Journal of Applied Sciences

ISSN 1812-5654

Journal of Applied Sciences 14 (16): 1798-1808, 2014
ISSN 1812-5654 / DOI: 10.3923/jas.2014.1798.1808

Random Image Steganography using Pixel Indicator to Enhance Hiding Capacity

M. Padmaa and Y. Venkataramani
Saranathan College of Engineering, Trichirapalli, Tamil Nadu, India

Abstract: Steganography presents us with a secure means of data transfer which protects confidential information from unauthorized change. Putting it simple, it is a boon to prevent the unauthorized access or misuse of secret information. There are a lot of techniques (both spatial and transform domain) in Steganography. The question of "Which technique is the best" can only be answered hypothetically. Every steganographic technique is unique in its own way and produces desired result, that is, protection of information. The technique proposed in this study sheds light on capacity of embedding and high quality visual while being immune to steg analysis attack. Complexity is driven by means of stego key and LSB substitution.

Key words: Cryptography, data hiding, information security, steganography, pixel indicator

INTRODUCTION

Cryptography can be explained as the transformation of meaningful information into a scrambled code using a key (or keys). The receiver can decode with the help of a key to revive the plaintext. The fundamental notion of cryptography is that between one to one communications (Schneier, 2007; Zaidan *et al*., 2010), impostor should not or cannot extract the covert data. Depending on the complexity required same keys or different keys can be used for both encryption and decryption. The broad classifications of cryptography are private key cryptography and public key cryptography. For a good cryptographic algorithm, emphasis is laid on key length, type of key (duration of key like session key), lifetime of keys, complexity and security of the algorithm, encrypting procedure (double or triple encryption), medium of transmission and so on.

Steganography (Bender *et al*., 1996, 2000) crams the plan of veiling secrets in innocuous media keen on the communication between two parties so that, a third party cannot sense the secret's subsistence (Amirtharajan *et al*., 2011, 2012, 2013a-g; Cheddad *et al*., 2010; Hmood *et al*., 2010a, b; Janakiraman *et al*., 2012a, b; Mohammad *et al*., 2011; Padmaa *et al*., 2011; Praveenkumar *et al*., 2012a, b, 2013a, b; Rajagopalan *et al*., 2012; Stefan and Fabin, 2000; Thenmozhi *et al*., 2012; Zanganeh and Ibrahim, 2011). The universal theory underlying a large amount of steganographic methods is to situate the covert data in the message's noise component. If the information is coded such that it is impossible to differentiate from true noise, a intruder cannot perceive the secret message. To withstand security attacks, any steganographic algorithm should be robust, safe and sound (Chan and Cheng, 2004; Gutub, 2010; Hong *et al*., 2009; Luo *et al*., 2008, 2011; Zanganeh and Ibrahim, 2011; Zhao and Luo, 2012; Zhu *et al*., 2011).

A secures steganographic algorithm should satisfy 4 prerequisites, viz., there should be a unique secret key to every sender; the holder of the truthful key only can detect and access the concealed message; though the attacker recognizes a part of the hidden content, he or she should not be able to detect the remaining; it must be computationally difficult to detect secret messages. While spatial domain schemes (Al-Azawi and Fadhil, 2010; Amirtharajan and Rayappan, 2012a-d, 2013; Thanikaiselvan *et al*., 2011; Thanikaiselvan *et al*., 2012a, b, 2013; Xiang *et al*., 2011; Yang *et al*., 2011; Zaidan *et al*., 2010) exploits LSB, PVD (Padmaa *et al*., 2011), Pixel Indicator methods PIs (Gutub, 2010; Padmaa *et al*., 2011; Amirtharajan *et al*., 2011, 2012, 2013d), transform domain involves DCT, DFT, DHT, DWT. Steganography is useful in ownership verification, electronic labeling, copyright protection, piracy and many more and the counter attack is steganalysis (Qin *et al*., 2009; 2010; Xia *et al*., 2009).

Digital Watermarking refers to the techniques which are used to hide confidential information in digital media (Zeki *et al*., 2011). Robust portrays the capacity of the watermark to survive manipulations of the file, such as lossy compression, cropping, scaling just to spell out some. Fragile means the watermark must not oppose tampering, or would do so only upto a certain extent. At present, watermarking concept is widely employed in e-commerce, tamper detection, advertising, broadcasting, customized media delivery, fraud detection and many

Corresponding Author: M. Padmaa, Saranathan College of Engineering, Trichirapalli, Tamil Nadu, India

more. Needless to mention the threats posed to this scheme. Some of them are collusion attacks, transcoding, linear and nonlinear filtering, signal enhancement. Since online communication in each and every way has seen a phenomenal evolution, watermarking has become the field of interest and numerous procedures are discovered to combat the above mentioned problems.

