# Research Journal of Information Technology

ISSN 1815-7432

Academic Journals Inc.

www.academicjournals.com

Research Journal of Information Technology 5 (3): 383-392, 2013
ISSN 1815-7432 / DOI: 10.3923/rjit.2013.383.392


# Pixel Indicates, Standard Deviates: A Way for Random Image Steganography

R. Amirtharajan, V. Rajesh, P. Archana and J.B.B. Rayappan
School of Electrical and Electronics Engineering, SASTRA University, India

*Corresponding Author: R. Amirtharajan, School of Electrical and Electronics Engineering, SASTRA University, India*

## ABSTRACT

The last few decades have seen a tremendous growth in computing machines as well as the digital information with internet expansion. The transmission and storage of this huge volume of information is a high priority issue and has lead to the evolvement of information hiding and cryptographic techniques. Cryptography scrambles the message to be transmitted safely and different key sizes implement different security levels. Steganography is an information hiding technique and embeds the information in undetectable files like images or texts such that their very presence is not detected with the naked eyes. Cryptography and steganography have their own advantages and disadvantages and though each is resistant to attacks in their own ways, a combination of both results in a better cryptosystem and is a chief domain of research these days. Completely different from other methods, this paper makes use of the basic traits of statistical distribution given by mean and standard deviation; the basic building block for this paper. Embedding is done by adopting LSB substitution and PI. Bits to be infixed are decided by some prerequisites for increasing ramification. Justification for this algorithm is given by rudimentary of images along with bits per pixel and capacity of embedding. This paper promises high security and enhanced robustness as well.

**Key word:** Data security, image steganography, pixel indicator, variable bit embedding

## INTRODUCTION

Science redeems itself with inventions, redefining its dimensions with time. These new technologies and new applications not only help us but also bring with it many new threats. Thus, it is the need of the hour for the protection mechanisms to keep re-inventing itself along with their respective technologies. When businesses started to build networked computer systems, Cryptography became important (Salem *et al*., 2011; Schneier, 2007). Increased usage of PCS for communication led to virus outbreak and thanks to Internet, Firewall diligence got profited. Information Security, right now (Amirtharajan *et al*., 2012; Janakiraman *et al*., 2012a, b; Rajagopalan *et al*., 2012; Thenmozhi *et al*., 2012) has become a buzzword, with government drawing up laws to intensify surveillance and copyright infringements, making life difficult for media houses (Stefan and Fabin, 2000).

With the growing popularity of MP3 encoded music and the perfection with which copies of digital music and video are made, the entertainment industry has become nervous that their content might be pirated much more than what currently happens with analogue home taping

(Stefan and Fabin, 2000). In the course of recurrent acclivity, networking protocols, online check, trial of buccaneers, software commerce has dumped copy control. But as for music and video, technical protection mechanisms plays a vital role, of these mechanisms is copyright marking-hiding copyright notices and serial numbers in the audio or video so that pirates find it difficult to remove (Abdulfetah *et al*., 2010; Stefan and Fabin, 2000; Zeki *et al*., 2011).

One can think of encryption methodologies making wiretapping thorny for government bureaus; their common reaction is to try to restrict the strength of encryption algorithms or require that spare copies of the keys are available somewhere for them to seize (Salem *et al*., 2011; Schneier, 2007). On the other hand, the advocates of Civil liberties are outraged at this and declared it as an intolerable assault on privacy. But most police communication intelligence is not about wiretapping, so much as tracing networks of contacts. The prepaid mobile phone is the typical criminal communications tool. Criminals also hide their communication using the kind of techniques developed for copyright marking but the issue is not the secrecy of communications but their trace-ability.

Information hiding and security is very crucial for exclusive rights (Stefan and Fabin, 2000) and discretion. At times, researchers de-identify the personal information of people for processing while other times it is possible to re-identify the data subjects without too much effort. Because of so many forces driving it, research in information hiding has seen an exponential growth (Zaidan *et al*., 2010). What has been achieved in the field of cryptology from 1945-1990 (45 years) has been achieved by information hiding in the last 13 years (Stefan and Fabin, 2000).

