Research Journal of Information Technology

ISSN 1815-7432

Academic Journals Inc.

www.academicjournals.com

Research Journal of Information Technology 5 (3): 277-290, 2013
ISSN 1815-7432 / DOI: 10.3923/rjit.2013.277.290

High Performance Pixel indicator For Colour Image Steganography

Rengarajan Amirtharajan, K. Mohamed Ashfaaq, A. Kingsly Infant 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

In this study, a steganographic run is espoused for images with LSB as a building block. Living in the world of advanced technologies where zillions of people get connected online every day, problem of cyber crimes has also become inevitable. Since innumerable digital files are exchanged, importance given to problem solving measures has also up risen. For the security of images sake, steganography has introduced many modus operandi which are implementable both commercially and domestically. Steganography involves the hiding of data such that it is invisible to the naked eye and it also aims at hiding the very existence of the message itself by a cover medium which could be image or audio or video. Depending on the need of the user, any type can be used. Image steganography is very prevalent among these three. The choice of the algorithm is driven by parameters such as veracity, sturdiness, capacity and availability. Modified LSB is used in this algorithm but with a different perspective that give adequate implication to all of the previously mentioned. The algorithm is rationalized by means of MSE and PSNR results.

Key words: Data hiding, distortion, embedding rate, pixel indicator, steganography

INTRODUCTION

We are now living in a world where data is analogous to currency; precious, vulnerable and can be used by anybody. However if data were to be plundered and used, it would give rise to inequity and immorality thus unleashing anarchy in the world. It is therefore a necessity to preserve data and prevent it from being used unlawfully (Schneier, 2007). Integrity of data is very important especially when one is dealing with data that can alter the Geo-economics. Such data have to carefully deal with and should be safely kept away from hackers and espionages (Amirtharajan and Rayappan, 2012a-d; Bender *et al*., 2000). But with data being so extensive and obvious how would one achieve the security of stochastic data?

Back during the ancient times, symbols and encryptions were used to communicate secret messages; messages were converted to gibberish and then back to perceivable message (Kahn, 1996). Over time the art of cryptography evolved to Cipher texts. Scholars and Mathematicians came up with different methods of encryption of data to make the secret message inaccessible to interceptors. With the advancement of digital systems cryptology evolved and took various forms but so did the controversies (Schneier, 2007). Cryptography attracted lot of attention to itself. It facilitated privacy but failed to protect the communicating parties, it also an act of incrimination in some countries to use cryptography.

Steganography the idea "security through obscurity" was the brain child Johannes Trithemius in 1499 that answered the puzzling question (Stefan and Fabin, 2000). Although this technique is of Greek origin the first documented usage was in his first book Steganographia which was known as the book of magic. Steganography was an extrapolation of Cryptography. Steganography on the other hand concealed the data and its communicator (Amirtharajan *et al*., 2011, 2012; Cheddad *et al*., 2010; Hmood *et al*., 2010a, b; Janakiraman *et al*., 2012a, b; Padmaa *et al*., 2011; Thenmozhi *et al*., 2012). The digital Steganography involved a carrier medium "Cover" such as a document (Al-Azawi and Fadhil, 2010; Xiang *et al*., 2011; Yang *et al*., 2011), audio (Zhu *et al*., 2011), video (Al-Frajat *et al*., 2010) or an image (Chan and Cheng, 2004; Gutub, 2010; Hong *et al*., 2009; Luo *et al*., 2008, 2011; Zanganeh and Ibrahim, 2011; Zhao and Luo, 2012) which supported fractionation. The data to be embedded was the secret message and the medium after the embedment "the stego image" (Mohammad *et al*., 2011; Rajagopalan *et al*., 2012; Zaidan *et al*., 2010, 2011).

The choice of the algorithm is driven by parameters such as Integrity, robustness, capacity, availability (Amirtharajan and Rayappan, 2012a, b, c, d). The other factor that drives the choice of algorithm is the domain in which the data is encoded i.e. spatial domain (Thanikaiselvan *et al*., 2011) and frequency domain (Amirtharajan and Rayappan, 2012a, b, c, d; Cheddad *et al*., 2010). The counter attack called steganalysis (Qin *et al*., 2009, 2010), which tries to reveal the existence of confidential information (Xia *et al*., 2009). The other classification in information hiding exclusively for authentication and copyright protection is called watermarking (Zeki *et al*., 2011; Zhang *et al*., 2010).

The data to be covertly transmitted is embedded directly in the image pixels in the spatial domain. But in the case of transfer domain steganography secret bits are embedded into the coefficients values of the transform domain (Amirtharajan and Rayappan, 2012d).

Steganography has four main modules; they are as follows (Amirtharajan *et al*., 2011, 2012):

- A cover file which acts as the container/carrier for the secret message
- A secret message that contains the confidential data
- A key for encoding the secret message
- A steganography algorithm or function to sneak the secret message inside the cover object

Blend of these Stego output components creates the stego output which is then transmitted to the recipient. At the destination, using decoding routine undisclosed message is got back from the stego output.