This study proposed a method to improve the imperceptibility of the random image steganography without compromising the payload. The next section describes the materials and methods with the algorithm and flowchart of the proposed method. The followed section gives the results with comparison then the final conclusion of this study.

MATERIALS AND METHODS

In Steganography, seemingly random changes are introduced to the cover image, based on the secret data. The algorithms construct a robust security for the secret, at the same time without impacting the embedding capacity and imperceptibility (Amirtharajan and Rayappan, 2012a-d).

There exist varieties of algorithms that make use of LSB substitution and Pixel Indicator techniques for hiding data, But the routine used to build this method of steganography distinguishes itself from the others in the manner that, a high quality stego image is created by using more features of the cover images. Unlike conventional LSB substitution, pixel value decides embedding. Pixel indicator concept is employed for the selection of plane for embedding. The embedding process starts from the leftmost pixel and moving downwards (i.e., column wise scanning is adapted to increase the security).

Moreover, a match between the secret bits with that of the original is searched. For k = 4 bit embedding, if a match is found secret data is not embedded and if it is not so, pixel bits experience embedding. The starting bits of the matches are combined to form a bit stream which is nothing but the stego key. The receiver should be let known of this key for the recovery process. Here three such methods are suggested.

Method 1: It takes the default indicator as red channel, green and blue are say, data channels. If the 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

Data embedding, here, obeys the rules of defined LSB substitution in the corresponding planes.

Method 2: This method is slightly different from method 1. Here user is allowed to set the indicator channel and the remaining two act as data channels.

If the value of the indicator is:

00: Data is not embedded
01: Data is embedded in 1st plane
10: Data is embedded in 2nd plane
11: Data is embedded in both planes

Data embedding, here, obeys the rules of defined LSB substitution in the corresponding planes.

Method 3: Cyclic indicator routine is followed here. All planes are named indicator cyclically. That is if red is made the indicator for first pixel (green and blue act as data channels), green is made the indicator for the second pixel (red and blue act as data channels), blue for the third (green and red act as data channels), again red for fourth and so on and is shown in Fig. 1.

EMBEDDING ALGORITHM

The proposed method Flow chart for embedding is shown in Fig. 2.

Method 1:

- Read the cover image (C) and secret data (D)
- Divide the cover image into red, green and blue planes
- Form the encrypted secret data (M) with the use of key by using encryption algorithm
- Then use the pixel indicator method to embed the data in planes, by keeping one plane as indicator
- In this method1, red plane is taken as a default indicator and consider the green plane as data channel1 and blue plane as data channel 2
- Check the last two LSB pixel bits of the indicator plane
  If it is 00, no embedding
  01 means, embed in data channel 1
  10 means embed in data channel 2
  11 means embed in both the channels
- Then the secret message bits are checked with the last 4 LSB (1234) of pixel bits
  If it matches with that of the pixel, then form the stego key as 00
  Else
  Compare it with 2345 LSB of pixel bits, match is found, then form the stego key as 01
  Else
  Compare it with 3456 LSB of pixel bits, match is found, then form stego key here as10
  Else
  Compare it with 4567 LSB of pixel bits, match is found, then form the stego key as 11
  Else embed the data in last 4 LSB (1234) and form the stego key as 00
- If all the secret data is embedded, then store the resulting image as stego image
- The stego key is communicated to the receiver for extraction

