Journal of Applied Sciences

ISSN 1812-5654

Journal of Applied Sciences 14 (15): 1674-1688, 2014
ISSN 1812-5654 / DOI: 10.3923/jas.2014.1674.1688

Adaptive Data Hiding Based on Visual Cryptography

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

Abstract: Signals, images, emails, voice and videos, everything comes under screening before or after it is communicated. Protecting the information is highly essential especially in electronic communication which has become a stipulation in the routine life of zillions. Since safeguarding has many literal connotations, this study ntrates on one of them, privacy; technically secrecy or security. From the family of Information security, the proposed method can pick out cryptography and steganography to make this algorithm more secure and effective as well. As far as Visual Cryptography is concerned, the primary terminologies here are share, user and transparency. Its blend with steganography is worth mentionable here as it forms a new platform in information security and secret sharing. For embedding, Pixel Indicator (PI), Pixel Value Differencing (PVD) and OPAP are used. With reference to Pixel Indicator, two methods are discussed here. The effectiveness of the proposed method is assessed by calculating MSE and PSNR and the outcomes are tabulated and compared with existing methods.

Key words: Visual cryptography, pixel indicator, pixel value differencing, steganography

INTRODUCTION

At the budding of security developments, cryptography was introduced which completely destroys the user perspective of viewing and transforms the content to something that is unrecognized data. This could sustain for basic security, but as the threats started rising, cryptography succumbed as the process is well known to the viewer. As an enhancement, method whose changes are unperceivable irrespective of any operation was required. This got steganography and watermarking to limelight (Stefan and Fabin, 2000). Cryptography is an art of providing data security using methods of encryption and decryption (Schneier, 2007).

Cryptography lends a helping hand in keeping information safe and sound (Schneier, 2007). This is its ultimate aim for which the modern era version has come up with vast and different practices and procedures for real time application. Scores of cryptic algorithms are formulated for security's sake and of which the one that has recently found surprising is the expanse of Visual Cryptography (Noar and Shamir, 1995; Amirtharajan*et al*., 2013a, b) . It of course, has its origin from conventional cryptography. In simple words to put it, message to be communicated (secret) to the other end undergoes segmentation and is sent in operated forms. Thus, at the receiving end, one has to merge all the segments in a right way to read the secret.

Visual cryptography is a branch of cryptography concerned with providing data security using black and white pixels. As the name indicates, visual cryptography is based on human vision. It uses the characteristics of human vision to decipher the original message from the scrambled or encrypted images. It is an emerging trend of cryptography which uses the concept of shares. It assumes that the message consists of black and white pixels and each pixel appears in 'n' modified forms. These modified forms are called shares (Noar and Shamir, 1995; Amirtharajan *et al*., 2013a, b). Unlike other techniques, it does not require any knowledge of cryptography techniques. Also, it does not require any complex computations. Hence it is simple and self-sufficient in providing data security. Visual cryptography guarantees that hackers cannot comprehend the ideas about a secret image from different cover images. For instance, if there are 'n' images, then there shall be a constant 'k' of such images. Hence the secret can be revealed with 'n' or 'n-1' such images but not just with 'k' images. This comes from the fact that the output media of visual cryptography are transparencies as shown in Fig. 1. This term evolves from the way the white pixels of black and white images are considered as transparent. This method, also known as the black and white visual cryptography breaks down every pixel of the secret image into a 2×2 block. Hence the cover can be shared among a group of 'n' people.

Steganography invented by the Greek is a method of "covered writing" where only the beneficiary knows the existence of the secret message apart from the sender, even if were available on a public forum (Amirtharajan *et al*., 2011, 2012, 2013c-i;

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

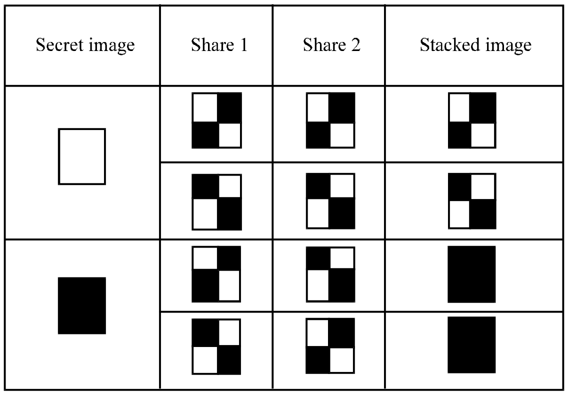

Fig. 1: Visual cryptography shares

Amirtharajan and Rayappan, 2012a-d; Cheddad *et al*., 2010; Hmood *et al*., 2010a, b; Janakiraman *et al*., 2012a, b; Padmaa *et al*., 2011; Thenmozhi *et al*., 2012). The secret message is transformed into a stego message when it is embedded on an innocent carrier medium i.e., a document (Al-Azawi and Fadhil, 2010; Xiang *et al*., 2011; Yang *et al*., 2011), picture, Image (Al-Frajat *et al*., 2010; Amirtharajan *et al*., 2011, 2012, 2013c-i; Amirtharajan and Rayappan, 2012a-d, 2013; Chan and Cheng, 2004; Hmood *et al*., 2010a, b; Janakiraman *et al*., 2012a, b; Zanganeh and Ibrahim, 2011) or an audio file (Zhu *et al*., 2011).