A lot of experiments have been done (Amirtharajan *et al*., 2011, 2012; Cheddad *et al*., 2010; Gutub, 2010; Hmood *et al*., 2010a, b; Luo *et al*., 2011; Mohammad *et al*., 2011; Padmaa *et al*., 2011; Thanikaiselvan *et al*., 2011a, b; Zanganeh and Ibrahim, 2011; Zhao and Luo, 2012; EI-Safy *et al*., 2009); a large number of systems have been proposed; many of them have been broken. And as a result we now have a fair idea of what works, what doesn't and where the interesting and successful research directions are. And we can now be sure Information Hiding is the key to avoid many of the new threats.

Water marking and Steganography are two major division of Information Hiding. Classification of Steganography is as shown in the Fig. 1. Further classification can be (Stefan and Fabin, 2000), as per key, pure, secret and public key steganography. Linguistic and Technical steganography can also be stated as steganography's division. Based on the medium used for hiding (Bender *et al*., 1996), steganography can be segmented into Text (Al-Azawi and Fadhil, 2010; Xiang *et al*., 2011), Video (Al-Frajat *et al*., 2010), Audio (Zhu *et al*., 2011) and Image steganography (Amirtharajan and Rayappan, 2012a-d; Amirtharajan *et al*., 2012; Chan and Cheng, 2004; Zhao and Luo, 2012). This paper proposes a novel method for variable bit embedding through statistics of the cover pixel blend with pixel indicator to offer high payload and imperceptibility.

## PROPOSED METHOD

This is a plan to incorporate variable bit embedding through the cover statistics. First calculate the Mean and Standard deviation of 4 MSBs of every pixel of the entire image. If the pixel