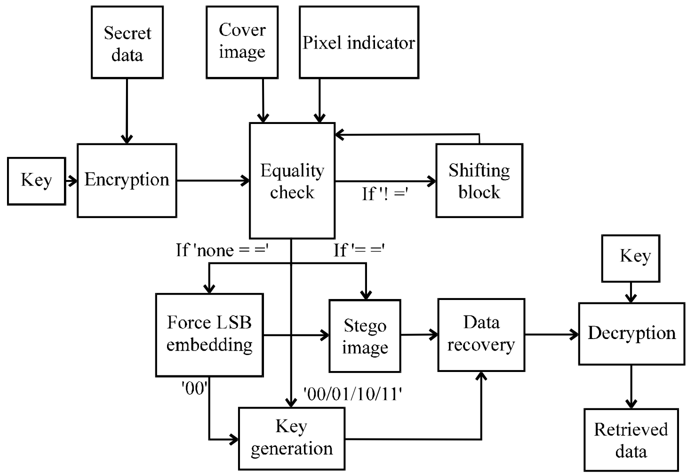

Fig. 1: Block diagram for proposed method

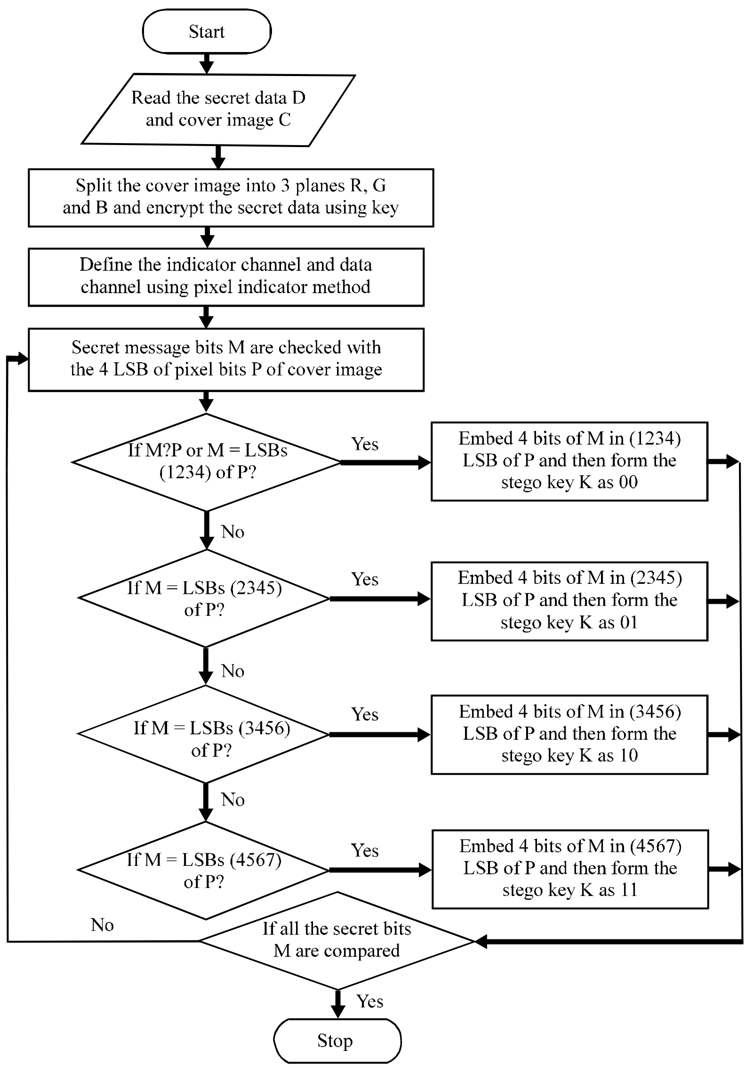

Fig. 2: Flow chart for embedding

Method 2:

- In this, user defined indicator is chosen and the other two channels are data channels
- Then encrypt the message bits, as per pixel indicator method select the embedding plane
- Form the encrypted secret data (M) with the use of key by using encryption algorithm
- Check the last two LSB pixel bits of the indicator plane
  If it is 00, no embedding.
  01 means, embed in data channel 1
  10 means, embed in data channel 2
  11 means, embed in both the channels
  Then the secret message bits are checked with the last 4 LSB (1234) of pixel bits
  If it matches with that of the pixel, then form the stego key as 00
  Else
  Compare it with 2345 LSB of pixel bits, match is found, then form the stego key as 01
  Else
  Compare it with 3456 LSB of pixel bits, match is found, then form stego key here as10
  Else
  Compare it with 4567 LSB of pixel bits, match is found, then form the stego key as 11
  Else embed the data in last 4 LSB (1234) and form the stego key as 00
- If all the secret data is embedded, then store the resulting image as stego image
- The stego key is communicated to the receiver for extraction

Method 3:

- In this method, cyclically indicator is chosen, say in pixel 1 red is default indicator, in pixel 2 green is default indicator and in pixel 3 blue is default indicator. The other two channels will be embedding channels
- Check the last two LSB pixel bits of the indicator plane
  If it is 00, no embedding
  01 means, embed in data channel 1
  10 means, embed in data channel 2
  11 means, embed in both the channels
- Then encrypt the message bits, as per pixel indicator method select the embedding plane
  Then the secret message bits are checked with the last 4 LSB (1234) of pixel bits
  If it matches with that of the pixel, then form the stego key as 00
  Else
  Compare it with 2345 LSB of pixel bits, match is found, then form the stego key as 01
  Else
  Compare it with 3456 LSB of pixel bits, match is found, then form stego key here as10
  Else
  Compare it with 4567 LSB of pixel bits, match is found, then form the stego key as 11
- Else embed the data in last 4 LSB (1234) and form the stego key as 00
- If all the secret data is embedded, then store the resulting image as stego image
- The stego key is communicated to the receiver for extraction

EXTRACTION ALGORITHM

The proposed method Flow chart for extraction is shown in Fig. 3.