The image post the embedment of the data is known as stego image is then sent into a public forum which can be accessed by the intended user or even the general public (Chang *et al*., 2003; Chang and Tseng, 2004; Hong *et al*., 2009; Zhao and Luo, 2012). The only difference would be that the public would not even suspect the presence of any hidden messages (Luo *et al*., 2008, 2011; Praveenkumar *et al*., 2012a, b, 2013a, b; Mohammad *et al*., 2011; Xiang *et al*., 2011; Yang *et al*., 2011); however, the user would have known the presence of a message and will also know how to extract it. Steganography alone is not robust technique as a statistical analysis would give away the presence of a secret message (Stefan and Fabin, 2000). Steganography needs to be coupled with techniques to fortify the algorithm and protect the data (Mohammad *et al*., 2011; Rajagopalan *et al*., 2012; Zaidan *et al*., 2010).

This study proposed a method to combine Visual Cryptography (VC) with random image steganography (RIS). The next section describes the proposed method with neat diagram and algorithm, to combine VC with RIS in material and methods followed by the result and discussion with comparative existing methods. The final section explorers the conclusion of this study.

MATERIALS AND METHODS

Cryptography enables information security by employing techniques in which the data is scrambled by a key in the process called encryption and re scrambling the encrypted message again with the key in order to get back the original data in the process called decryption. Here, the key plays a vital role. Without the correct key, the scrambled message cannot be recovered (Hou, 2003). Visual cryptography assumes that the message consists of black and white pixels and each original pixel appears in n modified versions called shares (Amirtharajan *et al*., 2013a-b). Each share is a collection of m black and white sub pixels and is generated by doing mathematical operation between subset (n X m) of original message and permuted version of any one of the two (n X m) random matrix Noar and Shamir (1995).

In Steganography the confidential information is embedded into innocent looking cover objects, such as digital images (Chang *et al*., 2003; Chang and Tseng, 2004; Chan and Cheng, 2004; Cheddad *et al*., 2010; Thanikaiselvan *et al*., 2012a-b, 2013). In this proposed method, visual cryptography and tri color random image steganography is combined for multiple users. Figure 2 represents the basic block diagram for this proposed method. For embedding, input color image can be taken as secret. To make encryption easy, color image should be converted into gray scale image. Dithering is used to convert gray image into binary image. By using (k, n) threshold scheme, shares are generated (Noar and Shamir, 1995) and these shares are once again encrypted with different keys. Then these encrypted shares are embedded in the cover image using Pixel indicator method.

In pixel indicator method (Gutub, 2010; Padmaa *et al*., 2011; Padmaa and Venkataramani, 2010) any one of the color plane is treated as indicator plane and remaining two planes are used to embed the data. The color plane for data embedding is decided by the last two bits of the pixel of indicator plane. The number of bits to be embedded is decided by calculating the difference value d between the maximum pixel value and the minimum pixel value of three neighbor pixels (Padmaa *et al*., 2011) and the quality of stego image is enhanced by OPAP method (Chan and Cheng, 2004). There are more explanation on steganography methods and its advantages are available in Amirtharajan *et al*. (2011, 2012, 2013c-i) and Zanganeh and Ibrahim (2011). For recovery, stego image is considered. Based on the last two LSB bits of each pixel in the indicator plane, the shares are recovered by using PVD method and then descrambled by using the keys (Gutub, 2010). These descrambled shares are stacked and