There are three main characteristics of steganography. They are imperceptibility, capacity and its robustness (Zaidan *et al*., 2010). The total amount of confidential information that can be hidden in a Stego-image defines its capacity. Robustness is the limit of modifications an adversary would have to do before he can break the secret code and get the hidden message (Gutub, 2010). Imperceptibility is how well the secret image is hidden before an intruder finds out about the hidden message, i.e., invisibility to human eyes (Amirtharajan *et al*., 2011, 2012; Zhang, 2010). Studying the available methods and its characteristics, this study has been proposed to implement a method to improve the imperceptibility and complexity by adapting Pixel Indicator (Gutub, 2010; Padmaa *et al*., 2011) along with modified LSB to reduce distortion (Zhang, 2010).

PROPOSED METHODOLOGY

The study takes the fundamental concept of LSB substitution along with Pixel indicator method (Gutub, 2010; Padmaa *et al.*, 2011) and follows the same but with different reckon. Two such methods are advised here; one with default indicator and other with cyclic indicator. LSB substitution offers enhanced quality and capacity. Separating LSB planes is not a usual way that too here it is limited for 3 planes. On the word of indicator, confidential data is embedded in data channels by modifying the cover image samples by ±1 and ±2. The schematic diagram and flowchart for this study is given in Fig. 1 and 2.

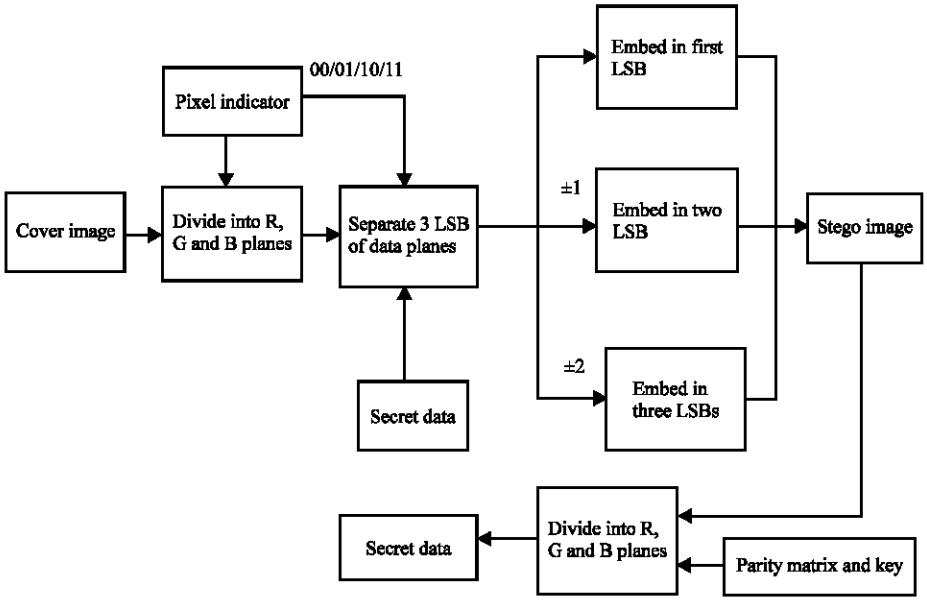

Fig. 1: Block diagram for proposed method

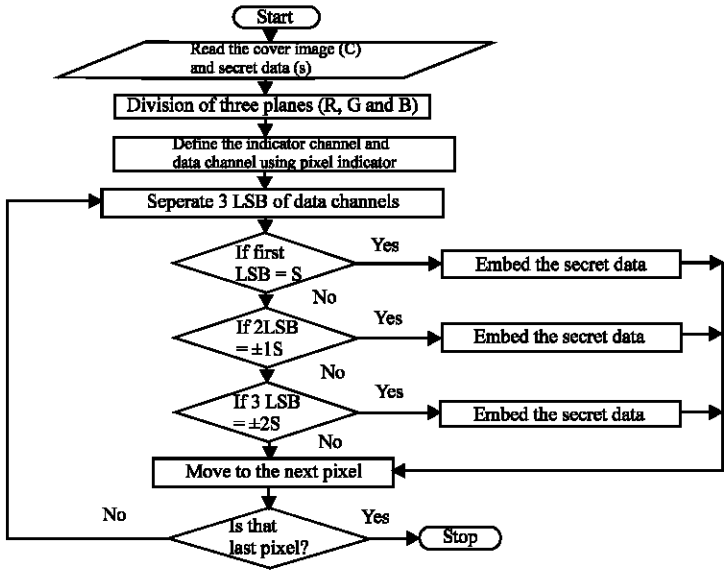

Fig. 2: Flow chart for proposed method

Algorithm for embedding

Method 1:

- Read the cover (C) and secret data to be embedded (D)
- Divide the cover image into R, G, B planes
- Take Red plane as default indicator and follow the below mentioned rules:
  If last two LSBs of the indicator is:
  - 00 = No embedding
  - 01 = embed in blue plane
  - 10 = embed in green plane
  - 11 = embed in both green and blue planes
- Separate 3 LSB planes in Green and Blue
- Take first bit of secret data and compare it with the first LSB of the data channel plane. If it matches then embed the bit
- Take the next two bits of secret data and compare it with the two LSBs. Only allow ±1 modification
- Take 3 bits of secret data and compare it with the three LSBs and allow ±2 modification
- Repeat the process till all the secret data is embedded
- Store the resultant image as stego image
- Generate the stego key for embedding and communicate it to the receiver