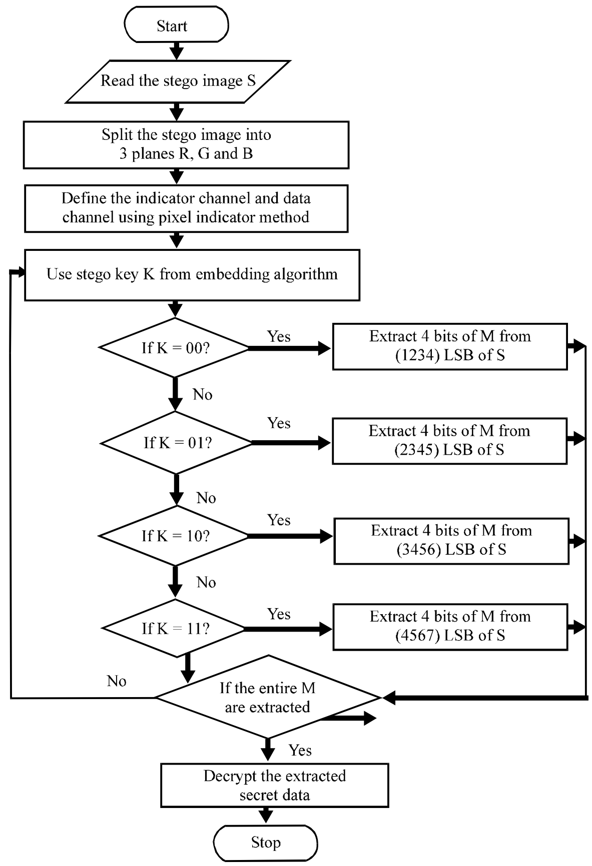

Fig. 3: Flow chart for extraction

- Split the stego image into red, green and blue planes (R, G and B planes)
- Select the indicator channel and data channel with respect to 3 methods given earlier
- Get the stego key(K) from embedding
  if K = 00, extract the data from 1234 LSB of stego image
  if K = 01, extract the data from 2345 LSB of stego image
  if K = 10, extract the data from 3456 LSB of stego image
  if K = 11, extract the data from 4567 LSB of stego image
- Once all the secret bits (M) are extracted, decrypt it to get the secret message bits(D)

RESULTS AND DISCUSSION

Four color cover images of dimension 256×256 each are taken to verify the performance of the algorithm. These images go through the testing of full embedding capability for all three methods. To have a vision about the efficacy, corresponding stego images are generated and studied (Fig. 4-7). MSE and PSNR values are calculated, Table 1-3 and compared. The mathematical equations for doing so are:

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

Fig. 4(a-d): Stego and cover images (a) Lena, (b) Baboon, (c) Mahatma Gandhi and (d) Temple

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	2.9083	43.4944	3.0876	43.2346	0	2.004	2.0187	263628
Baboon	0	8	2.8871	43.5262	2.9472	43.4368	0	2.0445	2.0077	262940
Mahatma Gandhi	0	8	3.0109	43.3439	2.9144	43.4853	0	2.0452	2.0269	266868
Temple	0	8	2.9112	43.49	2.8909	43.5205	0	2.0056	1.9801	261208

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 bit embedded
Lena	3.0957	43.2232	0	8	3.0271	43.3205	2.0093	0	1.9996	262728
Baboon	2.9722	43.4021	0	8	2.9339	43.4563	1.9987	0	1.9932	261612
Mahatma Gandhi	3.2810	42.9707	0	8	2.9071	43.4963	1.9705	0	2.0068	260656
Temple	3.0086	43.3471	0	8	2.8999	43.5070	2.0156	0	1.9938	262756

Table 3: Comparison with existing methods for MSE, PSNR and BPP values for method 3

