Research Journal of Information Technology

ISSN 1815-7432

Academic
Journals Inc.

www.academicjournals.com

Research Journal of Information Technology 5 (3): 373-382, 2013
ISSN 1815-7432 / DOI: 10.3923/rjit.2013.373.382

High Capacity Triple Plane Embedding: A Colour Stego

[1]Rengarajan Amirtharajan, [1]G. Devipriya, [2]V. Thanikaiselvan and [1]J.B.B. Rayappan
[1]School of Electrical and Electronics Engineering, SASTRA University, 613401, India
[2]School of Electronics Engineering, VIT University, Vellore-632014, Tamil Nadu, India

Corresponding Author: Rengarajan Amirtharajan, School of Electrical and Electronics Engineering, SASTRA University, 613401, India

ABSTRACT

In this study, we highlighted a new and efficient steganographic modus operandi based on pixel indicator routine to infix covert data in an RGB image. Usually when pixel indicator technique is employed on an RGB image, only one among the three planes (R, G and B) is labeled the indicant plane and the other two as depository planes in which the data can be stored. The proposed method is a similar concept by considering all the three planes for storage of the data instead of just two. This is carried out by using 5, 6 and 7 bits of a plane as indicator bits which increases the possible fields (from 4-8) to store the data. Because of this, the data embedding capacity of the image is improved to a greater extent since the indicator plane can also be used for embedding data in it. Optical Pixel Adjustment Process (OPAP) is also used here for reducing Mean Square Error. Furthermore the OPAP technique is not applied on the indicator plane as it modifies the indicator bits for reducing the MSE.

Key word: Data security, image steganography, pixel indicator, OPAP

INTRODUCTION

Nobody really owns the internet. It is a global collection of networks for which everyone has access to. These days internet has reached even remote villages. But the million dollar question that arises is 'How safe is this internet nowadays?' To make internet more secure and safe, along with the growth of information technology and communication, there has been a tremendous growth in technologies to secure this information too. Information hiding is the best possible way to secure confidential information (Cheddad *et al*., 2010; Stefan and Fabin, 2000; Qin *et al*., 2010).

Many different methods are invented to encrypt and decrypt data to keep our data secret. Few among them are Cryptography (Salem *et al*., 2011; Schneier, 2007), Steganography (Amirtharajan and Rayappan, 2012a-d; Amirtharajan *et al*., 2012; Bender *et al*., 1996; Cheddad *et al*., 2010; Janakiraman *et al*., 2012a, b; Rajagopalan *et al*., 2012; Thanikaiselvan *et al*., 2011; Thenmozhi *et al*., 2012), finger printing and water marking (Zeki *et al*., 2011). Cryptography is the art of scrambling of data in an unintended format so that no one other than the authorised receiver can decode it. It would look gibberish to any third person viewing it. But it has a disadvantage in that a person looking at it would find out that it is some encoded secret message (Zaidan *et al*., 2010). And if he gets hold of the secret code then any third person can extract it. Water marking is just for copy right protection and protection of intellectual property (Abdulfetah *et al*., 2010). The kind of data hidden in objects in the case of watermarking is a signature. This signature helps to signify the authority or ownership of the legal user. This study highlights about steganography and the algorithms used.

Steganography is derived from the Greek word 'stegos' meaning secret or something that is covered. '-graphy' means art or drawing or writing, hence both put together means 'a covered drawing' (Al-Azawi and Fadhil, 2010; Luo *et al.*, 2011; Mohammad *et al.*, 2011; Zanganeh and Ibrahim, 2011; Zhao and Luo, 2012). Steganography is not new science. It has existed from the ancient times. In the olden days the secret messenger had his message encrypted in the form of tattoo and this was tattooed on his shaven head, thus, hiding the information from the third person. Only when the person's head was shaven the image and the encrypted message could be decoded.