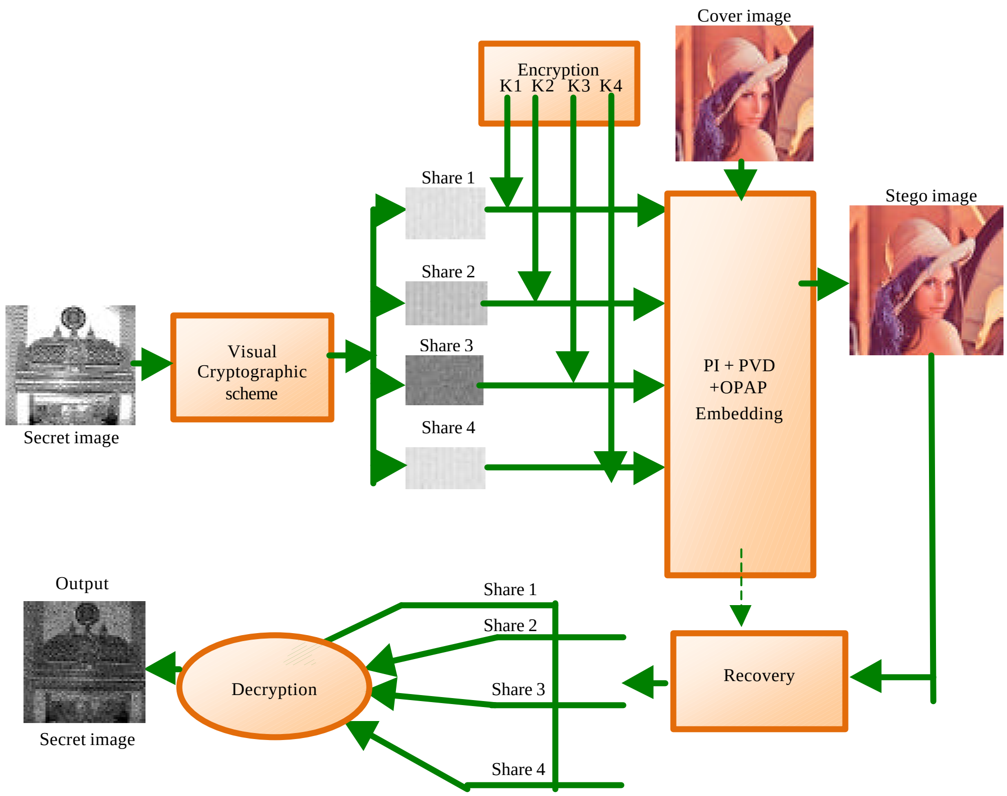

Fig. 2: Block diagram of proposed method

extracted and then split into shares by decryption with keys which have been used in encryption. Then these decrypted shares are stacked and the original secret image is obtained.

EMBEDDING ALGORITHM

Method 1:

- Read the Cover image (U) and Secret image (S)
- Apply (k, n) Threshold scheme to secret image which constructs four shares of this secret image say S1, S2, S3 and S4
- Divide the color cover image into three planes (Red, Blue and Green)
- In this first method, take the default indicator as Red and perform the following
  - Let r [0] = First LSB of current pixel in Red plane
  - Let r [1] = Second LSB of current pixel in Red plane
  - If r = 00, then

No entrenching, move to next pixel

Else if r = 01, then

Scramble the first share of secret image S1 with key K[1], then embed the scrambled first share S1 in current pixel of Green plane by means of PVD

Else if r=10, the

Scramble the second share of secret image S2 with key K[2], then embed the scrambled second share S2 in current pixel of Blue plane by means of PVD

Else

Scramble the third and fourth shares of secret image S3 and S4 with key K[2], then embed the scrambled shares in both the planes by means of PVD

Once all the shares are embedded, apply OPAP to get the Stego image (V)

RECOVERY ALGORITHM

- Read the Stego image (V) and split into three planes
- To retrieve the embedded shares of secret image, verify the last two bits of the Indicator plane

If r = 00, travel to next pixel

Else if r = 01, then

Recover the First share S1 from Green plane by means of PVD and descramble it with key K [1]

Else if r = 10, then

Recover the second share S2 from Blue plane by means of PVD and descramble it with key K [2]

Else

Recover the third and fourth share S3 and S4 from Green and Blue planes by means of PVD and de-scramble it with keys K [3] and K [4], respectively

If all the shares are recovered, combine it to acquire the Secret Image(S)

Method 2: Embedding algorithm

- Read the Cover image (U) and Secret image (S)
- Apply (k, n) Threshold scheme to secret image which constructs four shares of this secret image say S1, S2, S3 and S4
- Divide the color cover image into three planes (Red, Blue and Green)
- In this method, Indicator planes are chosen in a cyclic manner
  - Let E[0] = Indicator plane; E[1] and E[2] = Data Channel1 and 2
  - Let r[0] = First LSB of current pixel in Red plane
  - Let r[1] = Second LSB of current pixel in Red plane
  - If r = 00, then

No entrenching, move to next pixel

Else if r = 01, then

Scramble the first share of secret image S1 with key K [1], then embed the scrambled first share S1 in current pixel of Data channel1 E[1] by means of PVD

Else if r=10, then

Scramble the second share of secret image S2 with key K[2], then embed the scrambled second share S2 in current pixel of Data channel2 E[2] by means of PVD

Else

Scramble the third and fourth shares of secret image S3 and S4 with keys K [3] and K [4] and then embed the scrambled shares in both the data channels by means of PVD

- Once all the shares are embedded, apply OPAP to get the Stego image (V)

Recovery algorithm:

- Read the Stego image (V) and split into three planes
- To retrieve the embedded shares of secret image, verify the last two bits of the Indicator plane

  If r = 00, travel to next pixel

  Else if r = 01, then

  Recover the first share S1 from Data channel1 E [1] by means of PVD and de-scramble it with Key K [1]

  Else if r=10, then

Recover the second share S2 from Data channel2 E[2] by means of PVD and de-scramble it with Key K [2]

Else

Recover the third and fourth share S3 and S4 from both the data channels by means of PVD and descramble it with keys K [3] and K [4], respectively

- If all the shares are recovered, combine it to acquire the Secret Image (S)

RESULTS AND DISCUSSION

In this execution, four cover color images Lena, Baboon, Mahatma Gandhi and Temple of size 256×256 are chosen for embedding. The cover and stego images along with their histograms are shown in Fig. 3-10. This algorithm is simulated in MATLAB 7.1. To have an idea about effectiveness of the system, MSE, PSNR, BPP and embedding capacity are calculated and tabulated in Table 1, 2 and 3. The equations are:

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

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

$$\text{Embedding Capacity} = \text{Bits per pixel} \times \text{No. of pixels in the cover image}$$

For the chosen images, full embedding capacity for the two methods is examined here. Method 1 takes RED as indicator; as per the algorithm no embedding is done in this plane. It is clear from the table that all the images

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	0.6949	49.7115	0.5898	50.4241	0	0.8439	0.8113	105982
Baboon	0	8	2.2491	44.6106	2.3251	44.4664	0	1.4287	1.4496	188639
Mahatma Gandhi	0	8	0.6194	50.2108	0.6165	50.2312	0	0.8123	0.8278	107492
Temple	0	8	0.9323	48.4354	0.8759	48.7064	0	0.9435	0.9443	123725

