Research Journal of Information Technology

ISSN 1815-7432

Academic Journals Inc.

www.academicjournals.com

Research Journal of Information Technology 5 (2): 73-86, 2013
ISSN 1815-7432 / DOI: 10.3923/rjit.2013.73.86

Pixel Indicated User Indicator: A Muxed Stego

Rengarajan Amirtharajan, P. Shanmuga Priya and J.B.B. Rayappan
Department of Electronics and Communication Engineering, School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, 613 401, India

Corresponding Author: Rengarajan Amirtharajan, Department of Electronics and Communication Engineering, School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, 613 401, India

ABSTRACT

There is more to an image than what just meets the naked eye. Images are no longer just memories or records of the past. Image steganography has made sure of this. With the growing need to secure our valuable information and data, the concept of information hiding was born. And from the day of its invention, it has evolved significantly. It has evolved from cryptography to watermarking for the copyright protection to Steganography. This study describes how the covert communication takes place effectively by means of Pixel Indicator (PI) and Pixel Value Differencing (PVD) for multi-user. The former is employed in the color cover image to separate it into three planes and any one plane indicating the data channel through its last two bits of its intensity values to entrench and the later introduces the variable bit embedding in cover image. To increase the complexity, scrambling of secret data is introduced before embedding itself. Steganalysis results proved that this method is more resistive to chi-square attack. The proposed methods performance is appraised by manipulating MSE and PSNR and the results are tabulated.

Key words: Cryptography, data hiding, information security, steganography, PI, PVD

INTRODUCTION

The dramatic increase in the multimedia and communications over the Internet protocol, the secretive transmission of data has become the want of the hour nowadays. A quick method for this purpose is the use of steganography (Amirtharajan *et al*., 2010, 2012; Wang and Wang, 2004; Hmood *et al*., 2010a, b; Zaidan *et al*., 2010) but the direct modification of the Least Significant Bit (Amirtharajan and Rayappan, 2012a-c; Chan and Cheng, 2004; Thanikaiselvan *et al*., 2011b) has resulted in quite some distortions in the image (Stefan and Fabin, 2000; Zanganeh and Ibrahim, 2011).

Apart from the general services offered by the internet, generation is getting more innovative in terms of transmission and is presently at remote desktop connections giving the users a complete Home-like experience when not in home. But the security of the Home control is lost! Hence the image or data hiding principles (Bender *et al*., 1996; Cheddad *et al*., 2010) appeared and these principles are classified based on the operation as Cryptography (Salem *et al*., 2011; Schneier, 2007) and Steganography (Janakiraman *et al*., 2012a, b; Provos and Honeyman, 2003; Rajagopalan *et al*., 2012). Cryptography being widely used in digital communications while the

latter is best used for image, audio transmission purposes. One more classification is watermarking especially for authentication purposes (Abdulfetah *et al*., 2010; Stefan and Fabin, 2000; Zeki *et al*., 2011).

Steganography's significance was nothing other than the sky after the internet evolution (Stefan and Fabin, 2000; Zanganeh and Ibrahim, 2011). The process uses a carrier image for the blinding the message and sending it over any carrier like image (Cheddad *et al*., 2010; Luo *et al*., 2011; Mohammad *et al*., 2011; Wu *et al*., 2005; Zhao and Luo, 2012), audio (Zhu *et al*., 2011), video (Al-Frajat *et al*., 2010) and text (Al-Azawi and Fadhil, 2010; Shirali-Shahreza and Shirali-Shahreza, 2008; Xiang *et al*., 2011). Importantly the steganographic embedding process must have the three important characteristics to provide a platform with high capacity for heavy and mass data to be hidden and send across (Thanikaiselvan *et al*., 2011a), aesthetic look to ensure security against visual findings and resisting any other steganalysis (Qin *et al*., 2010; Amirtharajan and Rayappan, 2012d) or random randomizations of steganography being applied on the stego image (Thenmozhi *et al*., 2012; Luo *et al*., 2011).

Looking deeper into the area of interest, image steganography is sub-classified into two domains-Spatial and Transform (Amirtharajan and Rayappan, 2012d; Thanikaiselvan *et al*., 2011a). The former is the direct manipulation on the intensities (Padmaa *et al*., 2011) and the latter involves various transforms (Amirtharajan and Rayappan, 2012d; EI-Safy *et al*., 2009; Provos and Honeyman, 2003; Thanikaiselvan *et al*., 2011a) like DCT, DWT, IWT etc.

A combination of the two domains is also possible, while the hot cake now being the adaptive technique (Gutub, 2010) which is analogous to an adaptive array of antennas where they steer based on the direction of the signal but here the method is decided based on the image type and the other parameters (Padmaa *et al*., 2011). Hence the adaptive technique can also be called smart technique leads the way to a clueless means of embedding which have proven to be more efficient in all terms, from the appeal of the cover to the maximum amount of hiding of the message (Amirtharajan and Rayappan, 2012a, b, d).

The interesting part here is that these schemes do not in any form spoil the natural appearance of the image since the area of embedding and capacity is changed dynamically depending on the cover image and payload parameters (Padmaa *et al*., 2011; Zhao and Luo, 2012). This approach is the first in the category.