Ultimate aim of steganography is in the secure communication of the hidden data in a totally untraceable manner and to avoid any attention or suspicion to the transmission of the secret data. Apart from keeping others from knowing the hidden data, it should also prevent third persons from knowing that the secret data even exists. A simple classification is methods in spatial domain (Gutub, 2010; Padmaa *et al.*, 2011) or transform domain (Amirtharajan and Rayappan, 2012d), but the cover object may be text (Xiang *et al.*, 2011), video (Al-Frajat *et al.*, 2010), audio (Zhu *et al.*, 2011) or an image (Amirtharajan and Rayappan, 2012a-d; Cheddad *et al.*, 2010). Aforementioned methods gives proper insight to steganography, in this study, a method is coined to improve the payload, imperceptibility with additional complexity in color image.

PROPOSED METHOD

The familiar method pixel indicator is proposed here by implementing new idea in that, by this way it improves embedding capacity as well as imperceptibility. It reduces the visual distortion by giving good image quality. In this method, number of bits embedded is defined by the user, say k-bit embedding. Indicator plane pixel bits tells that which plane is going to be a data plane. Two methods are introduced here; Red is taken as default indicator in method1. Method 2 uses the indicator plane cyclically. The block diagram of this study is shown in Fig. 1.

The flowcharts for embedding and extraction of the secret message are given in Fig. 2 and 3.

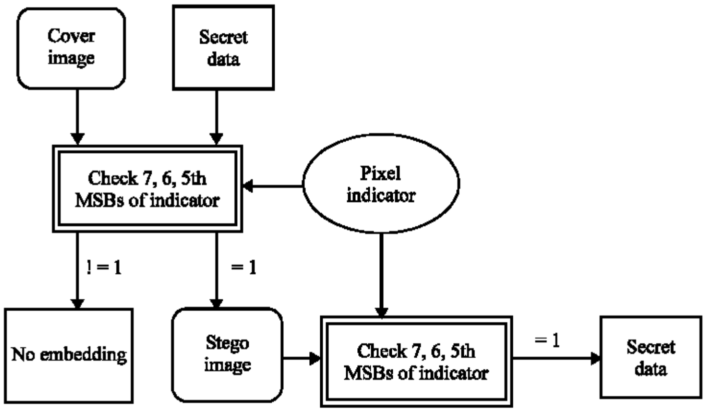

Fig. 1: Block diagram for the proposed method

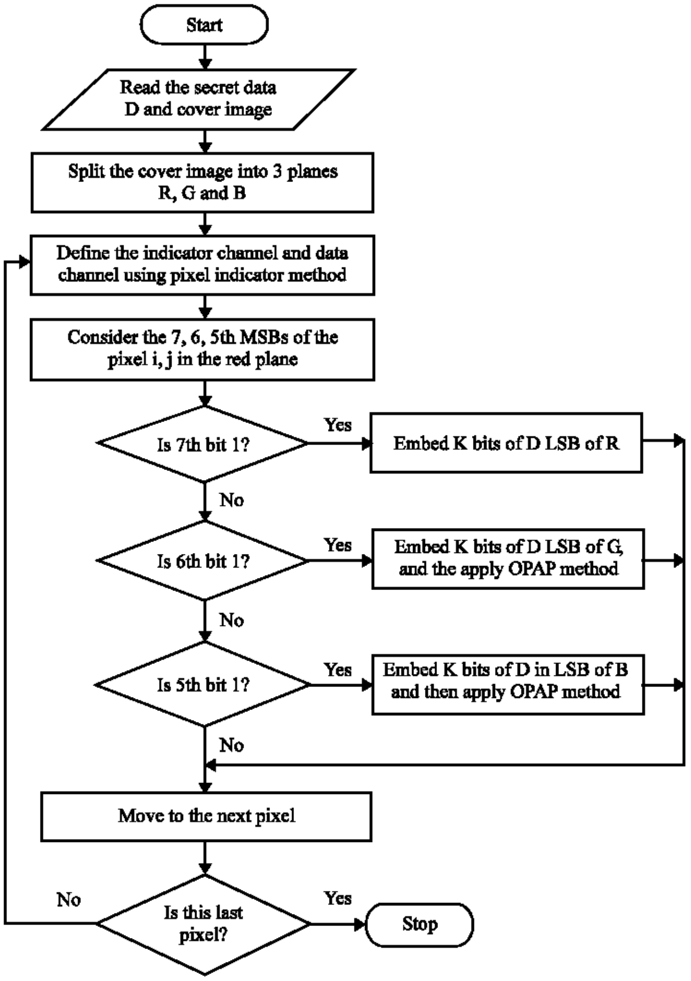
Start
Read the secret data D and cover image
Split the cover image into 3 planes R, G and B
Define the indicator channel and data channel using pixel indicator method
Consider the 7, 6, 5th MSBs of the pixel i, j in the red plane
Is 7th bit 1?
Yes
Embed K bits of D LSB of R
No
Is 6th bit 1?
Yes
Embed K bits of D LSB of G, and the apply OPAP method
No
Is 5th bit 1?
Yes
Embed K bits of D in LSB of B and then apply OPAP method
No
Move to the next pixel
No
Is this last pixel?
Yes
Stop