Method 2

Cyclic PI approach:

- Read the cover (C) and secret data to be embedded (D)
- Divide the cover image into R, G, B planes
- Cyclic indicator is selected in this method; that is if red is default indicator for pixel 1, then green is the indicator for pixel 2 and blue for pixel 3. The remaining two act as data channels.
  If last two LSBs of the indicator is:
  - 00 = No embedding
  - 01 = Embed in blue plane
  - 10 = Embed in green plane
  - 11 = embed in both green and blue planes
- Separate 3 LSB planes in Green and Blue
- Take first bit of secret data and compare it with the first LSB of the data channel plane. If it matches then embed the bit
- Take the next two bits of secret data and compare it with the two LSBs. Only allow ±1 modification
- Take 3 bits of secret data and compare it with the three LSBs and allow ±2 modification
- Repeat the process till all the secret data is embedded
- Store the resultant image as stego image
- Generate the stego key for embedding and communicate it to the receiver

Algorithm for extraction:

- Read the stego image
- Split the image into R, G, B planes and then divide by 3 LSB planes
- Select the indicator channel and data channel with respect to 2 methods

Using stego key from embedding extract all the secret data bits.

RESULTS AND DISCUSSION

The algorithm is tested in MATLAB 7.1 with cover images as Baboon, Lena, Mahatma Gandhi and Kovil which are of 256×256×3. The obtained MSE and PSNR values are tabulated. In method 1, default indicator is RED. Hence, no embedding is done on that plane. As it is evident, Kovil image affords high PSNR of 69.7667 dB. Any stego image of higher 38dB is said to be a high quality one. All four images are said to be highly imperceptible, escaping naked eye attempt. Histograms also depict the same results. Cover images with their corresponding stego images and histograms for the subsequent cover and stego images for method 1 are shown in Fig. 3-5 and 6. Analytical results for method 1 are tabled in Table 1.

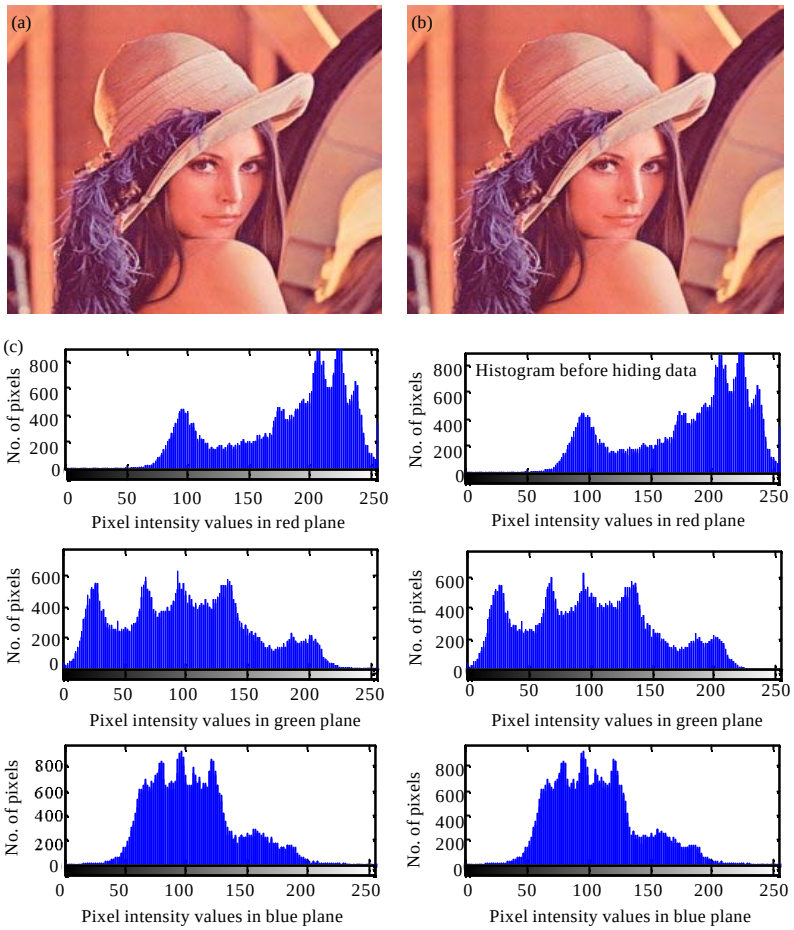

Fig. 3(a-c): Method 1: (a) Cover, (b) Stego images for Lena and (c) Corresponding histograms for 3a