The central aim of this study is to share the secret in the image confidentially and securely. For this, the secret from four different users are encrypted by four different methods using four different keys. Then, the encrypted results undergo conventional but with twist, embedding procedure to form a stego image. This indeed is a complex routine, because, to get the secret back, one should have the knowledge about encryption methods employed and their corresponding keys. Also, unless and until, one knows the plot of embedding variable bits, the retrieval process becomes a nightmare. Thus, this model assures all the parameters of a good steganographic scheme are well convinced with likelihood to put into action.

PROPOSED METHOD

Steganography is used to protect the information from illegal parties. The block diagram for this proposed method is represented in Fig. 1. In embedding block, first encrypt the secret data from four users using keys preferably Advanced Encryption Standard (AES) or of users choice may be any public key cryptography (Schneier, 2007). Then embed it in cover image using Pixel

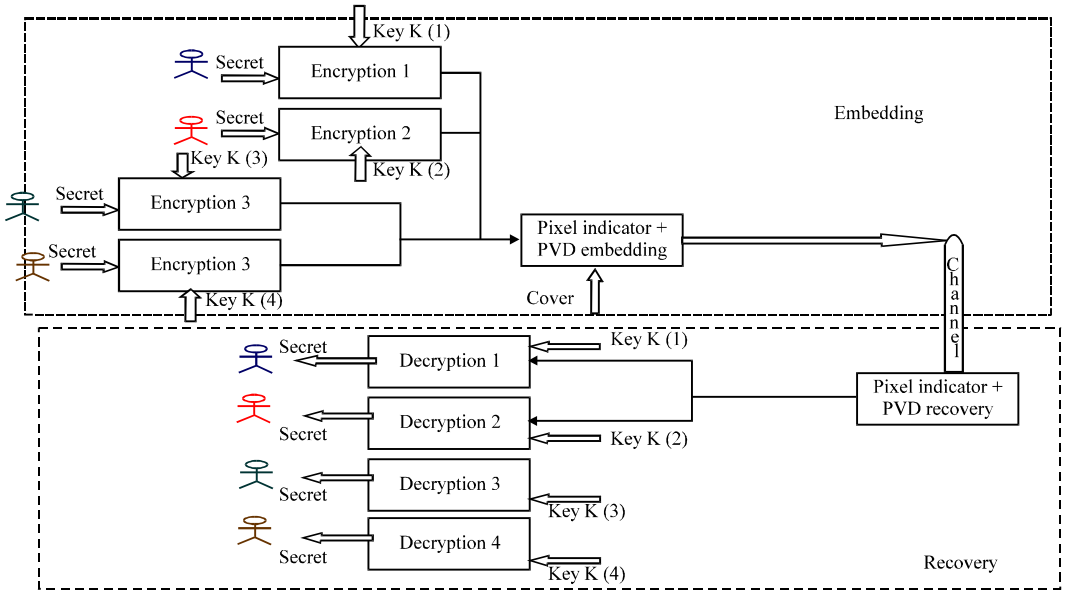

Fig. 1: Block diagram for multiuser tri-color random image steganography

Indicator (Gutub, 2010; Janakiraman *et al*., 2012a) and PVD (Padmaa *et al*., 2011; Wu *et al*., 2005). In recovery block, first recover the data and then decrypt it using keys which are used in encryption.

Three methods are discussed in this study. In method 1, red plane is the indicator channel forever and remaining two planes (i.e., blue and green planes) are data channels. In method 2, users have to select their indicator channel. In method 3, all the planes are considered as indicator channel in cyclic manner. In first two methods, data should be embedded in data channels but not in indicator channel. In third method, data should be embedded in data channels as well as in indicator channel. So Method3 gives good embedding capacity compared to the previous two methods. Flow chart for embedding and recovery are represented in Fig. 2 and 3.

Method 1: Multi user PVD with tri-color random image steganography

Embedding Algorithm:

- Read the cover image (X) and secret data (D)
- Divide the cover image into three planes (red, blue and green planes)
- Considering Red as default indicator here, do the following

Let a (0) = First LSB in red channel

Let a (1) = Second LSB in red plane

If a = 00 then there is no change, no embedding takes place

Else If a = 01, then

Scramble data of first user with key K (1), then embed this scrambled data in green plane by using PVD

Else If a = 10,

Scramble data of second user with key K (2) and then embed this scrambled data in blue plane by using PVD

Else

Scramble data of third and fourth user with key K (3) and K(4), respectively

Then embed this scrambled data in both planes (green and blue planes) by using PVD.

- Once all the users secret data is embedded, then Go to step 4
- Finally apply OPAP, then store the resulting image as Stego image (Y)

Recovery algorithm:

- Read the Stego image (Y) and separate it into three planes
- To recover the secret data, check the last two bits of the Indicator plane, here defaultly it is red plane
  If a = 00, move to next pixel
  Else If a = 01
  Then by using PVD recovery get the data of first user from Green plane and De-scramble it with Key K (1)
  Else If a = 10,
  Then by using PVD recovery get the data of second user from Blue plane and De-scramble it with Key K (2)
  Else
  Then by using PVD recovery get the data of third and fourth user from Green and Blue plane and De-scramble it with Key K (3) and Key (4), respectively
- Once all the secret data is recovered, store it as Secret Data (D)

Method 2: Multi user PVD with custom-indicator-plane tri-color random image steganography: Method 2 is same as that of Method1, except that user defined Indicator plane is defined here.