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	0.4127	51.9749	0.4434	51.66	0.3772	52.3650	2.1952	2.2218	2.1329	142982
Baboon	1.4478	46.5237	1.4590	46.49	1.5046	46.3566	3.7520	3.7594	3.8207	247553
Mahatma Gandhi	0.4016	52.0926	0.3969	52.14	0.3934	52.1821	2.1019	2.1373	2.1352	139251
Temple	0.6361	50.0954	0.6005	50.34	0.5663	50.6002	2.5418	2.4891	2.4916	164331

Table 3: Comparative estimation parameters of the proposed embedding method 2

		Pixel indicator method (Padmaa *et al*., 2011)			Pixel authorized by pixel to trace (Amirtharajan and Rayappan, 2012c)			Proposed method		
Cover image	Parameter	Ch-I (R)	Ch-II (G)	Ch-III (B)	Ch-I (R)	Ch-II (G)	Ch-III (B)	Ch-I (R)	Ch-II (G)	Ch-III (B)
Lena	MSE	1.227	1.3641	1.02	2.4387	2.3066	2.3389	0.4127	0.4434	0.3772
Babboon		4.065	4.002	4.2847	2.3702	2.3255	2.3255	1.4478	1.4590	1.5046
Gandhi		1.348	1.2901	1.2478	1.3480	0.5798	2.3595	0.4016	0.3969	0.3934
Temple		1.853	1.766	1.632	2.3143	2.3095	2.3764	0.6361	0.6005	0.5663
Lena	PSNR	47.24	46.782	48.045	44.2590	44.5010	44.4410	51.9749	49.7115	52.3650
Babboon		42.04	42.108	41.812	44.3829	44.4657	44.4390	46.5237	44.6106	46.3570
Gandhi		46.83	47.025	47.169	44.0267	44.2904	44.4030	52.0926	50.2108	52.1820
Temple		45.45	45.662	46.003	44.4866	44.4957	44.3720	50.0954	48.4354	50.6010
Lena	BPP	2.114			3.9181			2.1817		
Babboon		3.651			3.9232			3.777		
Gandhi		2.028			3.9184			2.1248		
Temple		2.351			3.9240			2.5075		
Lena	Embedding capacity	138549			261780			142982		
Babboon		239262			261824			247553		
Gandhi		132945			263244			139251		
Temple		154409			262000			164331		