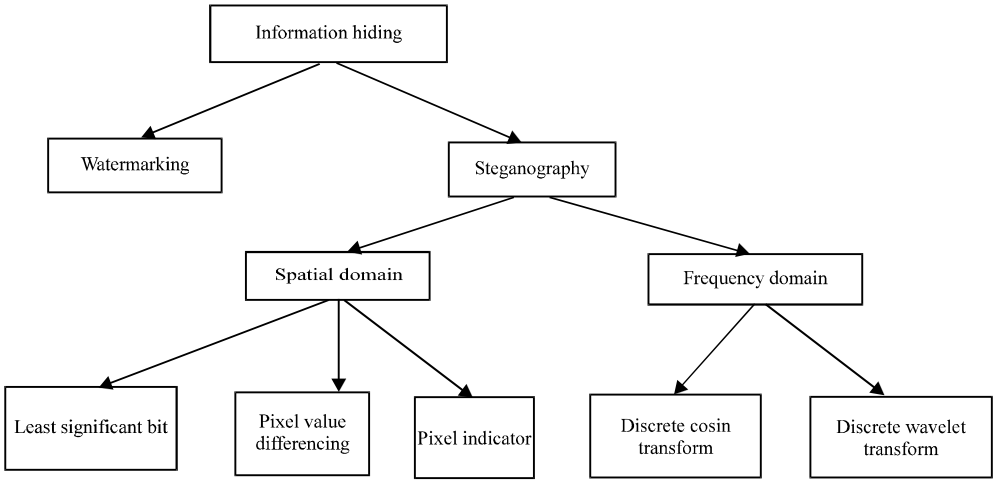


Fig. 1: Flow chart for classification of steganography

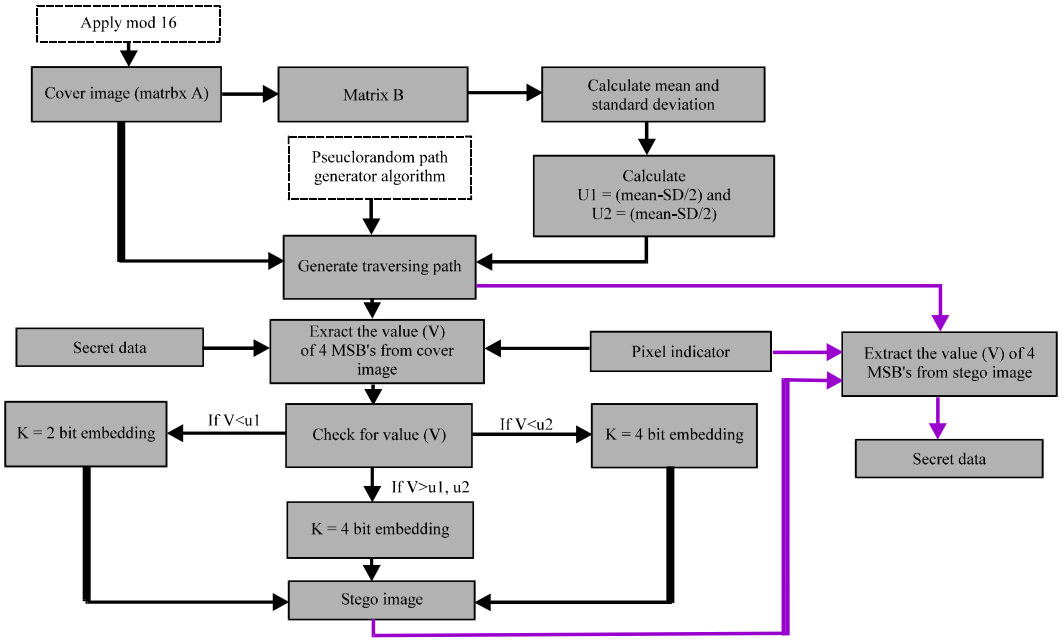


Fig. 2: Block diagram for proposed system

intensity value is less than (mean-SD/2), then 2 bits are embedded, otherwise if value is less than (mean+SD/2) 3 bits are embedded, else 4 bits are embedded. Random traversing path is used for embedding to increase disorderliness. The schematic for this study is given in Fig. 2 and flowcharts for embedding and extraction of secret information is shown in Fig. 3 and 4.

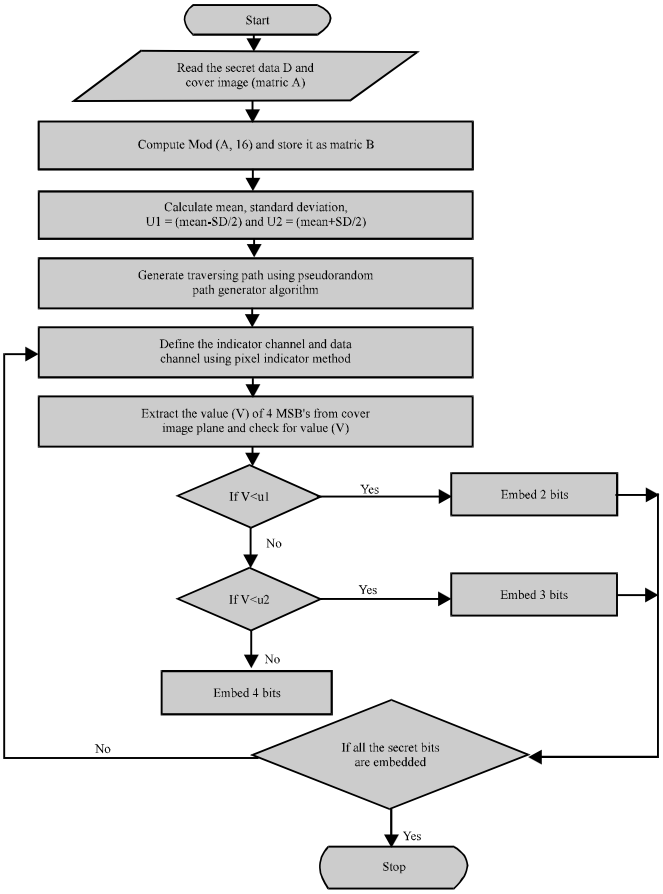


Fig. 3: Flow chart for embedding

**Embedding algorithm:**

- Assume cover image as a Matrix A
- Compute Mod(A,16) and store it as Matrix B
- Compute the mean and standard deviation of the Matrix B
- Compute the values U1 and U2 where U1=( mean - SD/2) and U2=(mean+SD/2)
- Using the Pseudorandom path generator algorithm generates a traversing path.
- Using pixel indicator method, it takes the default indicator as RED channel; Green and Blue are, say, data channels. If the LSB value of the indicator is