Algorithm

Method 3: Multi user PVD with cyclic-indicator-plane tri-colour random image steganography

Embedding algorithm:

- Read the cover image (X) and secret data (D)
- Divide the cover image into three planes. (Red, Blue and Green planes)
- Considering Cyclic indicator here,
  Let I (1) = Indicator plane; I (2) and I (3) = Data channels

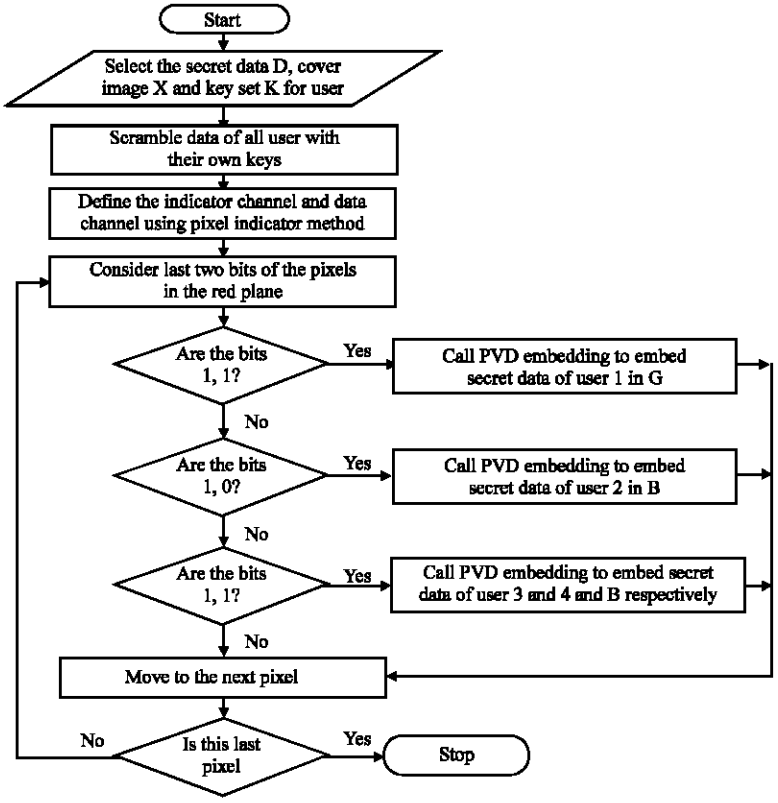

Fig. 2: Flowchart for Embedding

Algorithm: Continue

Let a(0) = First LSB in Red channel.

Let a(1) = second LSB in Red plane.

If a = 00 then there is no change, no embedding takes place.

Else If a = 01, then

Scramble Data of first user with key K (1), then embed this scrambled data in Data channel1 I(2) by using PVD.

Else If a = 10,

Scramble data of second user with key K (2) and then embed this scrambled data in data channel 2 I(2) by using PVD.

Else scramble data of third and fourth user with key K (3) and K(4), respectively

Then embed this scrambled data in both data planes by using PVD

- Once all the users secret data is embedded, then
- Go to step 4
- Finally apply OPAP and then store the resulting image as Stego image (Y)

Recovery algorithm

- Read the Stego image (Y) and separate it into three planes
- To recover the secret data, check the last two bits of the Indicator plane

If a = 00, move to next pixel

Else If a = 01

Then by using PVD recovery get the data of first user from Data Channel1 I(1) and De-scramble it with Key K (1)

Else If a = 10,

Then by using PVD recovery get the data of second user from Data Channel2 I(2) and De-scramble it with Key K (2)

Else

Then by using PVD recovery get the data of third and fourth user from both Data Channels and De-scramble it with Key K (3) and Key (4), respectively.

Once all the secret data is recovered, store it as Secret Data (D)

RESULTS AND DISCUSSION

In this presentation, Lena, Baboon, Mahatma Gandhi and Temple are chosen as cover images of size 256×256×3 and its stego images and histograms are shown in Fig. 4-7 for Method 1 and in Fig. 8-11 for Method 3.This implementation has been simulated in MATLAB 7.1 and its MSE and PSNR values are tabulated in Table 1-3 for all the three methods.

Method 1: The proposed stego method effectiveness can be estimated by calculating MSE and PSNR for stego image $S_{i,j}$ and cover image $O_{i,j}$. The mathematical expressions are given here:

$$MSE = \frac{1}{MN}\sum_{i=j}^{M}\sum_{j=1}^{N}\left(o_{i,j} - s_{i,j}\right)^2$$

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

For method1 and method3, the stego images and its histograms are shown in Fig. 4-11. The result shows that, there is no visual distortion in those images. The histograms of cover and Stego images are nearly identical, so it is difficult to hit the data. This grants better image quality even after embedding data of all the users.