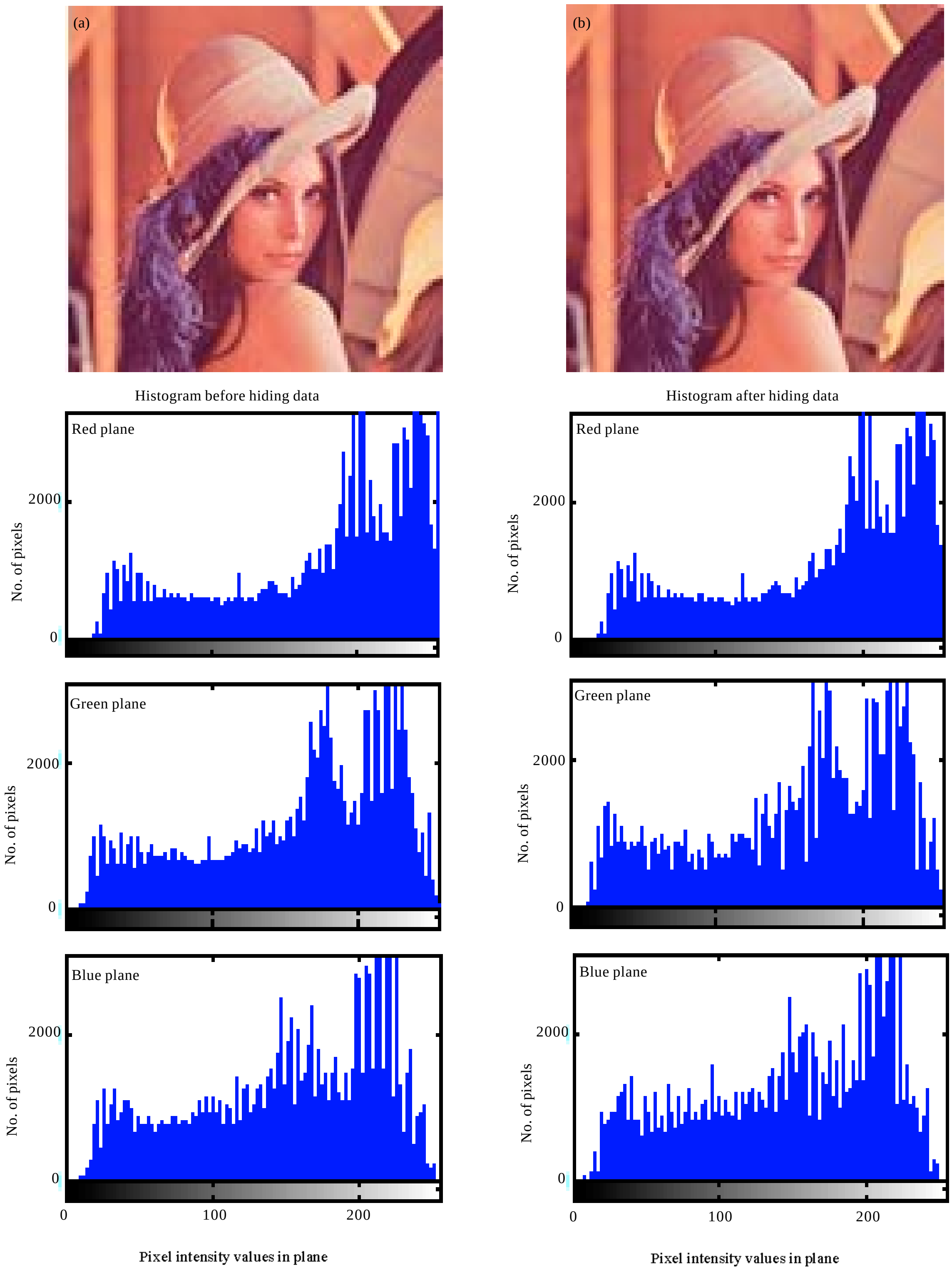

Fig. 3(a-b): (a) Cover and (b) Stego images of Lena and their corresponding histograms

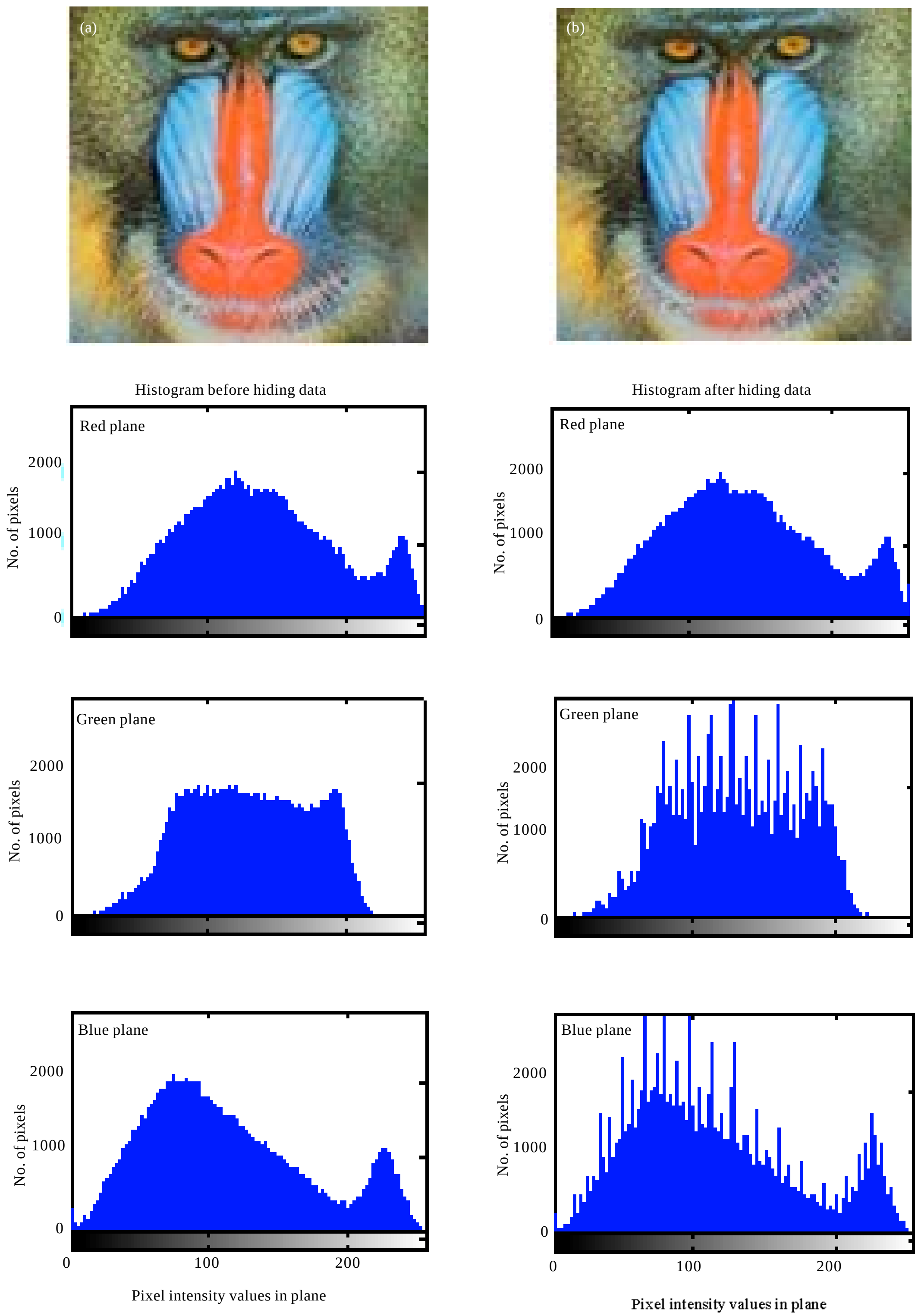

Fig. 4(a-b): (a) Cover and (b) Stego images of Baboon and their corresponding histograms

