) (2003) 2875–2881

[14] N. Provos and P. Honeyman, ―Hide and seek: An introduction to steganography, IEEE Security Privacy Mag.,1 (3) (2003) 32–44

[15] K.Thenmozhi, PadmaPriya Praveenkumar; Amirtharajan, Rengarajan; V.Pritiviraj, R.Varadharajan, Rayappan, John Bosco Balaguru, OFDM + CDMA + STEGO = SECURE COMMUNICATION - A Review, Research Journal of Information Technology 4: 31-46, 2012

[16] M. Padmaa, Y. Venkataramani and Rengarajan Amirtharajan, ―Stego on 2^n:1 Platform for Users and Embedding Information Technology Journal. 10 (10) (2011) 1896-1907.

[17] Thanikaiselvan V, Santosh Kumar, Narala Neelima, Rengarajan Amirtharajan, ―Data Battle On The Digital Field Between Horse Cavalry And Interlopers, Journal of Theoretical and Applied Information Technology, 2011, pp. 85-91.

[18] Thanikaiselvan V, Arulmozhivarman P, Amirtharajan, Rengarajan, John Bosco Balaguru Rayappan, ―Wave(Let) Decide Choosy Pixel Embedding for Stego IEEE Conference on Computer, Communication and Electrical Technology ICCCET 2011, (2011) 157 - 162 D.O.I 10.1109/ICCCET.2011.5762459

[19] Amirtharajan, R.; Subrahmanyam, R.; Prabhakar, P.J.S.; Kavitha, R.; Rayappan, J.B.B.; , "MSB over hides LSB — A dark communication with integrity," Internet Multimedia Systems Architecture and Application (IMSAA), 2011 IEEE 5th International Conference on , vol., no., pp.1-6, 12-13 Dec. 2011.

[20] Amirtharajan, Rengarajan; Mahalakshmi, V; Sridharan, Narendran; Chandrasekar, M.; John Bosco Balaguru Rayappan; , "Modulation of hiding intensity by channel intensity - Stego by pixel commando," Computing, Electronics and Electrical Technologies (ICCEET), 2012 International Conference on , vol., no., pp.1067-1072, 21-22 March 2012.

[21] Amirtharajan, Rengarajan; R, Anushiadevi.; V, Meena.; V, Kalpana.; Rayappan, John Bosco Balaguru; , "Seeable visual but not sure of it," Advances in Engineering, Science and Management (ICAESM), 2012 International Conference on , vol., no., pp.388-393, 30-31 March 2012

[22] Amirtharajan, Rengarajan; Ramkrishnan, K.; Vivek Krishna, M.; Nandhini, J.; Balaguru Rayappan, John Bosco; , "Who decides hiding capacity? I, the pixel intensity," Recent Advances in Computing and Software Systems (RACSS), 2012 International Conference on , vol., no., pp.71-76, 25-27 April 2012

[23] Thanikaiselvan, V, Arulmozhivarman. P, Rengarajan Amirtharajan, John Bosco Balaguru Rayappan, " Wavelet Pave the trio travel for a Secret mission – A Stego vision" GLOBAL TRENDS IN INFORMATION SYSTEMS AND SOFTWARE APPLICATIONS Communications in Computer and Information Science, 2012, Volume 270, 212-221,

[24] Thanikaiselvan, V, Arulmozhivarman. P, Rengarajan Amirtharajan, John Bosco Balaguru Rayappan, " Horse Riding & Hiding in Image for Data Guarding" Procedia Engineering, Volume 30, 2012, Pages 36-44

[25] Rengarajan Amirtharajan, Benita Bose, Sasidhar Imadabathuni, John Bosco and Balaguru Rayappan.(2010) " Security Building at the Line of Control for Image Stego". International Journal of Computer Applications Vol. 12. No. 5 pp.46–53, December 2010.