Fig. 2: Flow chart for embedding the secret data

Embedding algorithm

```
Method 1:
•   Read the cover image and secret data.
•   Split the cover image into Red(R), Green (G) and Blue planes (B).
•   Consider RED as default indicator, for each pixel in Red, do the following
    Let b[7] = Second MSB of current pixel in R
    b[6] = Third MSB of current pixel in R
    b[5] = Fourth MSB of current pixel in R
    If b[7] = 1
    Go for k-bit embedding in Red
    Else if b[6] = 1
    Go for k-bit embedding in Green and apply OPAP then and there
    Else if b[5] = 1
    Go for k-bit embedding in Blue and apply OPAP then and there
    Else no embedding
•   If all secret data are embedded, store it as stego image
    Else go to step3
```

Embedding algorithm: Continue

```
Method 2:
•   Read the cover image and secret data
•   Split the cover image into Red(R), Green (G) and Blue planes (B)
•   Here Cyclic indicator is preferred, that is for first pixel Red as Indicator, second pixel green as indicator and for third pixel Blue as
    Indicator
•   For each pixel in indicator plane, do the following
    Let b[7] = Second MSB of current pixel in indicator
    b[6] = Third MSB of current pixel in indicator
    b[5] = Fourth MSB of current pixel in indicator
    If b[7] = 1
    Go for k-bit embedding in Red
    Else if b[6] = 1
    Go for k-bit embedding in Green and apply OPAP then and there
    Else if b[5] = 1
    Go for k-bit embedding in Blue and apply OPAP then and there
    Else no embedding
•   If all secret data are embedded, store it as stego image
    Else go to step 4
```