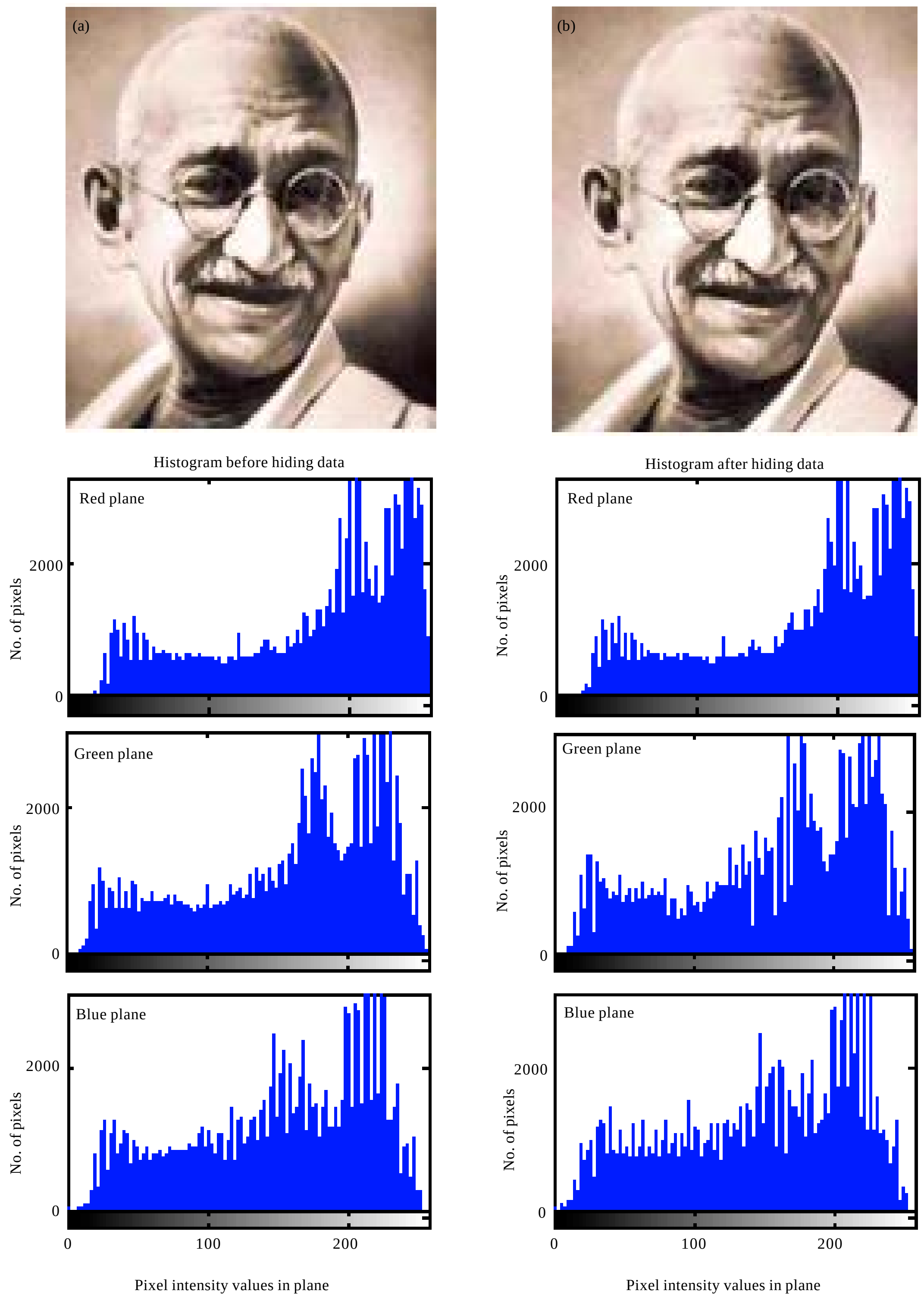

Fig. 5(a-b): (a) Cover and (b) Stego images of Mahatma Gandi and their corresponding histograms