		Channel I red		Channel II green		Channel III blue			
Cover image	PI methods	MSE	PSNR	MSE	PSNR	MSE	PSNR	Bits Per Pixel (BPP)	Total No. of bits Embedded
Lena	Proposed	2.0605	44.99	1.9069	45.32	1.0249	45.06	3.9945	261780
	Amirtharajan *et al.* (2013d)	0.4987	51.15	0.2594	53.99	0.7033	49.65	1.9958	130798
	Padmaa *et al.* (2011)	1.2270	47.24	1.3641	46.78	1.02	48.05	2.114	138549
	Amirtharajan *et al.* (2011)	1.2906	47.02	1.2374	47.21	1.2049	47.32	2.3139	151645
	Amirtharajan *et al.* (2012)	2.4387	44.26	2.3066	44.50	2.3389	44.44	3.9181	256776
Baboon	Proposed	1.9947	45.13	1.9392	45.25	1.9461	45.23	3.9951	261824
	Amirtharajan *et al.* (2013d)	0.4754	51.35	0.2587	54.00	4.6733	41.43	1.9858	130144
	Padmaa *et al.* (2011)	4.0650	42.04	4.002	42.11	4.2847	41.81	3.657	239262
	Amirtharajan *et al.* (2011)	1.5540	46.21	1.5544	46.22	1.5904	46.12	2.3975	157121
	Amirtharajan *et al.* (2012)	2.3702	44.39	2.3255	44.47	2.3619	44.39	3.9232	257108
Mahatma Gandhi	Proposed	2.2164	44.67	2.0049	45.11	1.9477	45.24	4.0168	263244
	Amirtharajan *et al.* (2013d)	0.4876	51.25	0.2558	54.05	3.8500	42.28	1.9822	131212
	Padmaa *et al.* (2011)	1.3480	46.83	2.4212	47.03	1.2478	47.17	2.07	132945
	Amirtharajan *et al.* (2011)	3.2721	42.98	3.2944	42.95	3.1355	43.17	2.07	202377
	Amirtharajan *et al.* (2012)	2.5728	44.03	0.5798	44.29	2.3595	44.41	3.9184	256796
Temple	Proposed	1.9968	45.1275	1.9199	45.298	1.9578	45.21	3.9978	262000
	Amirtharajan *et al.* (2013d)	0.4673	51.43	0.2569	54.03	0.8289	48.95	1.9921	130556
	Padmaa *et al.* (2011)	1.853	45.45	1.766	45.66	1.632	46.01	2.352	154409
	Amirtharajan *et al.* (2011)	1.1159	47.65	1.1062	47.69	1.1240	47.62	2.4659	161604
	Amirtharajan *et al.* (2012)	2.3143	44.49	2.3095	44.49	2.3764	44.37	3.9240	257160

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

If PSNR is high, stego image is highly imperceptible that is it suffers from negligible distortion. For four bit embedding, the probability that a 4-bit match is found in the bit stream will be 1/16. For example, if search is for 1011, it may be in the range from 0000 up to 1111. The chance for finding a match increases with the increase in bits used for searching