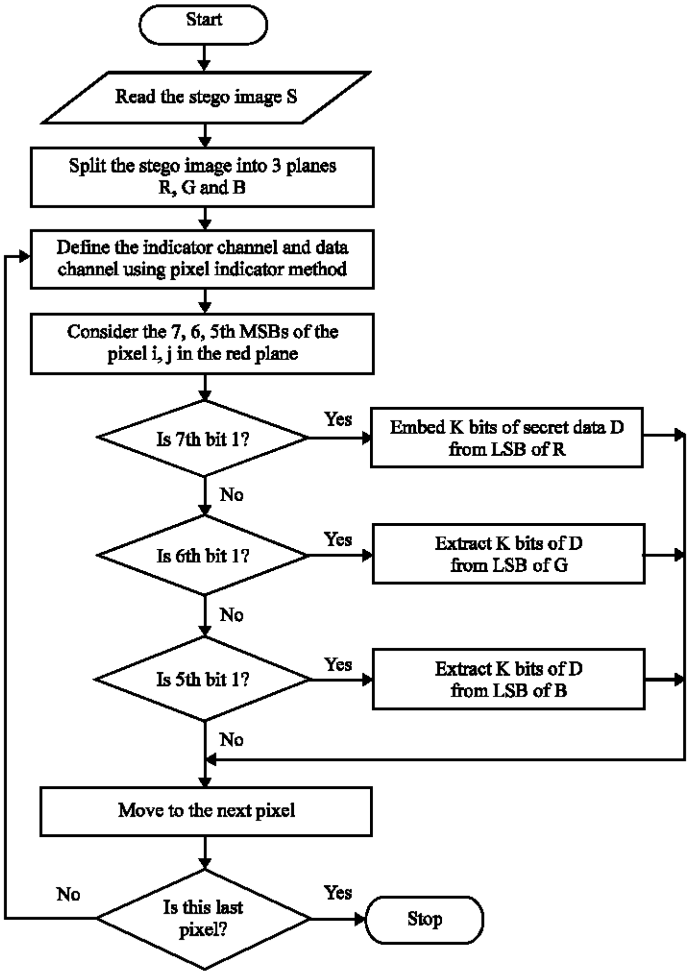
Start
Read the stego image S
Split the stego image into 3 planes R, G and B
Define the indicator channel and data channel using pixel indicator method
Consider the 7, 6, 5th MSBs of the pixel i, j in the red plane
Is 7th bit 1?
Yes
Embed K bits of secret data D from LSB of R
No
Is 6th bit 1?
Yes
Extract K bits of D from LSB of G
No
Is 5th bit 1?
Yes
Extract K bits of D from LSB of B
No
Move to the next pixel
No
Is this last pixel?
Yes
Stop

Fig. 3: Flow chart for extracting the secret data

Extraction algorithm

```
•   Split the stego image into three planes
•   Check 567 MSB's in indicator plane
    If b[7] = 1,
    Extract k-bit data from Red
    Else if b[6] = 1
    Extract k-bit data from Green
    Else if b[5] = 1
    Extract k-bit data from Blue
•   Once all the bits are extracted, combine it to get the secret data
```

RESULTS AND DISCUSSION

Four images are taken as covers namely Lena, Baboon, Mahatma Gandhi and Temple of size 256×256×3. The algorithm is executed in MATLAB 7.1 with k = 1, 2, 3, 4 bit for each image and the results are given in Fig. 4-9. MSE and PSNR values for each iteration along with bits embedded in each pixel and total embedding capacity for method 1 and 2 is given in Table 1 and 2, respectively. The tentative results for method 1 say that it has produced substantially high PSNR values for all the images which is well above the minimum standard of 38 dB. It also conveys that the resultant stego images are of fairly high quality and cannot attract naked eyes' attention. Of these covers, Lena holds the record of having high PSNR value of 59.0357 for k = 1 bit embedding. BPP is also passably decent. For each k bit embedding sensible amount of bits are entrenched showing that the algorithm works well with good capacity with increased complexity and security as well.

Method 2 results are given in Fig. 7-9, respectively which makes use of cyclic indicator method wherein each plane is termed indicator for subsequent iteration. Thus each plane gets a chance of being the indicator channel. Though one can witness high MSE value in all images, it produces sensibly genuine embedding capacity. Moreover, since OPAP is called the level of distortion is made under control. Stego images as well as the histograms prove this with which it can be concluded that the paper is detected to be good when equated against the subsisting ones. Unlike method 1, method 2 gives equalized grandness to every panorama of steganography.

Both the methods are probed against Chi-square run. The graphical record of Mahatma Gandhi image is shown Fig. 10. The original cover and all the four stego outputs (for k = 1, 2, 3, 4) are represented. It is evident from the graph that with the increase in number of rows the probability decreases and 2, 3, 4 bit embedding curves show almost the same results as that of the original. For 1 bit embedding the probability reduces to zero only after 100 rows in the image. Partially contrary to method 1, method 2 exhibits splendid end results. All the resultants go hand-in-hand with the cover, thus, on seeing the images one cannot even sense that they have some secret entrenched in them. After some good number of rows for all the four embedding processes the probability is zero and remains the same for the rest of the image. Thus, this routine boasts about the well built constructs and is undoubtedly full-bodied against Chi-square test.