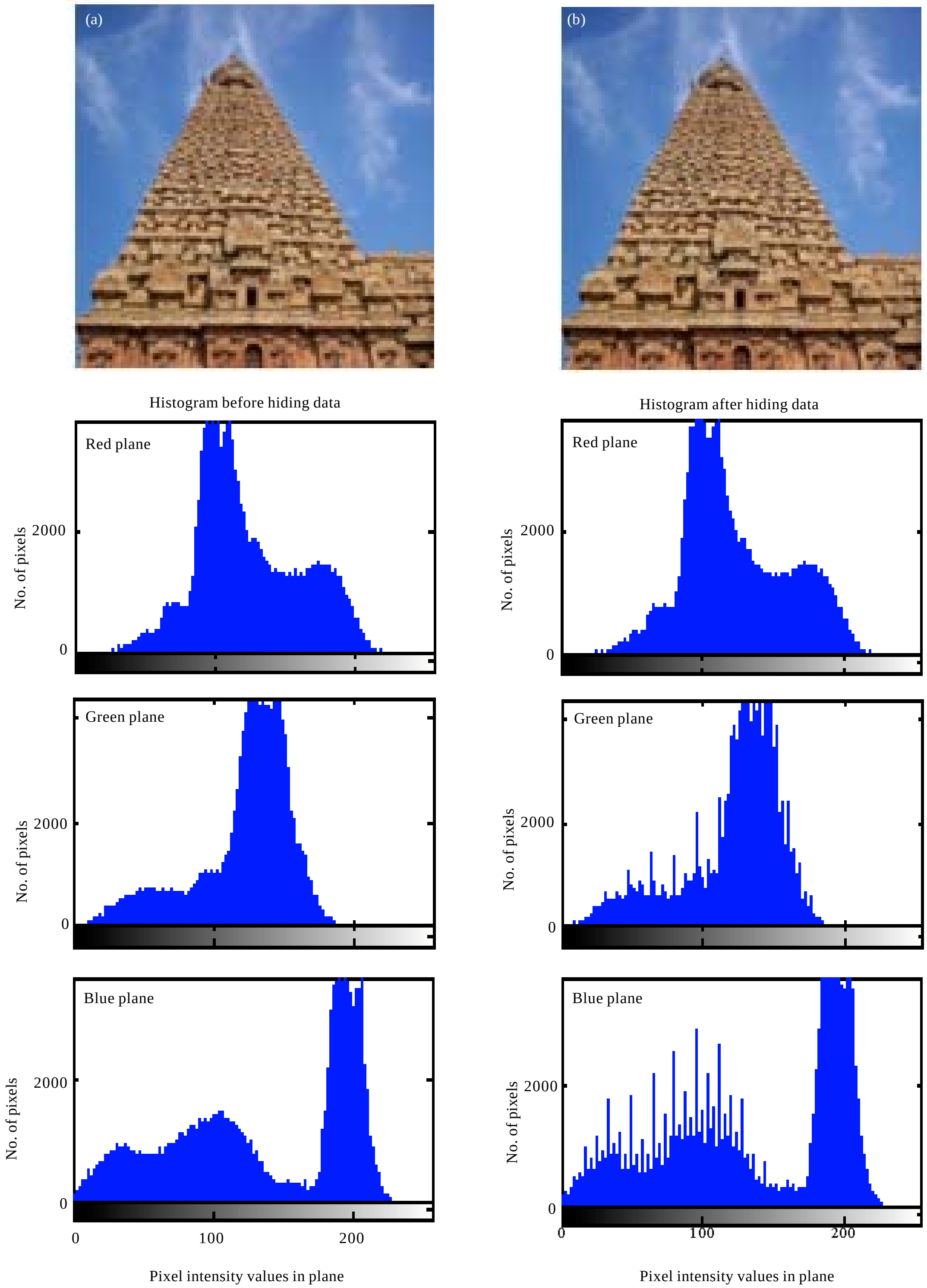

Fig. 6(a-b): (a) Cover and (b) Stego images of Temple and their corresponding histograms