00: data is not embedded

01: data is embedded in Blue plane

10: data is embedded in Green plane

11: data is embedded in both planes

- Extract the value of 4MSBs for the current pixel being traversed in the cover image
- Check for the following cases and embed appropriately
  - If value < U1 k = 2 else
  - If value<U2 k = 3 else
  - K = 4
- Embed k bits in the current pixel and jump to next pixel value
- Repeat steps 6 to 8 till end of image is reached

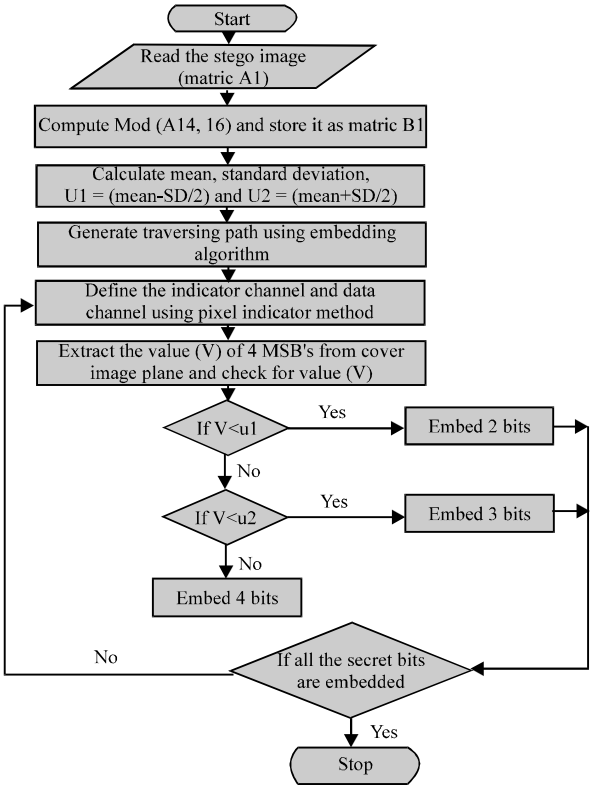


Fig. 4: Flow chart for extraction

**Extracting algorithm:**

- Assume stego image as a Matrix A1
- Compute Mod(A,16) and store it as Matrix B1
- Compute the mean and standard deviation of the Matrix B1
- Compute the values U1 and U2 where U1=(mean-SD/2)and U2=(mean+SD/2)
- Using the traversing path used in embedding algorithm traverse the image
- Using pixel indicator method, It takes the default indicator as RED channel; Green and Blue are, say, data channels. If the LSB value of the indicator is

00: data is not embedded

01: data is embedded in Blue plane

10: data is embedded in Green plane

11: data is embedded in both planes

- Extract the value of 4MSB's for the current pixel being traversed in the cover image.
- Check for the following cases and extract appropriately
  - If value < U1 k = 2 else
  - If value<U2 k = 3 else
  - K = 4
- Extract k bits in the current pixel and jump to next pixel value
- Repeat steps 6 to 8 till end of image is reached.

## RESULTS AND DISCUSSION

For experimental analysis, Lena, baboon, temple and Mahatma Gandhi of 256 x256 x3 are taken as cover as in Fig. 5a,b,c and d, respectively. As per the algorithm, the bits for embedding

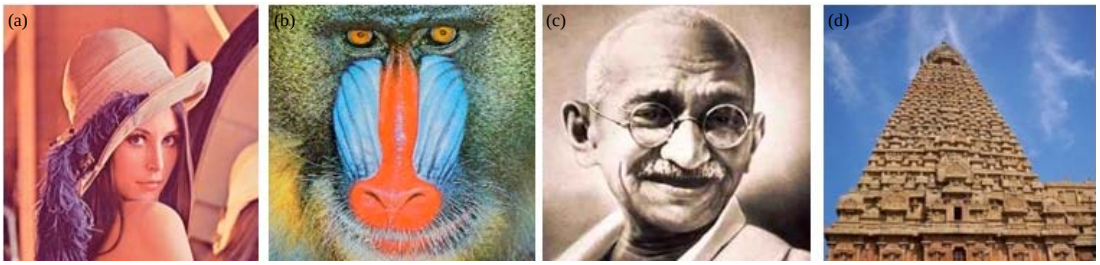


Fig. 5(a-d): Cover images, (a) Lena, (b)Baboon, (c) Mahatma Gandhi and (d) Temple