Complexity analysis: Advanced Encryption Standard (AES) is adopted for encrypting the confidential information, it acquaints 2^128 intricacy. Of 3 planes, one act as indicator and the

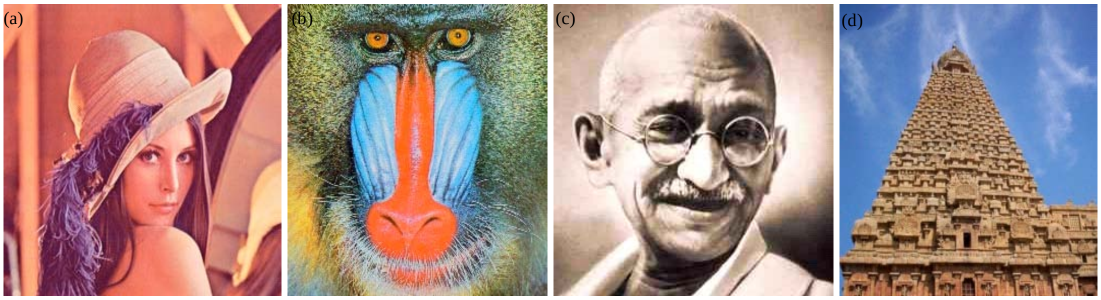

Fig. 4(a-d): Cover Images for method 1, (a) Lena, (b) Baboon, (c) Gandhi and (d) Temple

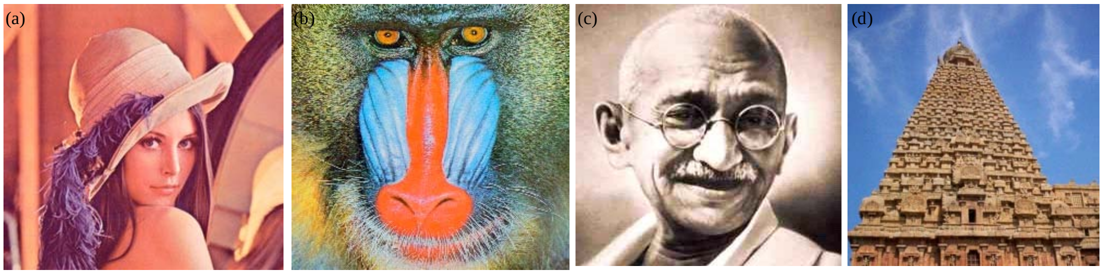

Fig. 5(a-d): Stego Images exhibiting maximum embedding capacity, (a) Lena (b) Baboon (c) Gandhi and (d) Temple

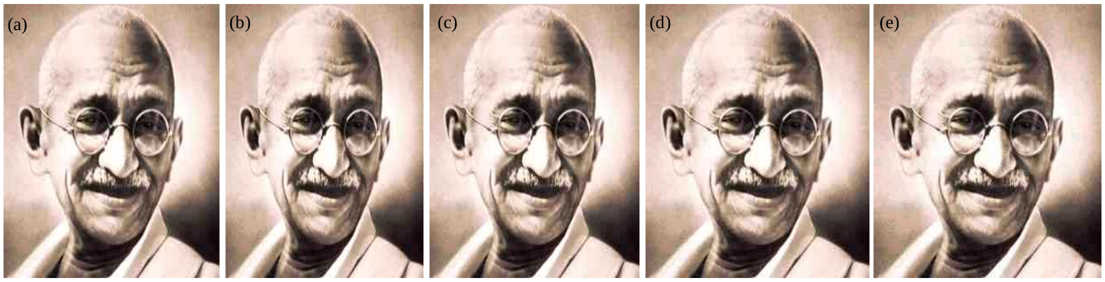

Fig. 6(a-e): Sample Results for a single image in method 1 (a) Cover image Mahatma Gandhi. Stego images for 'K' bit embedding, (b) K = 1, (c) K = 2 (d) K = 3 and (e) K = 4