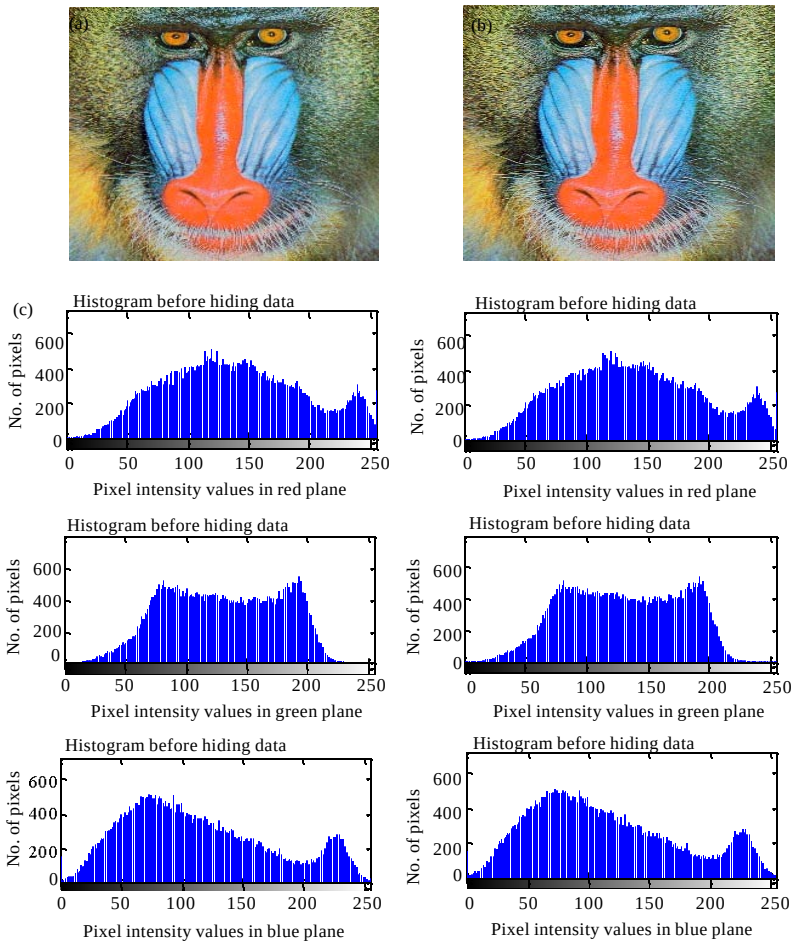

Fig. 4(a-c): Method 1: (a) Cover, (b) Stego images for Baboon and (c) Corresponding histograms for 4a

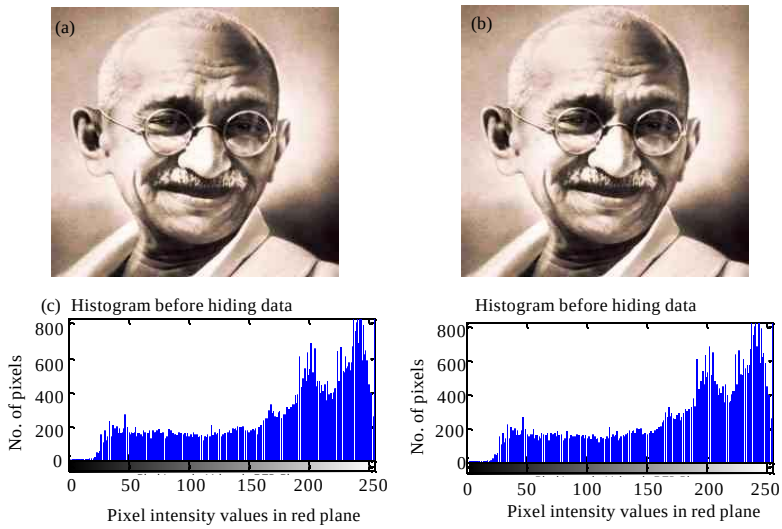

Fig. 5(a-c): Continue

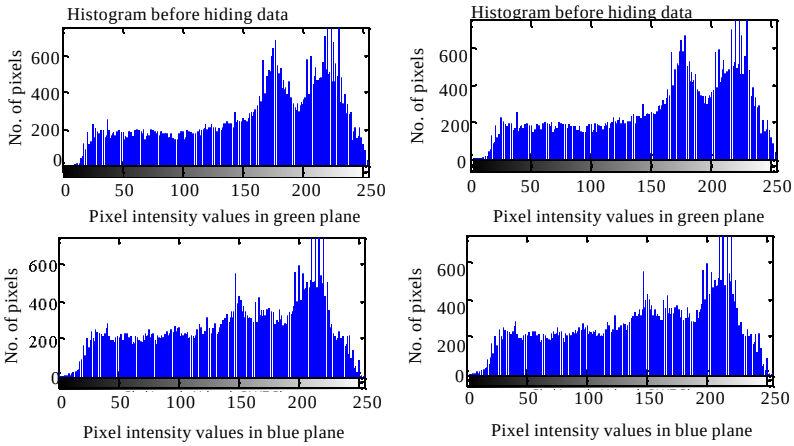

Fig. 5(a-c): Method 1: (a) Cover, (b) Stego images for Mahatma Gandhi and (c) Corresponding Histograms for 5a