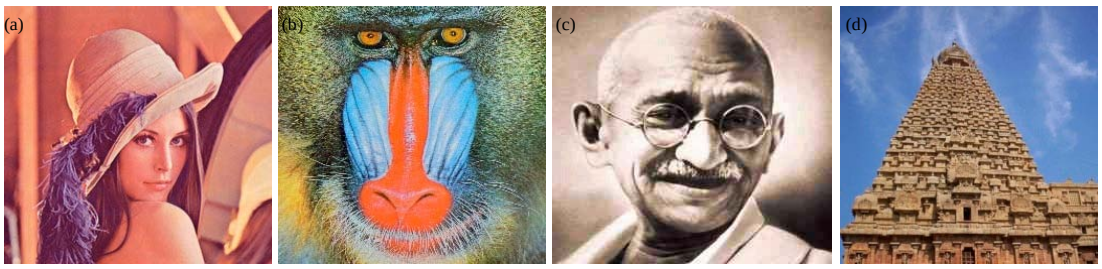


Fig. 6(a-d): Stego images, (a) Lena (b), Baboon, (c) Mahatma Gandhi and (d) Temple

vary from 2 to 4. Before embedding, each cover image submits itself to manipulation by means of conversion of matrix and modulo. The traversing path is decided by the pseudo random generator. Hence the cover image undergoes subsequent alterations even before embedding. The idea of computing mean and standard deviation also increases the complexity. The stego images of Lena, baboon, temple and Mahatma Gandhi are shown in Fig. 6a, b, c and d respectively. The histograms for both cover and stego images of Lena, baboon, temple and Mahatma Gandhi are publicized in Fig. 7a-d, respectively.

Higher PSNR indicates that the stego images are of high quality and does not seek the interest of the invader because of nil visual artifacts. MSE and PSNR are given by:

$$MSE = \frac{1}{MN} \sum_{i=1}^{M} \sum_{i=1}^{N} (C_{i,j} - S_{i,j})^2$$

Where:
M,N = Dimensions of the image
$C_{i,j}$ = The pixels in the original image
$S_{i,j}$ = The pixels of the stego-image

$$PSNR = 10\log_{10}\left(\frac{I_{max}^{2}}{M_{SE}}\right) dB$$

where, for color image $I_{max} = 255$.