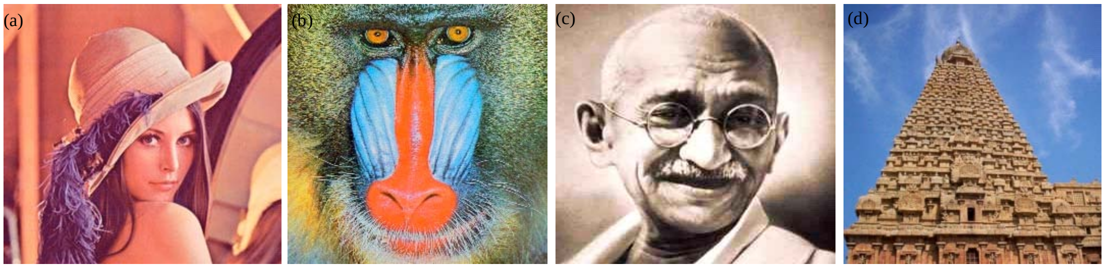

Fig. 7(a-d): Cover Images for method 2, (a) Lena, (b) Baboon, (c) Gandhi and (d) Temple

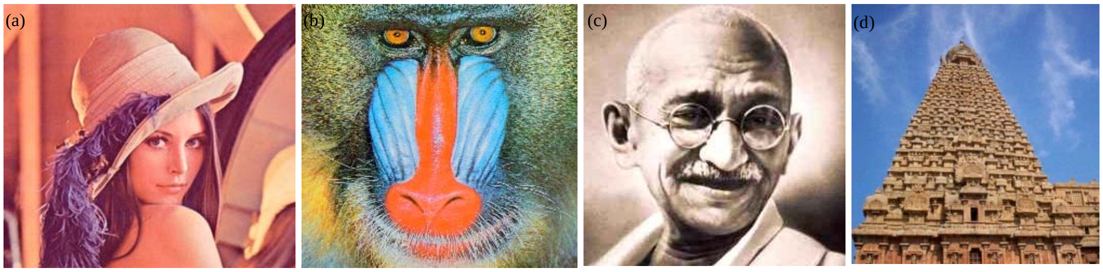

Fig. 8(a-d): Stego images exhibiting maximum embedding capacity, (a) Lena, (b) Baboon, (c) Gandhi and (d) Temple

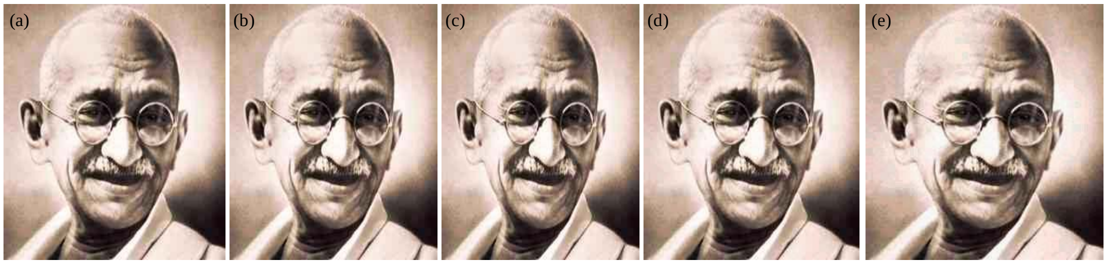

Fig. 9(a-e): Sample Results for a single image in method 2 (a) Cover image Mahatma Gandhi. Stego images for 'K' bit embedding, (b) K = 1, (c) K = 2, (d) K = 3 and (e) K = 4