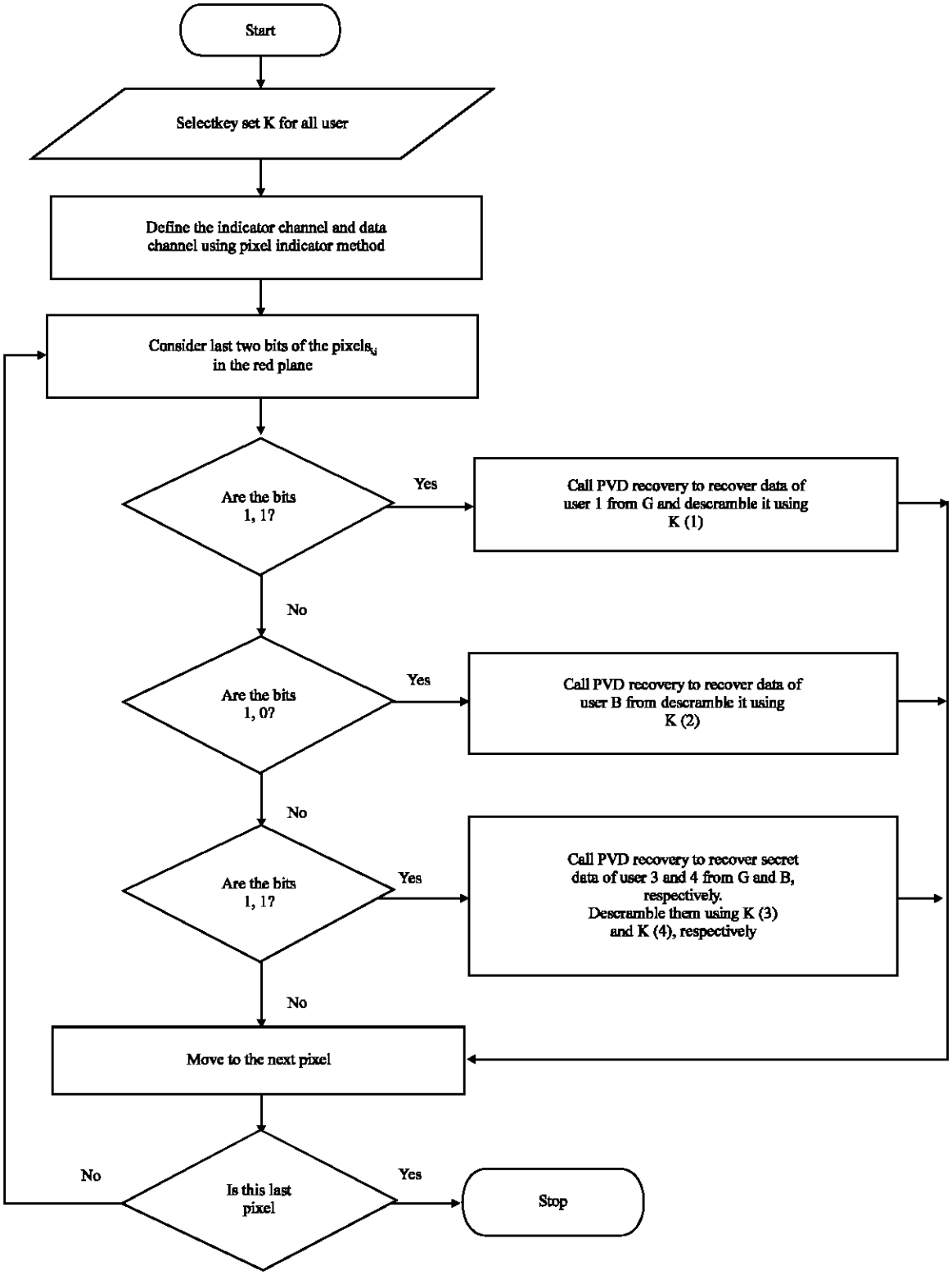

Fig. 3: Flowchart for Extraction

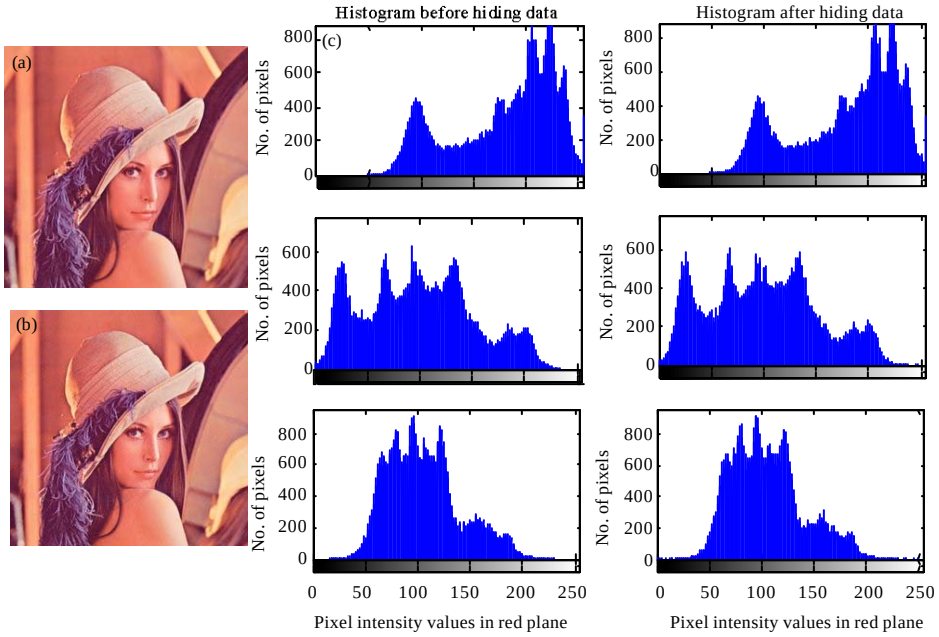

Fig. 4(a-c): Method 1, Lena (a) Cover images (b) Stego images and (c) Corresponding histograms of cover and stego images before and after hidding data