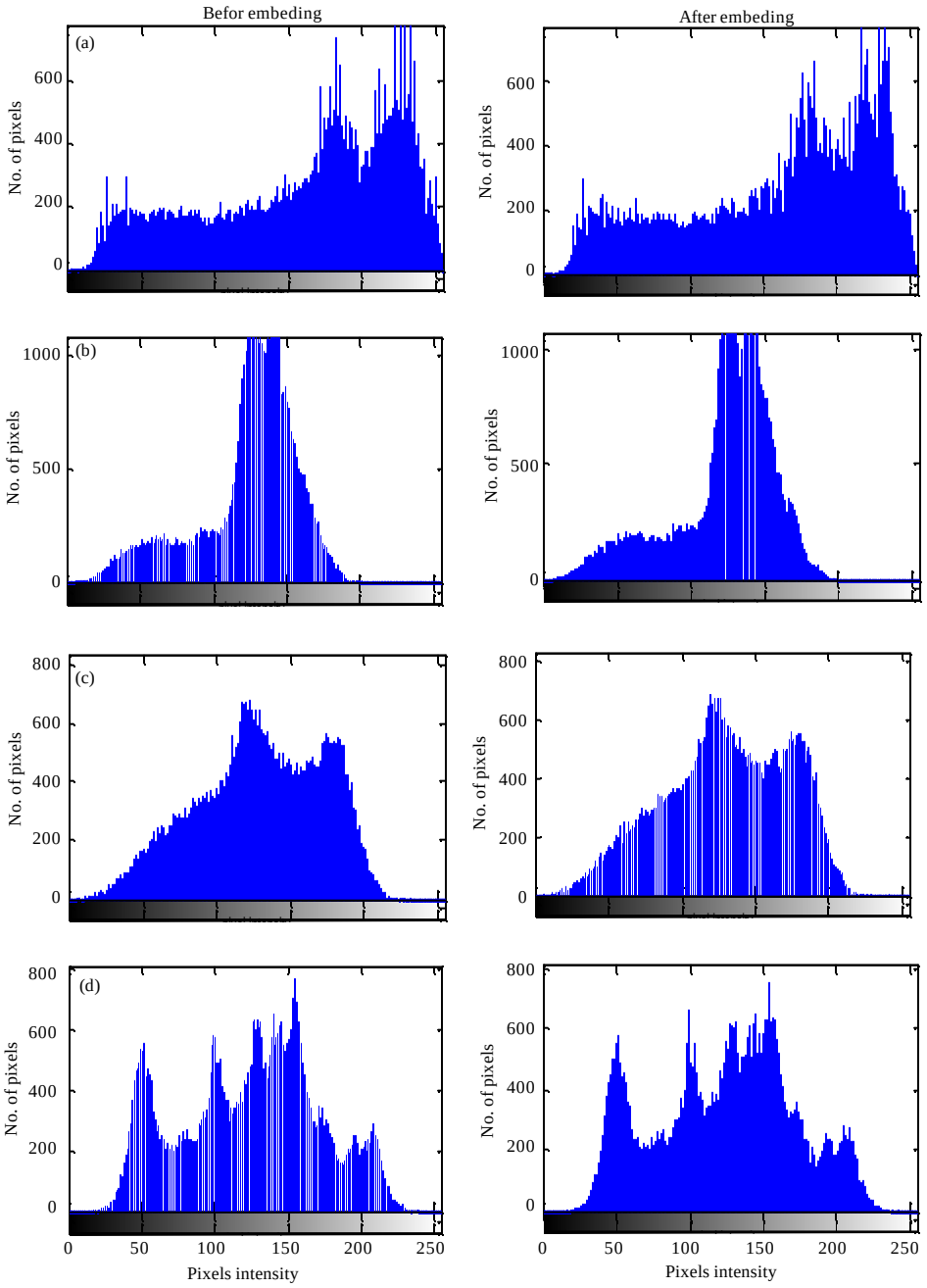


Fig. 7(a-d): Histogram of cover and stego images before and after embeding, (a) Lena, (b) Baboon, (c) Mahatma Gandhi and (d) Temple

From the Table 1, we can infer the fact that more bits are embedded in each cover image. Since, RED is the default indicator here in this algorithm, the bits per pixel value is calculated is computed for each data channel is depicted. Apart from the table and output images, the histograms of the covers and their respective stego outputs confirm the efficiency and competence level.

Table 1: MSE, PSNR, BPP values for proposed method

| | | Channel red | | Channel green | | Channel blue | | | |
|---|---|---|---|---|---|---|---|---|---|
| Cover image | PI Methods | MSE | PSNR | MSE | PSNR | MSE | PSNR | Bits per pixel | No. of bits embedded |
| Lena | Proposed | 0 | 8 | 1.9694 | 45.1875 | 1.5880 | 46.1223 | 3.7780 | 247600 |
| | Padmaa *et al*. (2011) | 1.227 | 47.24 | 1.3641 | 46.782 | 1.02 | 48.045 | 2.114 | 138549 |
| | Amirtharajan *et al*. (2012) | 2.4387 | 44.26 | 2.3066 | 44.501 | 2.3389 | 44.441 | 3.9181 | 256776 |
| Baboon | Proposed | 0 | 8 | 1.9525 | 45.2250 | 1.8269 | 45.5136 | 3.7802 | 247744 |
| | Padmaa *et al*. (2011) | 4.065 | 42.04 | 4.002 | 42.108 | 4.2847 | 41.812 | 3.657 | 239262 |
| | Amirtharajan *et al*. (2012) | 2.3702 | 44.39 | 2.3255 | 44.4657 | 2.3619 | 44.3981 | 3.9232 | 257108 |
| Mahatma gandhi | Proposed | 0 | 8 | 2.3386 | 44.4412 | 2.2619 | 44.5861 | 3.7874 | 248216 |
| | Padmaa *et al*. (2011) | 1.348 | 46.83 | 2.4212 | 47.025 | 1.2478 | 47.169 | 2.07 | 132945 |
| | Amirtharajan *et al*. (2012) | 2.5728 | 44.03 | 0.5798 | 44.2904 | 2.3595 | 44.4026 | 3.9184 | 256796 |
| Temple | Proposed | 0 | 8 | 1.8617 | 45.4318 | 2.6012 | 43.9790 | 3.7806 | 247768 |
| | Padmaa *et al*. (2011) | 1.853 | 45.45 | 1.766 | 45.662 | 1.632 | 46.003 | 2.352 | 154409 |
| | Amirtharajan *et al*. (2012) | 2.3143 | 44.49 | 2.3095 | 44.4957 | 2.3764 | 44.3716 | 3.9240 | 257160 |