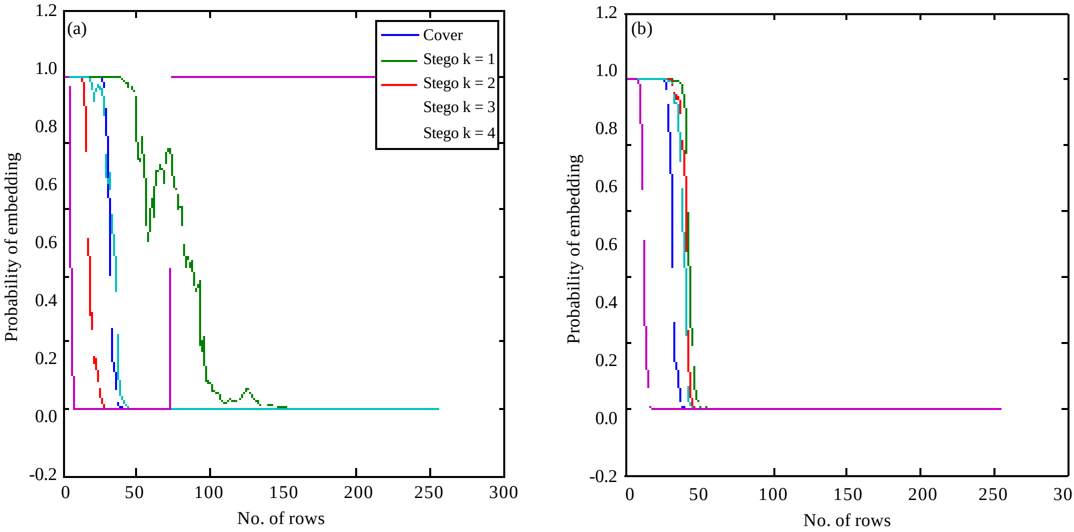

Fig. 10(a-b): Graphical results for checking (a) Method 1, (b) Method 2 against chi-square attack

other two function as data channels. This is arranged in 3×2 ways. Of the total of 8 cases, there is no embedding done for 000. This makes the total cases as 7. As a result, the total embedding complexity is given by 2^128×3×2×(8/7)×(32+(64/7)+(32/7)+(128/35)+(32/7)+(64/7)+32+256).

Table 1: MSE, PSNR, BPP and embedding capacity for method 1

		Channel red		Channel green		Channel blue		Bits per pixel (BPP)			Total No. of
Cover image	No of bits	MSE	PSNR	MSE	PSNR	MSE	PSNR	Red	Green	Blue	bits embedded
Lena	K = 1	0.1224	57.2546	0.0835	58.916	0.0812	59.0357	0.7333	0.4938	0.4897	112513
	K = 2	0.5658	50.6041	0.2469	54.2049	0.2451	54.2368	1.4667	0.9875	0.9794	225026
	K = 3	2.5230	44.1117	0.8955	48.6103	0.8985	48.5956	2.2000	1.4813	1.4691	337539
	K = 4	10.6821	37.8442	3.5512	42.6271	3.5454	42.6342	2.9333	1.9751	1.9588	450052
Baboon	K = 1	0.0918	58.5025	0.0900	58.5898	0.0851	58.8295	0.5498	0.5388	0.5146	105068
	K = 2	0.4244	51.8530	0.2721	53.7841	0.2582	54.0108	1.0997	1.0776	1.0291	210136
	K = 3	1.9041	45.3339	0.9822	48.2087	0.9498	48.3546	1.6495	1.6164	1.5437	315204
	K = 4	7.5555	39.3482	3.8442	42.2827	3.7549	42.3848	2.1993	2.1552	2.0583	420272
Mahatma Gandhi	K = 1	0.1135	57.5812	0.1001	58.1279	0.0853	58.8197	0.6838	0.6013	0.5125	117807
	K = 2	0.5374	50.8278	0.2974	53.3975	0.2551	54.0629	1.3676	1.2025	1.0251	235614
	K = 3	2.3746	44.3749	1.1038	47.7017	0.9354	48.4206	2.0514	1.8038	1.5376	353421
	K = 4	9.6022	38.3071	4.3570	41.7389	3.7039	42.4442	2.7352	2.4051	2.0501	471228
Temple	K = 1	0.1044	57.9455	0.0979	58.2239	0.0813	59.0313	0.6263	0.5914	0.4853	111612
	K = 2	0.4842	51.2802	0.2945	53.4402	0.2430	54.2755	1.2527	1.1829	0.9706	223224
	K = 3	2.1425	44.8216	1.0816	47.7903	0.8850	48.6613	1.8790	1.7743	1.4558	334836
	K = 4	8.8247	38.6738	4.1964	41.9020	3.5293	42.6539	2.5054	2.3658	1.9411	446448