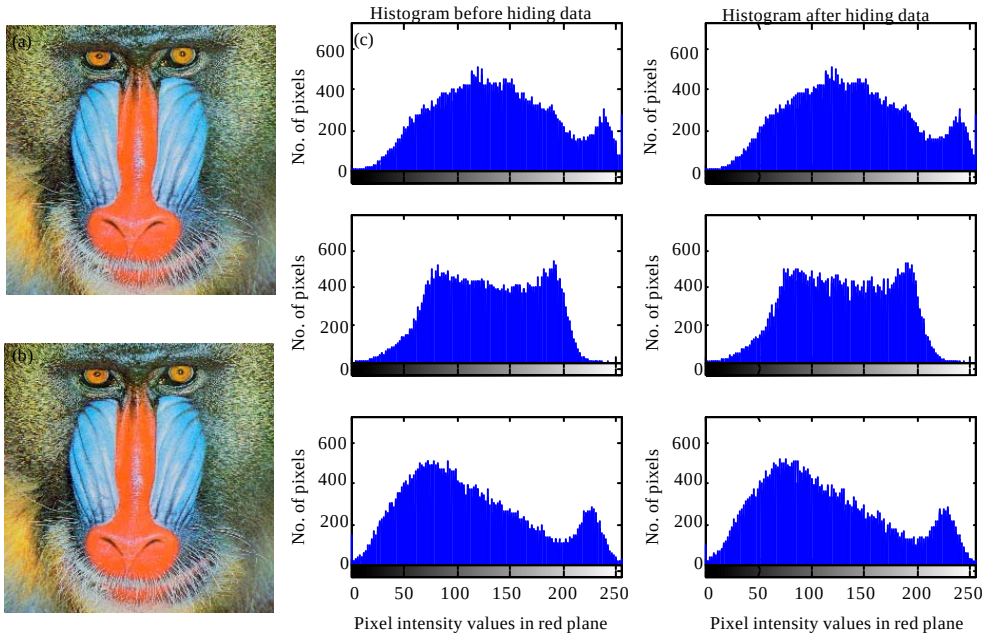

Fig. 5(a-c): Method 1, Baboon (a) Cover images (b) Stego images and (c) Corresponding histograms of cover and stego images before and after hidding data

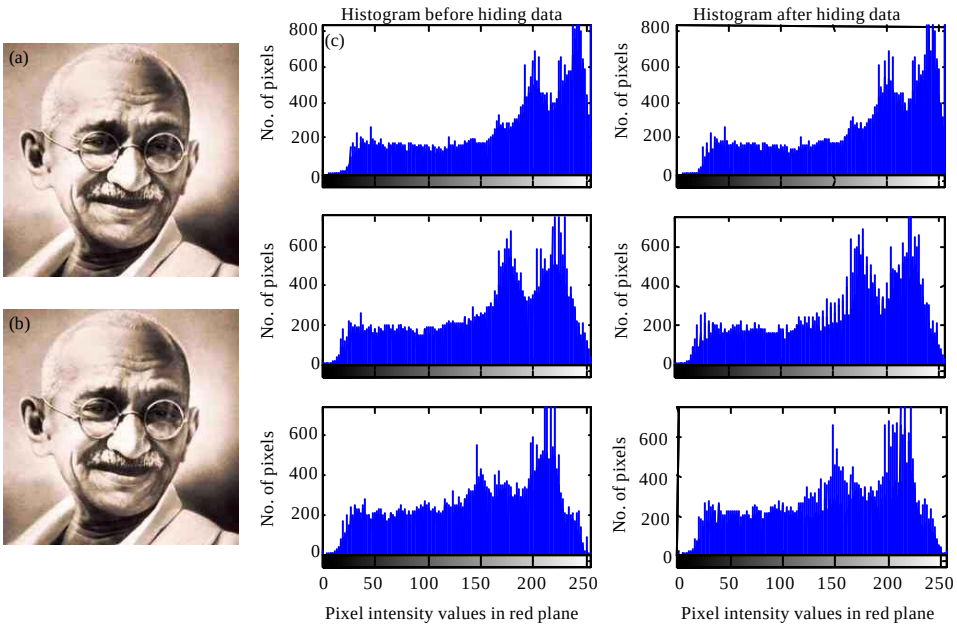

Fig. 6(a-c): Method 1, Mahatma Gandhi (a) Cover images (b) Stego images and (c) Corresponding histograms of cover and stego images before and after hidding data