## CONCLUSION

In this study a new way of image steganography is done with creative thinking. Using pixel indicator method, modulus function and pseudorandom generator resulting in a distinct embedding process, traversing path is calculated with the support of pseudorandom generator. The parameters such as mean square error, peak signal to noise ratio, bits per pixel and embedding capacity are measured for a stego-image, found to be marvelous. Since tracing the pseudorandom alignment is hectic, attacks posed on this algorithm is awful. Hence one cannot modify the content and attempts for doing so go vain. This new steganography forms a high quality stego-image as compared with the existing ones, it boasts that it can repel over any type of attacks and provides privacy as well as secure communication.

## REFERENCES

Abdulfetah, A.A., X. Sun, H. Yang and N. Mohammad, 2010. Robust adaptive image watermarking using visual models in DWT and DCT domain. Inform. Technol. J., 9: 460-466.

Al-Azawi, A.F. and M.A. Fadhil, 2010. Arabic text steganography using kashida extensions with huffman code. J. Applied Sci., 10: 436-439.

Al-Frajat, A.K., H.A. Jalab, Z.M. Kasirun, A.A. Zaidan and B.B. Zaidan, 2010. Hiding data in video file: An overview. J. Applied Sci., 10: 1644-1649.

Amirtharajan, R., R.R. Subrahmanyam, P.J.S. Prabhakar, R. Kavitha and J.B.B. Rayappan, 2011. MSB over hides LSB: A dark communication with integrity. Proceedings of the IEEE 5th International Conference on Internet Multimedia Systems Architecture and Application, December 12-14, 2011, Bangalore, Karnataka, India pp: 1-6.

Amirtharajan, R. and J.B.B. Rayappan, 2012a. An intelligent chaotic embedding approach to enhance stego-image quality. Inform. Sci., 193: 115-124.

Amirtharajan, R. and J.B.B. Rayappan, 2012b. Brownian motion of binary and gray-binary and gray bits in image for stego. J. Applied Sci., 12: 428-439.

Amirtharajan, R. and J.B.B. Rayappan, 2012c. Inverted pattern in inverted time domain for icon steganography. Inform. Technol. J., 11: 587-595.

Amirtharajan, R. and J.B.B. Rayappan, 2012d. Pixel authorized by pixel to trace with SFC on image to sabotage data mugger: A comparative study on PI stego. Res. J. Inform. Technol., 4:: 124-139.

Amirtharajan, R., J. Qin and J.B.B. Rayappan, 2012e. Random image steganography and steganalysis: Present status and future directions. Inform. Technol. J., 11: 566-576.

Bender, W., D. Gruhl, N. Morimoto and A. Lu, 1996. Techniques for data hiding. IBM Syst. J., 35: 313-336.

Chan, C.K. and L.M. Cheng, 2004. Hiding data in images by simple LSB substitution. J. Pattern Recognit. Soc., 37: 469-474.

Cheddad, A., J. Condell, K. Curran and P.M. Kevitt, 2010. Digital image steganography: Survey and analysis of current methods. Signal Process., 90: 727-752.