Table 2: MSE, PSNR, BPP and embedding capacity for method 2

		Channel red		Channel green		Channel blue		Bits per pixel (BPP)			Total No of
Cover image	No of bits	MSE	PSNR	MSE	PSNR	MSE	PSNR	Red	Green	Blue	bits embedded
Lena	K = 1	41.3373	31.9674	51.5458	31.0089	36.7562	32.4775	0.635	0.4741	0.5021	105593
	K = 2	41.4147	31.9593	51.6745	30.9980	36.876	32.4634	1.2701	0.9482	1.0042	211186
	K = 3	42.1480	31.8830	51.9164	30.9778	37.4905	32.3916	1.9051	1.4223	1.5063	316779
	K = 4	45.1970	31.5797	53.8997	30.8149	40.4541	32.0612	2.5401	1.8964	2.0084	422372
Baboon	K = 1	100.8750	28.0930	111.0924	27.6740	114.3477	27.5485	0.5403	0.5076	0.4995	101411
	K = 2	101.0182	28.0868	111.2516	27.6677	114.5243	27.5418	1.0806	1.0152	0.9990	202822
	K = 3	101.8792	28.0500	111.7879	27.6469	114.9508	27.5257	1.6208	1.5228	1.4985	304233
	K = 4	104.4536	27.9416	113.7481	27.5714	116.8335	27.4551	2.1611	2.0305	1.9980	405644
Mahatma Gandhi	K = 1	42.6733	31.8292	38.2405	32.3056	39.6172	32.1520	0.5891	0.5304	0.5122	106932
	K = 2	42.7159	31.8249	38.3604	32.2920	39.6801	32.1451	1.1783	1.0607	1.0243	213864
	K = 3	43.0705	31.7890	39.0931	32.2098	40.3522	32.0721	1.7674	1.5911	1.5365	320796
	K = 4	45.1503	31.5842	41.7793	31.9212	43.1249	31.7835	2.3565	2.1215	2.0486	427728
Temple	K = 1	43.0098	31.7951	42.8740	31.8089	39.6781	32.1453	0.5127	0.4801	0.4964	97605
	K = 2	43.1068	31.7853	43.0070	31.7954	39.8289	32.1288	1.0255	0.9603	0.9929	195210
	K = 3	43.8453	31.7116	43.6495	31.7310	40.5275	32.0533	1.5382	1.4404	1.4893	292815
	K = 4	46.6896	31.4386	46.1350	31.4905	43.1667	31.7793	2.0510	1.9206	1.9858	390420

CONCLUSION

The process of embedding secret data based on indicator-plane increases the embedding entropy considerably. OPAP decreases the Mean Square Error (MSE) thus making the stego image indistinguishable with the Cover. Thus, the proposed method which is an amalgam of the above mentioned methods, it incorporates reduction of delectability and increase of entropy at the same time. Imperceptibility, capacity is the major expectation in image steganography both is excellent in this study.

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. 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.

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.

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.

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.

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.

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.