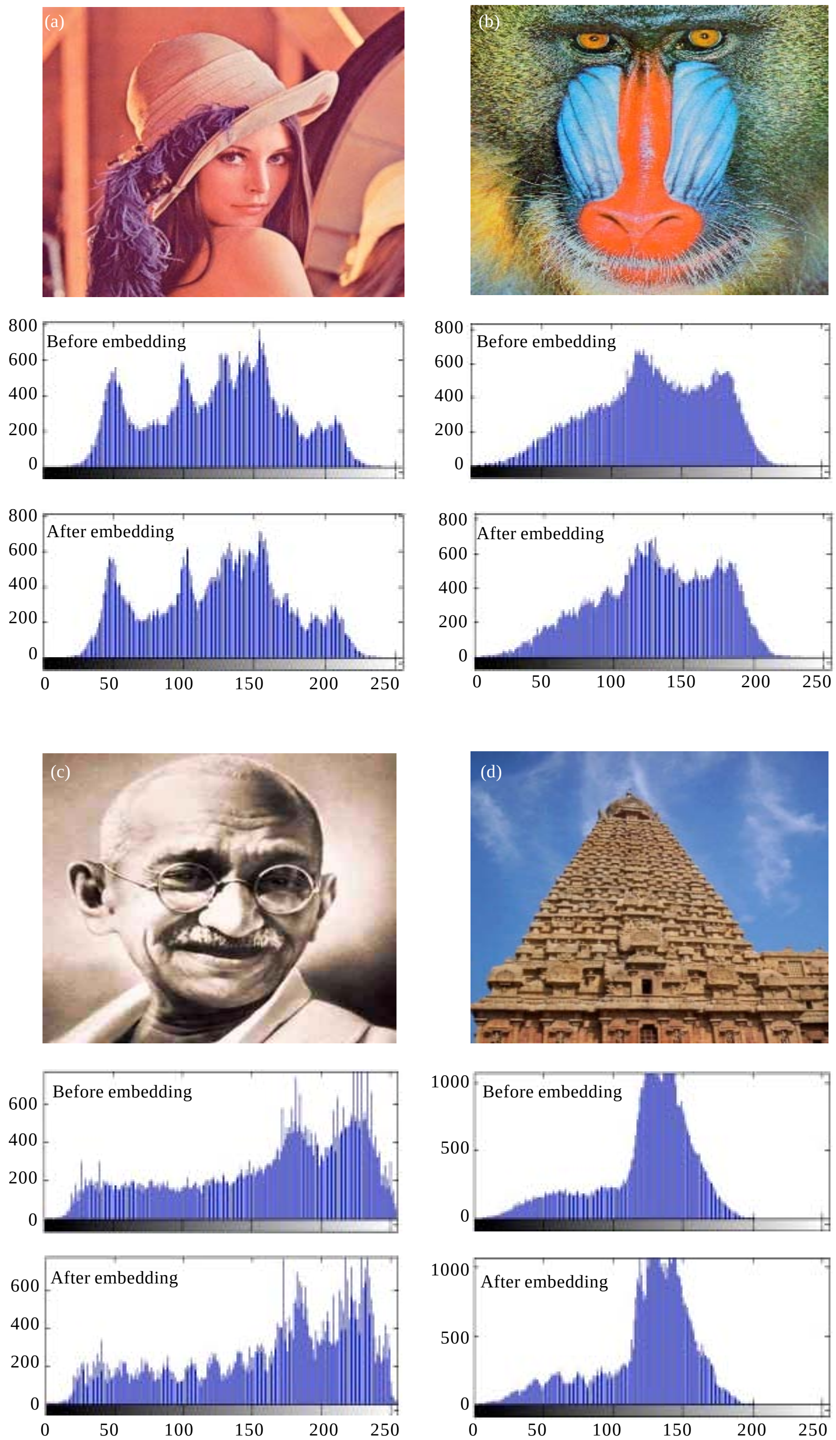

Fig. 5(a-d): Resultant stego images and their corresponding Histograms for Method 1. Cover images (a) Lena, (b) Baboon, (c) Mahatma Gandhi and (d) Temple