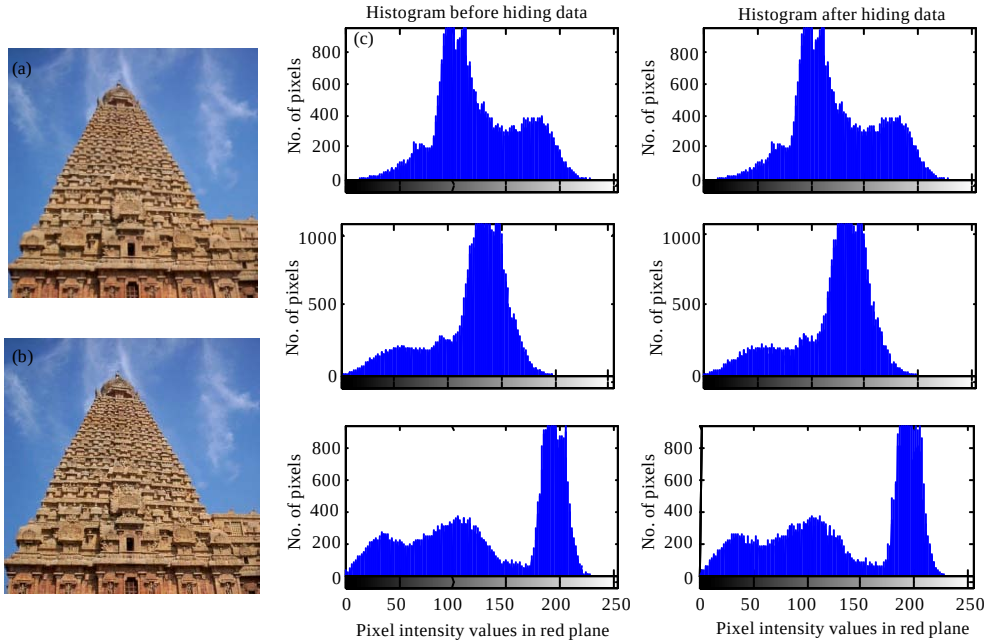

Fig. 7(a-c): Method 1, Temple (a) Cover images (b) Stego images and (c) Corresponding histograms of cover and stego images before and after hidding data

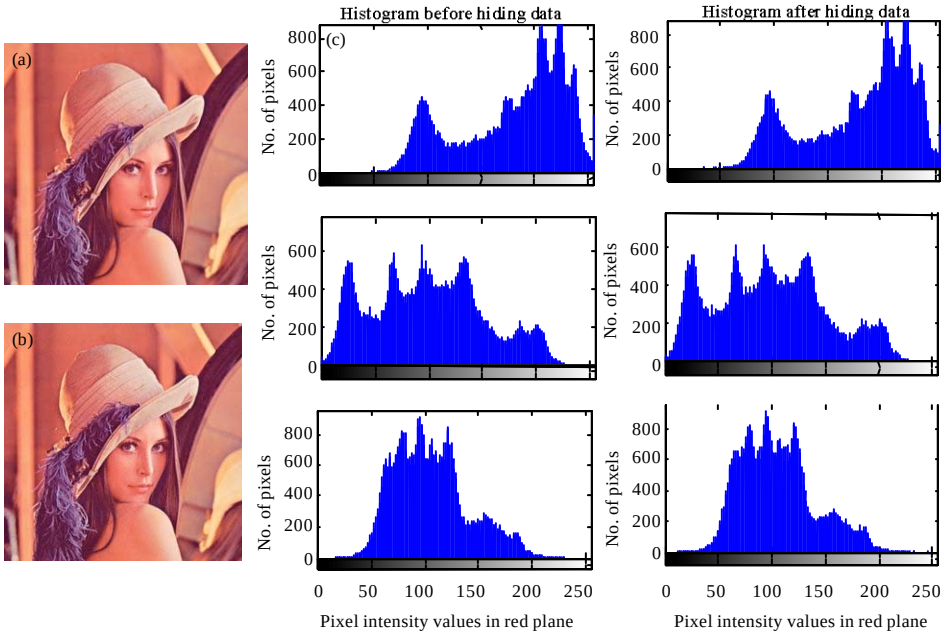

Fig. 8(a-c): Method 3, Lena (a) Cover images (b) Stego images and (c) Corresponding histograms of cover and stego images before and after hidding data

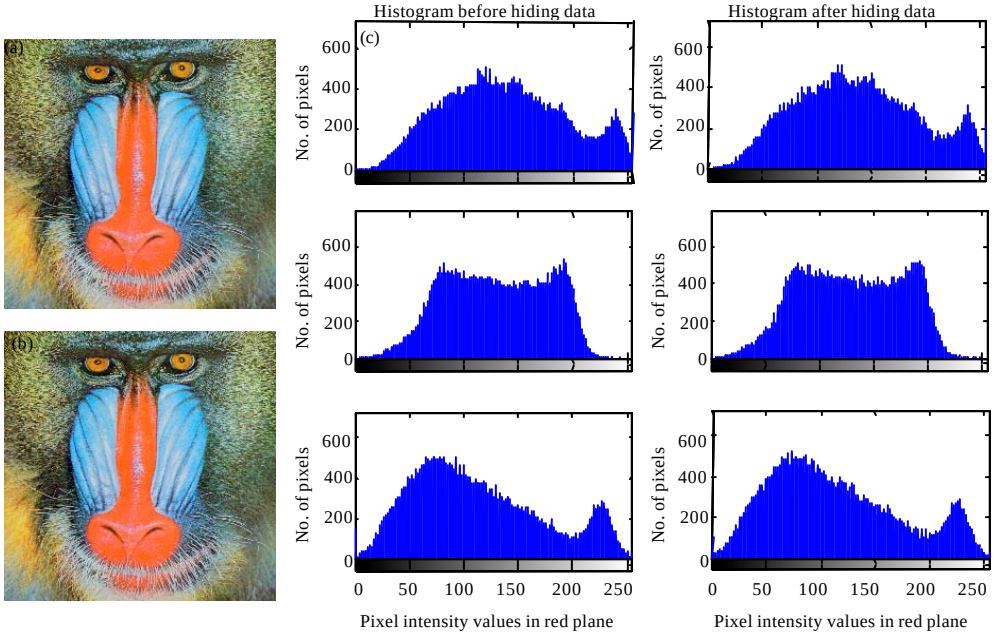

Fig. 9(a-c): Method 3, Baboon (a) Cover images (b) Stego images and (c) Corresponding histograms of cover and stego images before and after hidding data