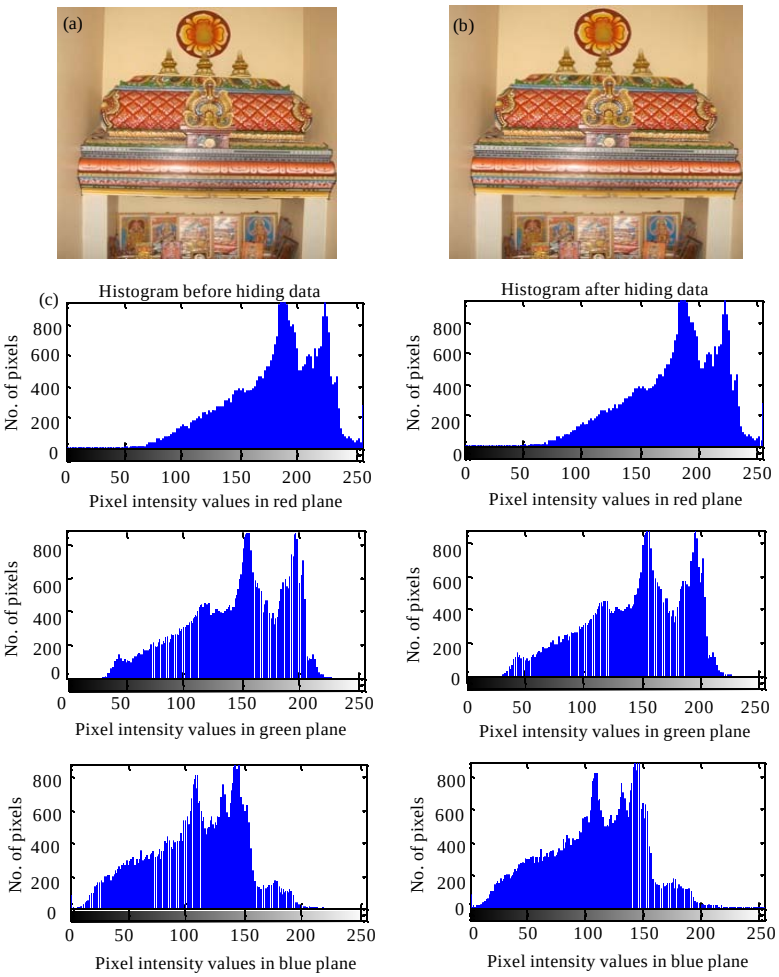

Fig. 6(a-c): Method 1: (a) Cover, (b) Stego images for Kovil and (c) Corresponding histograms for 6a

Table 1: MSE, PSNR values for method 1

	Channel red		Channel green		Channel blue	
Cover image	MSE	PSNR	MSE	PSNR	MSE	PSNR
Lena	0	8	0.0073	69.4862	0.0084	68.8999
Baboon	0	8	0.0081	69.0501	0.0089	68.6538
Mahatma Gandhi	0	8	0.0103	67.9897	0.0078	69.2057
Kovil	0	8	0.0085	68.8579	0.0082	68.9851

Method 2: Cyclic PI approach

Table 2: MSE, PSNR values for Method 2 along with comparison

	Proposed method						Simple LSB (k = 3 bits)					
	Channel red		Channel green		Channel blue		Channel red		Channel green		Channel blue	
Cover image	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
Lena	0.0105	67.9387	0.0079	69.1384	0.0081	69.0720	2.6304	43.9306	2.6659	43.8724	2.6634	43.8764
Baboon	0.0071	69.6086	0.0074	69.4382	0.0104	67.9726	2.6602	43.8817	2.6725	43.8616	2.6737	43.8597
Mahatma	0.0117	67.4590	0.0086	68.7751	0.0067	69.8381	2.6482	43.9013	2.6749	43.8578	2.6606	43.8809
Kovil	0.0087	68.7343	0.0102	68.0241	0.0099	68.1821	2.6749	43.8578	2.6402	43.9144	2.6501	43.8981

	Cyclic pixel indicator method					
	Channel red		Channel green		Channel blue	
Cover image	MSE	PSNR	MSE	PSNR	MSE	PSNR
Lena	1.1293	47.6026	1.1254	47.6178	1.1351	47.5805
Baboon	1.1251	47.6189	1.1331	47.5883	1.1476	47.5329
Mahatma	1.1644	47.4696	1.1508	47.5208	1.1385	47.5675
Kovil	1.1388	47.5663	1.1109	47.6742	1.1313	47.5950

In method 2, cyclic indicator approach is adopted. That is if Red is indicator for pixel 1, then Green and Blue act as data channels. If Green is indicator for next pixel, Red and Blue are assigned data channels and if Blue is indicator for the third one, Red and Green are termed data channels and so on. Here Green channel offers good PSNR characteristics. Here, fracas is homogeneous in all the channels. This indeed increases the capability of entrenching and also maximizes imperceptibility. Of the two methods presented here, method 2 fulfills the anticipation and hence is the best method. Cover images with their corresponding stego images and histograms for the subsequent cover and stego images for method 2 are shown is Fig. 7-10. Analytical results for method 2 are tabled in Table 2.