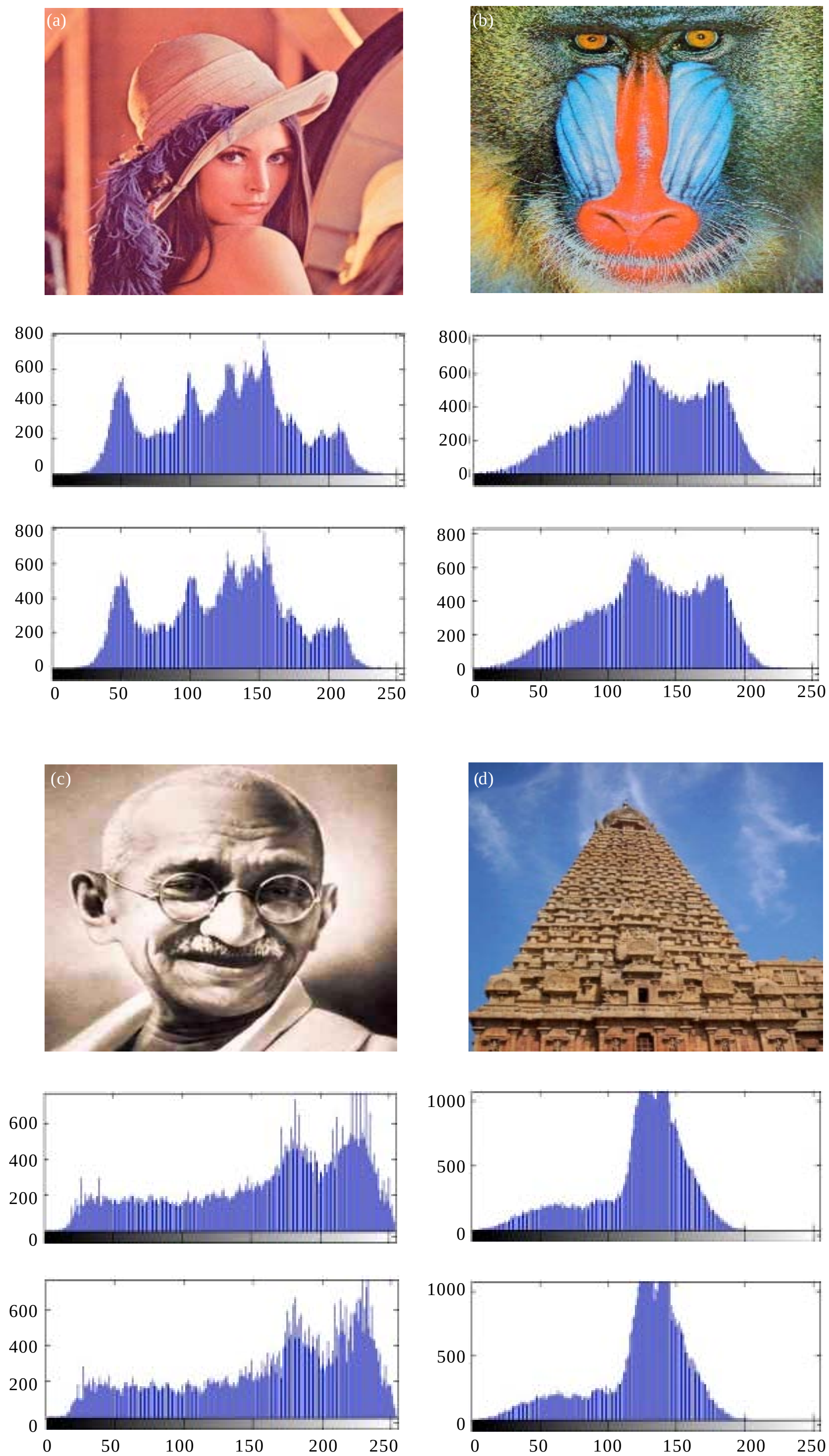

Fig. 6(a-d): Resultant stego images and their corresponding Histograms for Method 2. Cover images (a) Lena (b) Baboon (c) Mahatma Gandhi and (d) Temple

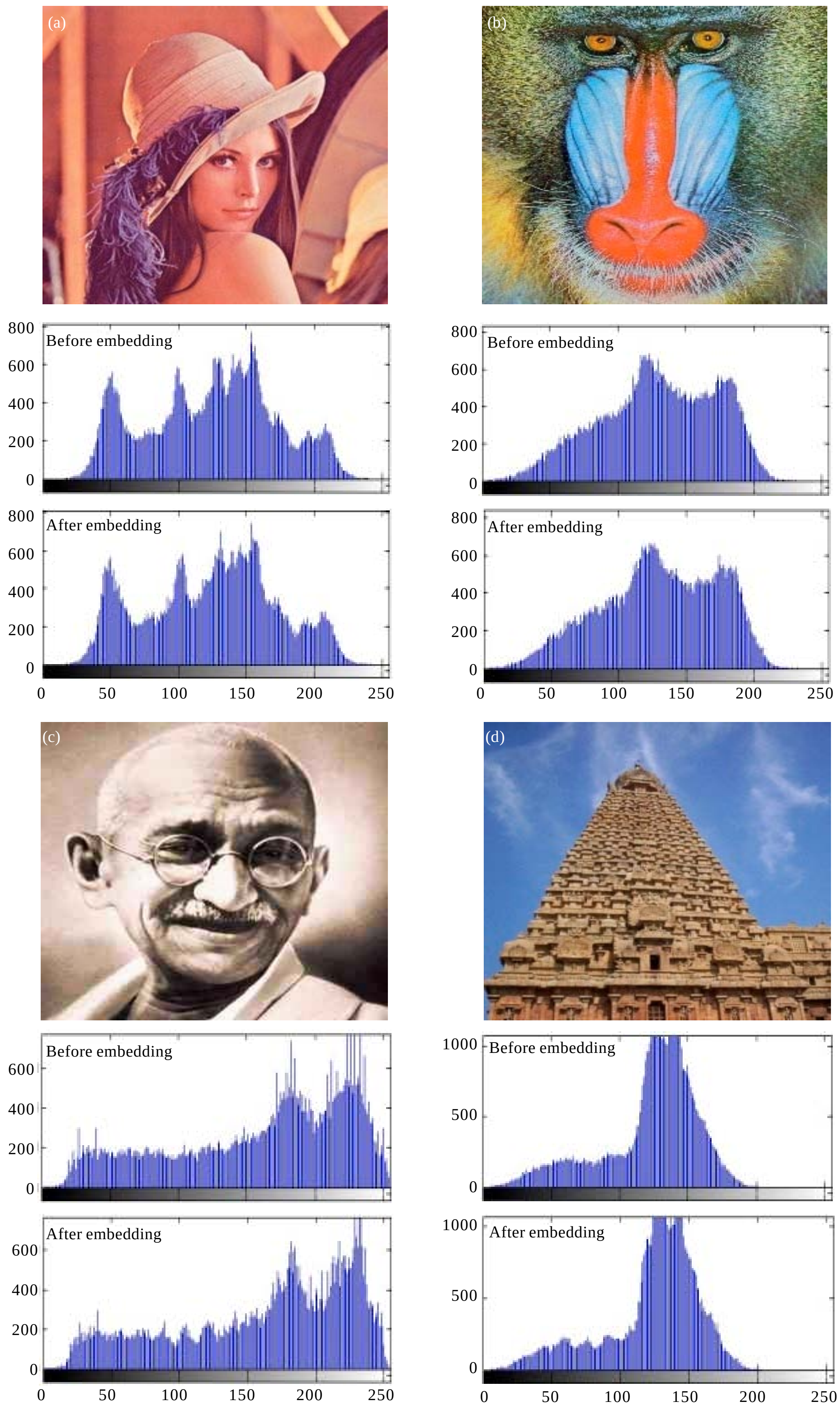

Fig. 7(a-d): Resultant stego images and their corresponding Histograms for Method 3. Cover images (a) Lena, (b) Baboon, (c) Mahatma Gandhi and (d) Temple in pixels in the cover. If there does not exist a match, then the secret 4 bits are set in first four LSBs.