EI-Safy, R.O., H.H. Zayed and A. EI-Dessouki, 2009. An adaptive steganographic technique based on integer wavelet transform. Proceedings of the International Conference on Networking and Media Convergence, March 24-25, 2009, Cairo, pp: 111-117.

Gutub, A.A.A., 2010. Pixel indicator technique for RGB image steganography. J. Emerging Technol. Web Intell., 2: 56-64.

Hmood, A.K., B.B. Zaidan, A.A. Zaidan and H.A. Jalab, 2010a. An overview on hiding information technique in images. J. Applied Sci., 10: 2094-2100.

Hmood, A.K., H.A. Jalab, Z.M. Kasirun, B.B. Zaidan and A.A. Zaidan, 2010b. On the Capacity and security of steganography approaches: An overview. J. Applied Sci., 10: 1825-1833.

Janakiraman, S., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012a. Firmware for data security: A review. Res. J. Inform. Technol., 4: 61-72.

Janakiraman, S., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012b. Pixel forefinger for gray in color: A layer by layer stego. Inform. Technol. J., 11: 9-19.

Luo, H., Z. Zhao and Z.M. Lu, 2011. Joint secret sharing and data hiding for block truncation coding compressed image transmission. Inform. Technol. J., 10: 681-685.

Mohammad, N., X. Sun and H. Yang, 2011. An excellent Image data hiding algorithm based on BTC. Inform. Technol. J., 10: 1415-1420.

Padmaa, M., Y. Venkataramani and R. Amirtharajan, 2011. Stego on $2^n$: 1 Platform for users and embedding. Inform. Technol. J., 10: 1896-1907.

Rajagopalan, S., R. Amirtharajan, H.N. Upadhyay and J.B.B. Rayappan, 2012. Survey and analysis of hardware cryptographic and steganographic systems on FPGA. J. Applied Sci., 12: 201-210.

Salem, Y., M. Abomhara, O.O. Khalifa, A.A. Zaidan and B.B. Zaidan, 2011. A review on multimedia communications cryptography. Res. J. Inform. Technol., 3: 146-152.

Schneier, B., 2007. Applied Cryptography: Protocols, Algorithm and Source Code in C. 2nd Edn., Wiley, India.

Stefan, K. and A. Fabin, 2000. Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, London, UK.

Thanikaiselvan, V., P. Arulmozhivarman, R. Amirtharajan and J.B.B. Rayappan, 2011a. Wave (let) decide choosy pixel embedding for stego. Proceedings of the International Conference on Computer, Communication and Electrical Technology, March 18-19, 2011, India, pp: 157-162.

Thanikaiselvan, V., S. Kumar, N. Neelima and R. Amirtharajan, 2011b. Data battle on the digital field between horse cavalry and interlopers. J. Theor. Applied Inform. Technol., 29: 85-91.

Thenmozhi, K., P. Praveenkumar, R. Amirtharajan, V. Prithiviraj, R. Varadarajan and J.B.B. Rayappan, 2012. OFDM+CDMA+Stego = Secure Communication: A Review. Res. J. Inform. Technol., 4: 31-46.

Xiang, L., X. Sun, Y. Liu and H. Yang, 2011. A secure steganographic method via multiple choice questions. Inform. Technol. J., 10: 992-1000.

Zaidan, B.B., A.A. Zaidan, A.K. Al-Frajat and H.A. Jalab, 2010. On the differences between hiding information and cryptography techniques: An overview. J. Applied Sci., 10: 1650-1655.

Zanganeh, O. and S. Ibrahim, 2011. Adaptive image steganography based on optimal embedding and robust against chi-square attack. Inform. Technol. J., 10: 1285-1294.

Zeki, A.M., A.A. Manaf and S.S. Mahmod, 2011. High watermarking capacity based on spatial domain technique. Inform. Technol. J., 10: 1367-1373.

Zhao, Z. and H. Luo, 2012. Reversible data hiding based on Hilbert curve scan and histogram modification. Inform. Technol. J., 11: 209-216.

Zhu, J., R.D. Wang, J. Li and D.Q. Yan, 2011. A huffman coding section-based steganography for AAC audio. Inform. Technol. J., 10: 1983-1988.