This study is compared with two other eminent methods of steganography by considering the same payload viz., Simple LSB and cyclic indicator Pixel indicator routine. It is realizable from the table that of the 2 methods, proposed method shows mended upshots in all the channels. PSNR values are outstandingly high thus making it worthy for practical implementation since the stego outputs do not leave behind any vestige for beholders. In spite of having higher complexity than LSB and cyclic indicator method, this paper offers more than anticipated results and thus vouches security. Hence, when glancing through the comparison, the proposed technique is determined to be beneficial.

The algorithm is run against Chi-square and is justified for its creation shown in Fig. 11. The plot is between embedding probability and number of rows participated in the process. It is vivid

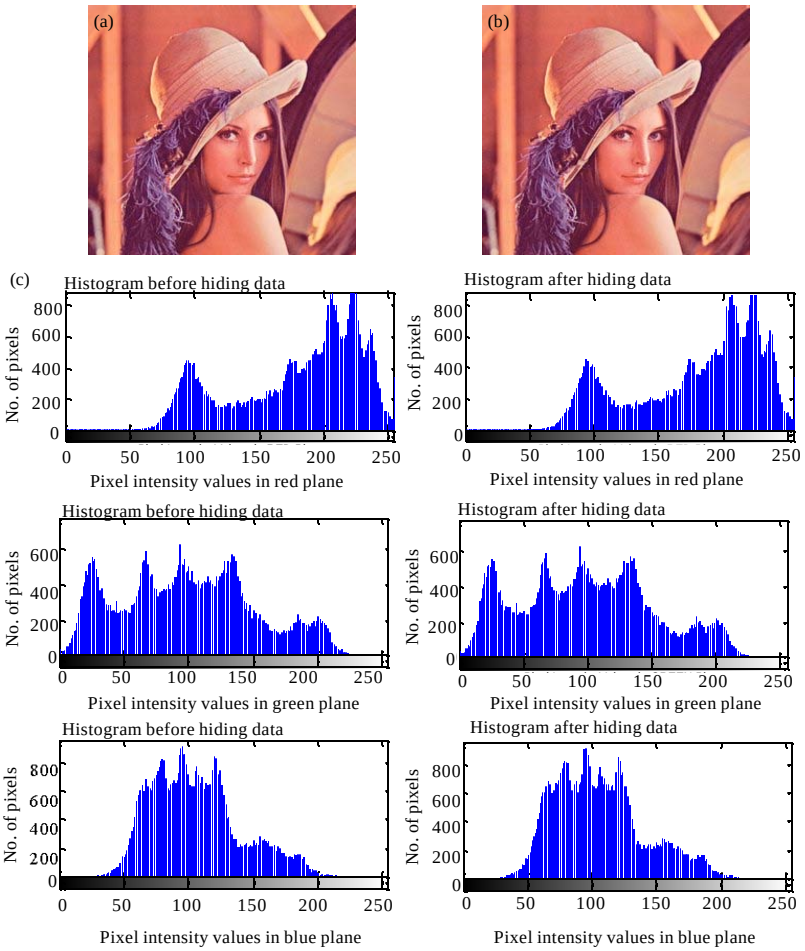

Fig. 7(a-c): Method 2: (a) Cover, (b) Stego images for Lena and (c) Corresponding histograms for 7a