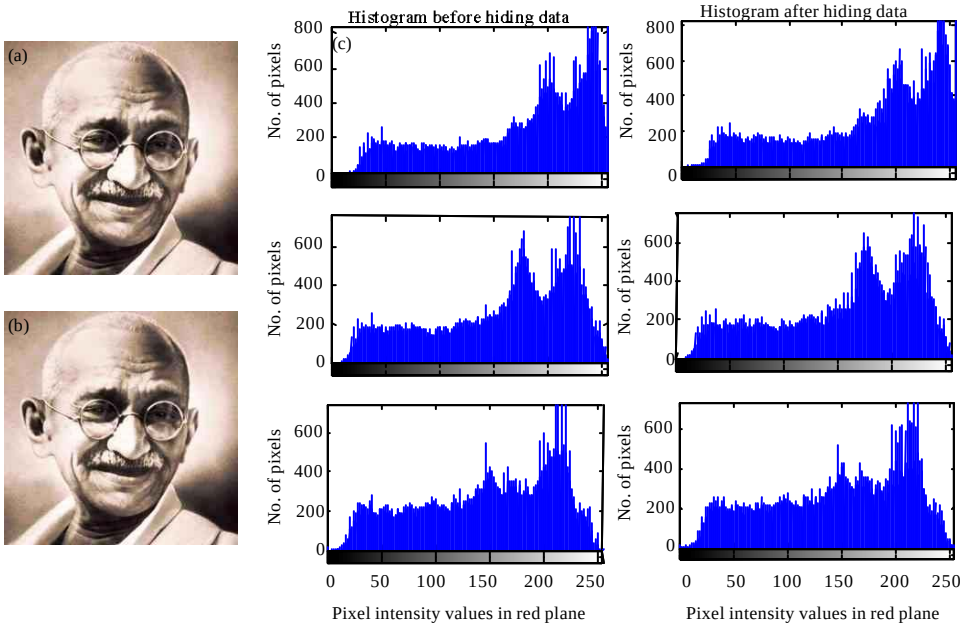

Fig. 10(a-c): Method 3, Mahatma Gandhi (a) Cover images (b) Stego images and (c) Corresponding histograms of cover and stego images before and after hidding data

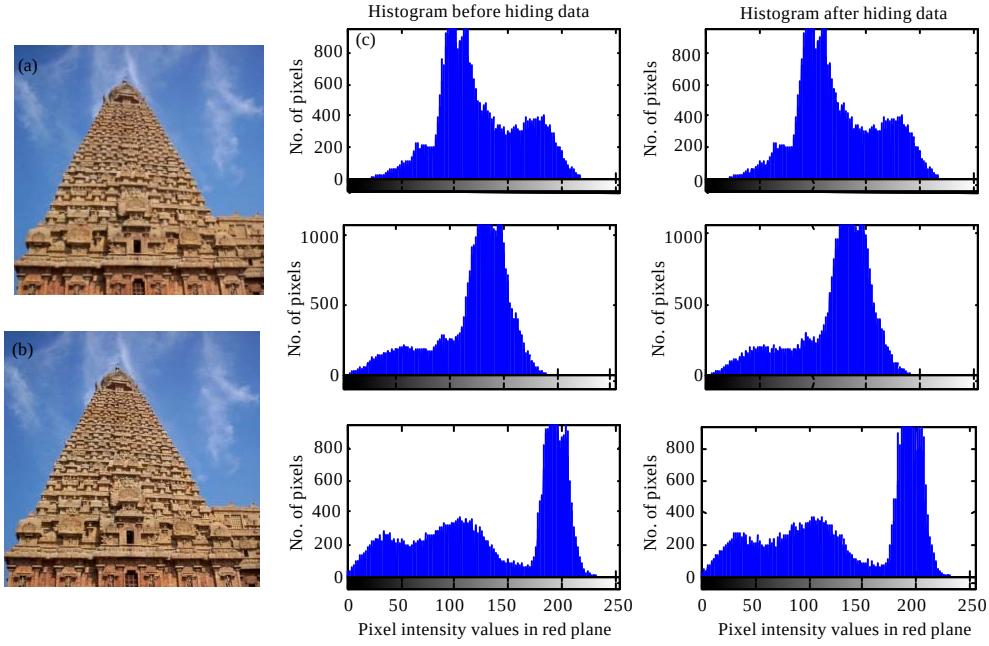

Fig. 11(a-c): Method 3, Temple (a) Cover images (b) Stego images and (c) Corresponding histograms of cover and stego images before and after hidding data

Table 1: MSE, PSNR values for method 1

	Channel I red		Channel II green		Channel III blue		Bits per pixel (BPP)			
Cover image	MSE	PSNR	MSE	PSNR	MSE	PSNR	R	G	B	Total No. of bits embedded
Lena	0	8	2.1408	44.8250	1.6205	46.0343	0	1.1032	1.0437	140702
Baboon	0	8	6.1348	40.2528	6.5066	39.9973	0	1.8314	1.8469	241066
Mahatma Gandhi	0	8	1.8947	45.3553	1.7909	45.6000	0	1.0280	1.0460	135933
Temple	0	8	2.6518	43.8954	2.5739	44.0248	0	1.1739	1.1717	153728