From the stego images we can infer that it is completely free of distortion and escapes human suspicion. Higher PSNR values of stego images guarantees that they are of fairly high quality.

CONCLUSION

An inimitable approach is presented in this script to settle the significant problem of capacity of payload and imperceptibility in a steganographic scheme. This study makes use of Pixel Indicator and modified Least Significant Bit Substitution methods to construct the algorithm and also OPAP to reduce the distortion. Also the key used for encryption and stego key are not identifiable as the latter is based on the position of the bits of the original cover. The algorithm's strength is it could withstand steganalysis attack with the help of four color images. This method involves some computational forehead which indeed resists itself to security threats. The images do not suffer from artifacts as only the LSBs of the pixels undergo alteration. Thus, this study provides security both at the steganographic and cryptographic level. Tentative results also affirm the conclusion. Thus, it is an effective way of secret data communication.

ACKNOWLEDGMENT

The first author wishes to thank Dr. R. Amirtharajan Associate Professor/ECE School of Electrical and Electronics Engineering, for his valuable guidance to improve technical and linguistic quality of this study.

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.

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, 2012. Random image steganography and steganalysis: Present status and future directions. Inform. Technol. J., 11: 566-576.

Amirtharajan, R. and J.B.B. Rayappan, 2013. Steganography-time to time: A review. Res. J. Inform. Technol., 5: 53-66.

Amirtharajan, R., G. Devipriya, V. Thanikaiselvan and J.B.B. Rayappan, 2013a. High capacity triple plane embedding: A colour stego. Res. J. Inform. Technol., 5: 373-382.

Amirtharajan, R., K. Karthikeyan, M. Malleswaran and J.B.B. Rayappan, 2013b. Kubera kolam: A way for random image steganography. Res. J. Inform. Technol., 5: 304-316.

Amirtharajan, R., K.M. Ashfaaq, A.K. Infant and J.B.B. Rayappan, 2013c. High performance pixel indicator for colour image steganography. Res. J. Inform. Technol., 5: 277-290.

Amirtharajan, R., M.V. Abhiram, G. Revathi, J.B. Reddy, V. Thanikaiselvan and J.B.B. Rayappan, 2013d. Rubik's cube: A way for random image steganography. Res. J. Inform. Technol., 5: 329-340.

Amirtharajan, R., P. Archana and J.B.B. Rayappan, 2013e. Why image encryption for better steganography. Res. J. Inform. Technol., 5: 341-351.

Amirtharajan, R., R. Subrahmanyam, J.N. Teja, K.M. Reddy and J.B.B. Rayappan, 2013f. Pixel indicated triple layer: A way for random image steganography. Res. J. Inform. Technol., 5: 87-99.

Amirtharajan, R., V. Rajesh, P. Archana and J.B.B. Rayappan, 2013g. Pixel indicates, standard deviates: A way for random image steganography. Res. J. Inform. Technol., 5: 383-392.

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

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. Pattern Recognit., 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. Emerg. 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.

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.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012a. Phase for face saving-a multicarrier stego. Proc. Eng., 30: 790-797.

Praveenkumar, P., R. Amirtharajan, Y. Ravishankar, K. Thenmozhi, J. Bosco and B. Rayappan, 2012b. Random and AWGN road for MC-CDMA and CDMA bus to phase hide: A MUX in MUX stego. Proceedings of the International Conference on Computer Communication and Informatics, January 10-12, 2012, Coimbatore, India, pp: 1-6.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2013a. Can we reduce PAPR? OFDM+PTS+SLM+STEGO: A novel approach. Asian J. Sci. Res., 6: 38-52.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2013b. OFDM with low PAPR: A novel role of partial transmit sequence. Res. J. Inform. Technol., 5: 35-44.

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., John Wiley and Sons, New Delhi, 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.

Thanikaiselvan, V., P. Arulmozhivarman, J.B.B. Rayappan and R. Amirtharajan, 2012a. Graceful graph for graceful security-towards a STE (G) Raph. Res. J. Inform. Technol., 4: 220-227.

Thanikaiselvan, V., P. Arulmozhivarman, R. Amirtharajan and J.B.B. Rayappan, 2012b. Horse riding and hiding in image for data guarding. Proc. Eng., 30: 36-44.

Thanikaiselvan, V., K. Santosh, D. Manikanta and R. Amirtharajan, 2013. A new steganography algorithm against chi square attack. Res. J. Inform. Technol., 5: 363-372.

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, 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.