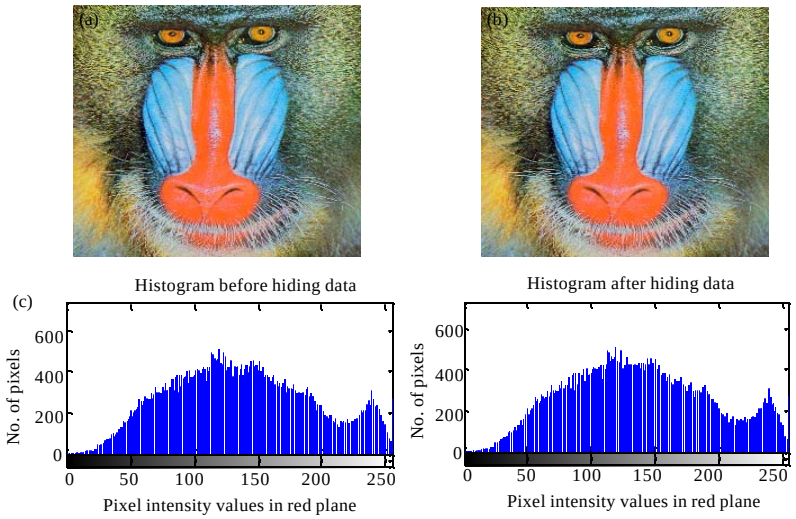

Fig. 8: Continue

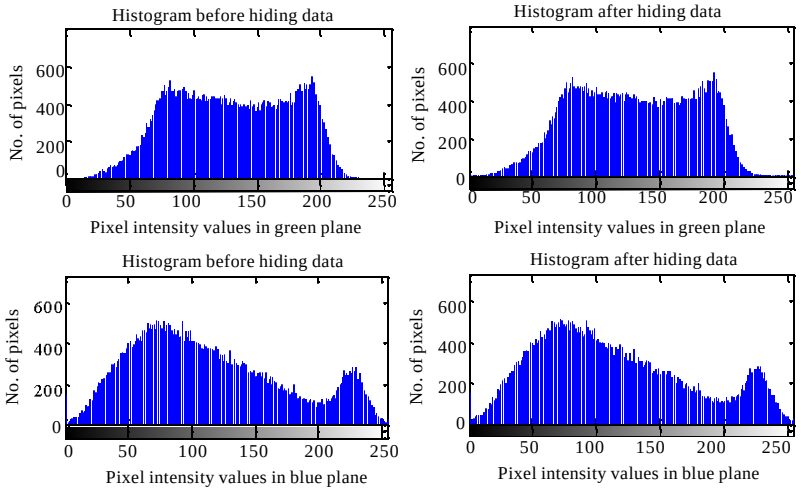

Fig. 8(a-c): Method 2: (a) Cover, (b) Stego images for Baboon and (c) Corresponding histograms for 8a

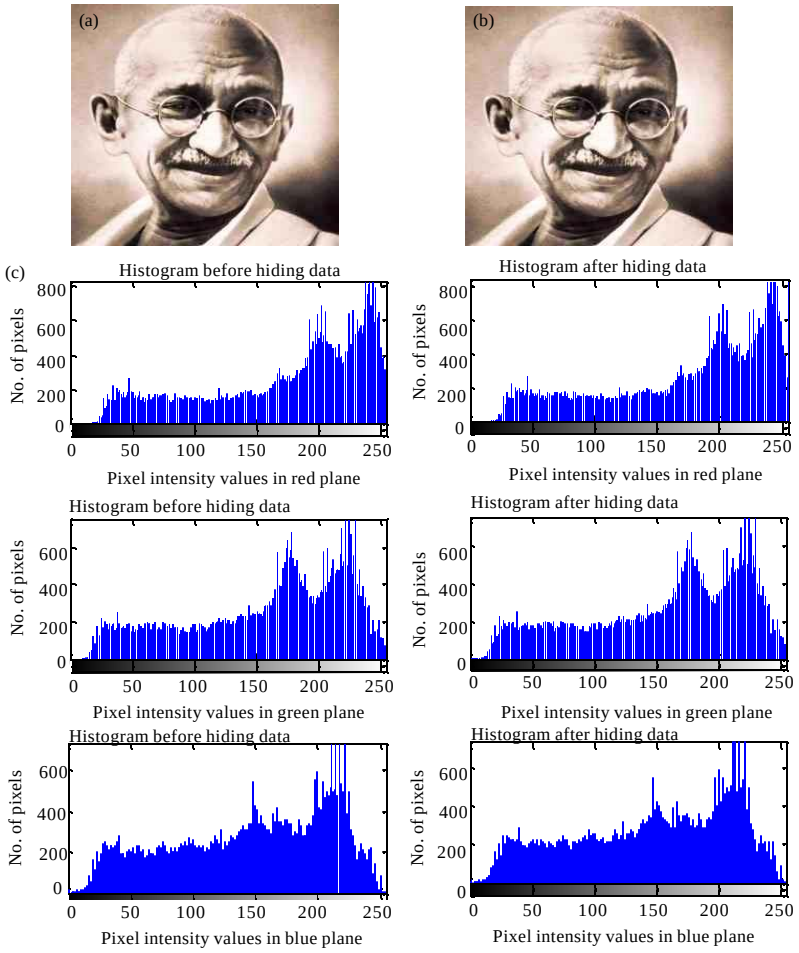

Fig. 9(a-c): Method 2: (a) Cover, (b) Stego images for Mahatma Gandhi and (c) Corresponding histograms for 9a