Table 2: MSE, PSNR values for method 2

	Channel I red		Channel II green		Channel III blue		Bits per pixel (BPP)			
Cover image	MSE	PSNR	MSE	PSNR	MSE	PSNR	R	G	B	Total No. of bits embedded
Lena	1.8749	45.4010	0	8	1.5974	46.0967	1.0630	0	1.0443	138111
Baboon	6.1219	40.2620	0	8	6.6008	39.9348	1.8195	0	1.8517	240601
Mahatma Gandhi	1.8806	45.3878	0	8	1.7635	45.6671	1.0090	0	1.0104	132353
Temple	2.6854	43.8407	0	8	2.5834	44.0090	1.1981	0	1.1748	155515

Table 3: Comparative results of MSE, PSNR values for method 3 with Padmaa *et al.* (2011)

	Channel I red		Channel II green		Channel III blue		Bits per pixel (BPP)			
Cover image	MSE	PSNR	MSE	PSNR	MSE	PSNR	R	G	B	Total No. of bits embedded
Lena										
Proposed	1.2572	47.13	1.3788	46.7357	1.04	47.959	0.701	0.724	0.687	138496
Padmaa *et al.* (2011)	1.227	47.24	1.3641	46.782	1.02	48.045	0.702	0.724	0.688	138549
Baboon										
Proposed	3.9377	42.1784	4.0462	42.0604	4.2185	41.8793	1.2108	1.2110	1.2275	239161
Padmaa *et al.* (2011)	4.065	42.04	4.002	42.108	4.2847	41.812	1.212	1.211	1.228	239262
Mahatma Gandhi										
Proposed	1.2402	47.1960	1.2859	47.0388	1.1931	47.3639	0.6702	0.6823	0.6781	133082
Padmaa *et al.* (2011)	1.348	46.83	1.2901	47.025	1.2478	47.169	0.670	0.681	0.6776	132945
Temple										
Proposed	1.8530	45.4520	1.7542	45.6900	1.7343	45.7396	0.7998	0.7748	0.7809	154373
Padmaa *et al.* (2011)	1.853	45.45	1.766	45.662	1.632	46.003	0.801	0.771	0.7798	154409

From the Table 1-3, its observed that, baboon color image of size 256×256×3 gives better embedding capacity compared to other three images in all the three methods and the proposed method offers better imperceptibility and also it varies from cover to cover. Mahatma Gandhi image provides good PSNR in all the three methods, which gives better imperceptibility along with good image quality.

Security analysis: To randomize each user secret data, Advanced Encryption Standard (AES) is introduced here, it offers 2^128 complexity in the system. Assuming 25% probability on each cases say 00,01,10,11, which decides the embedding capacity. The total complexity for four users will be 2^128*0.5*2*4.

Chi-square attack is a Steganalysis technique. This is based on probability of embedding data in an image. Figure 12 presents the graphical view of chi-square attack in Mahatma Gandhi image.

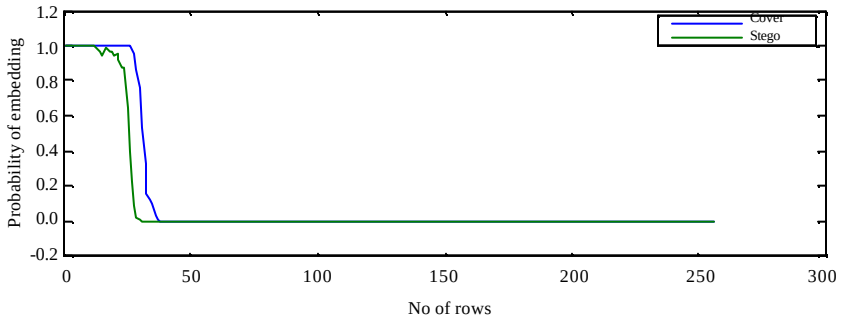

Fig. 12: Graphical representation of Mahatma Gandhi against chi-square attack

The graph is plotted between probability of embedding and number of rows in an image. It clearly proves that, the cover and stego are nearly alike, so this proposed method survives against chi-square attack.

CONCLUSION

Today innovative thinking sounds good, so this presentation gives the creative idea by using PVD, PI and OPAP. Pixel value differencing process gives smart embedding in all the planes provides visually undistorted image. Pixel Indicator for color cover image offers increase in embedding capacity by the way of embedding secret data in indicator plane. To make the stego image indistinguishable with cover image, of course OPAP afford this. The power of the algorithm can be tested against chi-square attack, which gives the awesome result. So this proposed method stand unique compared with all other existing methods.

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., D. Adharsh, V. Vignesh and R.J.B. Balaguru, 2010. PVD blend with pixel indicator-OPAP composite for high fidelity steganography. Int. J. Comput. Appl., 7: 31-37.

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, 2012. 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.

Provos, N. and P. Honeyman, 2003. Hide and seek: An introduction to steganography. IEEE Secur. Privacy, 1: 32-44.

Qin, J., X. Xiang and M.X. Wang, 2010. A review on detection of LSB matching steganography. Inform. Technol. J., 9: 1725-1738.

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.

Shirali-Shahreza, M. and S. Shirali-Shahreza, 2008. High capacity persian/arabic text steganography. J. Applied Sci., 8: 4173-4179.

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.

Wang, H. and S. Wang, 2004. Cyber warfare: Steganography vs. steganalysis. Commun. ACM, 47: 76-82.

Wu, H.C., N.I. Wu, C.S. Tsai and M.S. Hwang, 2005. Image steganographic scheme based on pixel-value differencing and LSB replacement methods. Proc. IEEE Vision Image Signal, 152: 611-615.

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.