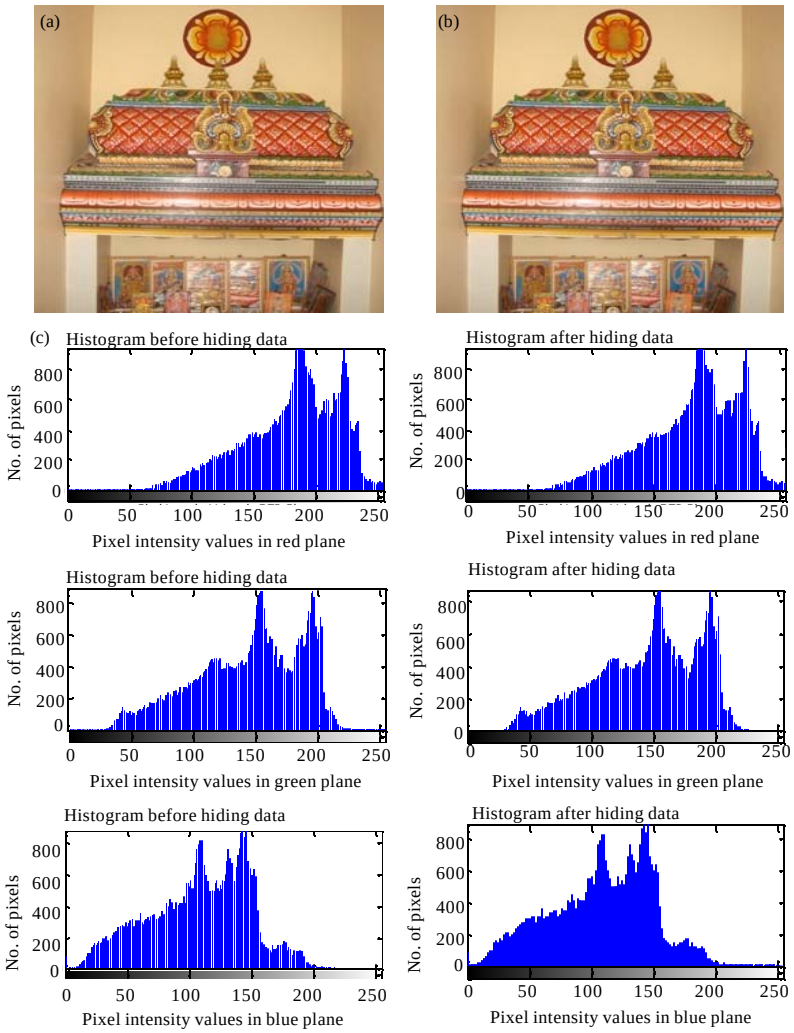

Fig. 10(a-c): Method 2: (a) Cover, (b) Stego images for Kovil and (c) Corresponding histograms for 10a

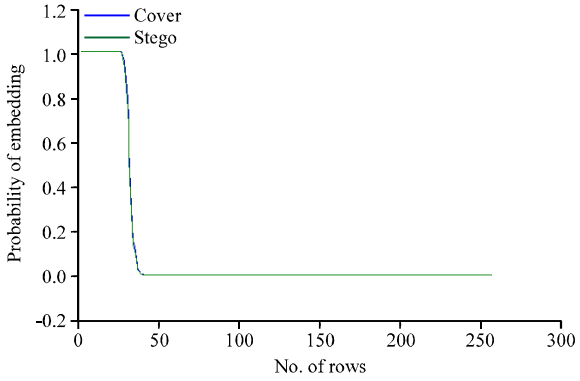

Fig. 11: Chi-square test for Mahatma Gandhi as Stego image for method 2

in the graph that even before fifty rows in the image, the probability becomes zero. What is more to the graph is that both the cover and the stego is concurred and there is nil deviation between the curves. In general, 1 is the probability for entire row embedding and 0 is for no embedding. Thus, this algorithm works really well and disguises the secret data's subsistence. Hence, this study is robust against chi-square.

CONCLUSION

Each and every expertise put into use nowadays needs updating and modernization and should be user friendly. Not only the end product but also the technologies behind the screens are not exemptions. Keeping this fact in mind, this study presents one more updated cum more beneficial technique which can be exercised in image steganography. This study has taken conventional LSB substitution routine to bury the secret message in cover image. But before embedding, substitution means is uniquely modified which has turned the paper into completely distinct algorithm. Here choice of indicator is also left to the user making it more user-friendly. The study is absolved by the illustration of experimental results in addition to histograms and output stego images. Finally, the script is examined by chi-square attack whose results substantiate this wrap up. Hence, to conclude, this study has got everything needed for a perfect steganographic algorithm and sounds good for domestic and saleable application.

REFERENCES

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. 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.

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.

Bender, W., W. Butera, D. Gruhl, R. Hwang, F.J. Paiz and S. Pogreb, 2000. Applications for data hiding. IBM Syst. J., 39: 547-568.

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.

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.

Hong, W., J. Chen and T.S. Chen, 2009. Blockwise reversible data hiding by contrast mapping. Inform. Technol. J., 8: 1287-1291.

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.

Kahn, D., 1996. The Codebreakers: The Story of Secret Writing. Scribner Publisher, New York, USA.

Luo, G., X. Sun and L. Xiang, 2008. Multi-blogs steganographic algorithm based on directed hamiltonian path selection. Inform. Technol. J., 7: 450-457.

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.

Qin, J., X. Sun, X. Xiang and Z. Xia, 2009. Steganalysis based on difference statistics for LSB matching steganography. Inform. Technol. J., 8: 1281-1286.

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.

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., S. Kumar, N. Neelima and R. Amirtharajan, 2011. 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.

Xia, Z., X. Sun, J. Qin and C. Niu, 2009. Feature selection for image steganalysis using hybrid genetic algorithm. Inform. Technol. J., 8: 811-820.

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

Yang, B., X. Sun, L. Xiang, Z. Ruan and R. Wu, 2011. Steganography in Ms Excel document using text-rotation technique. Inform. Technol. J., 10: 889-893.

Zaidan, B.B., A.A. Zaidan and M.L.M. Kiah, 2011. Impact of data privacy and confidentiality on developing telemedicine applications: A review participates opinion and expert concerns. Int. J. Pharmacol., 7: 382-387.

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.

Zhang, X., 2010. Efficient data hiding with plus-minus one or two. IEEE Signal Process. Lett., 17: 635-638.

Zhang, Y., Z.M. Lu and D.N. Zhao, 2010. A blind image watermarking scheme using fast hadamard transform. Inform. Technol. J., 9: 1369-1375.

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.