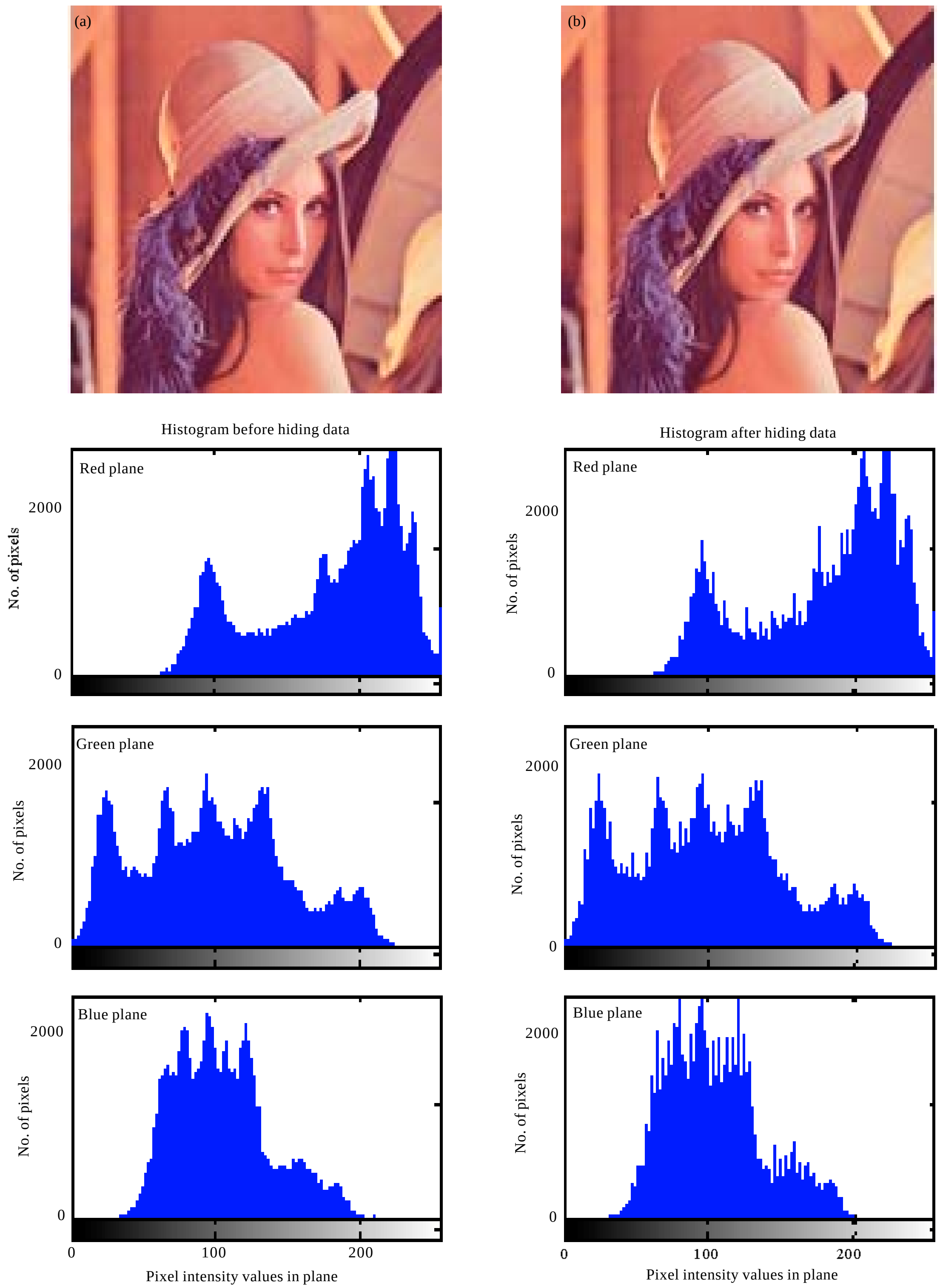

Fig. 7(a-b): (a) Cover and (b) Stego images of Lena and their corresponding histograms

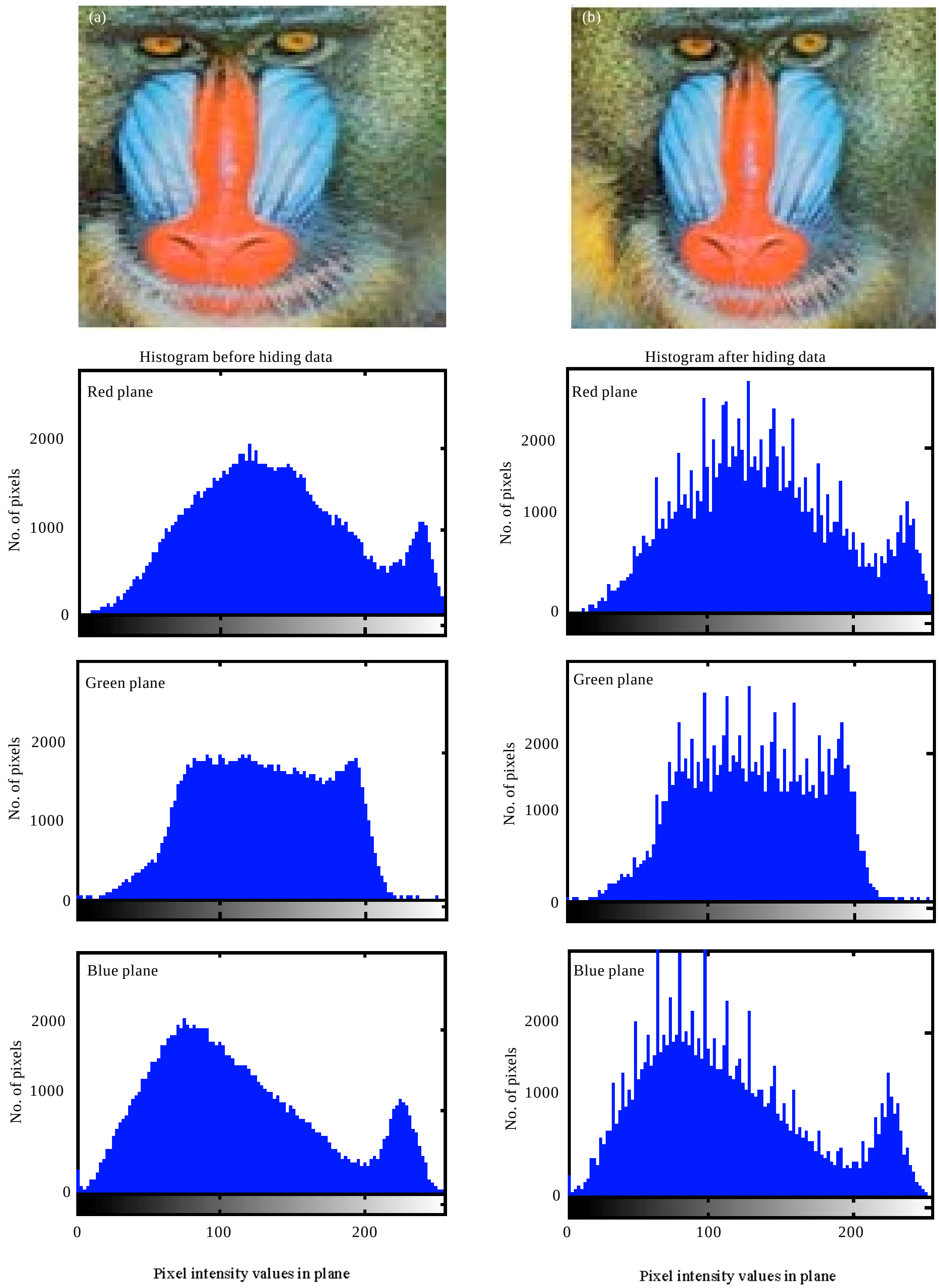

Fig. 8(a-b): (a) Cover and (b) Stego images of Baboon and their corresponding histograms

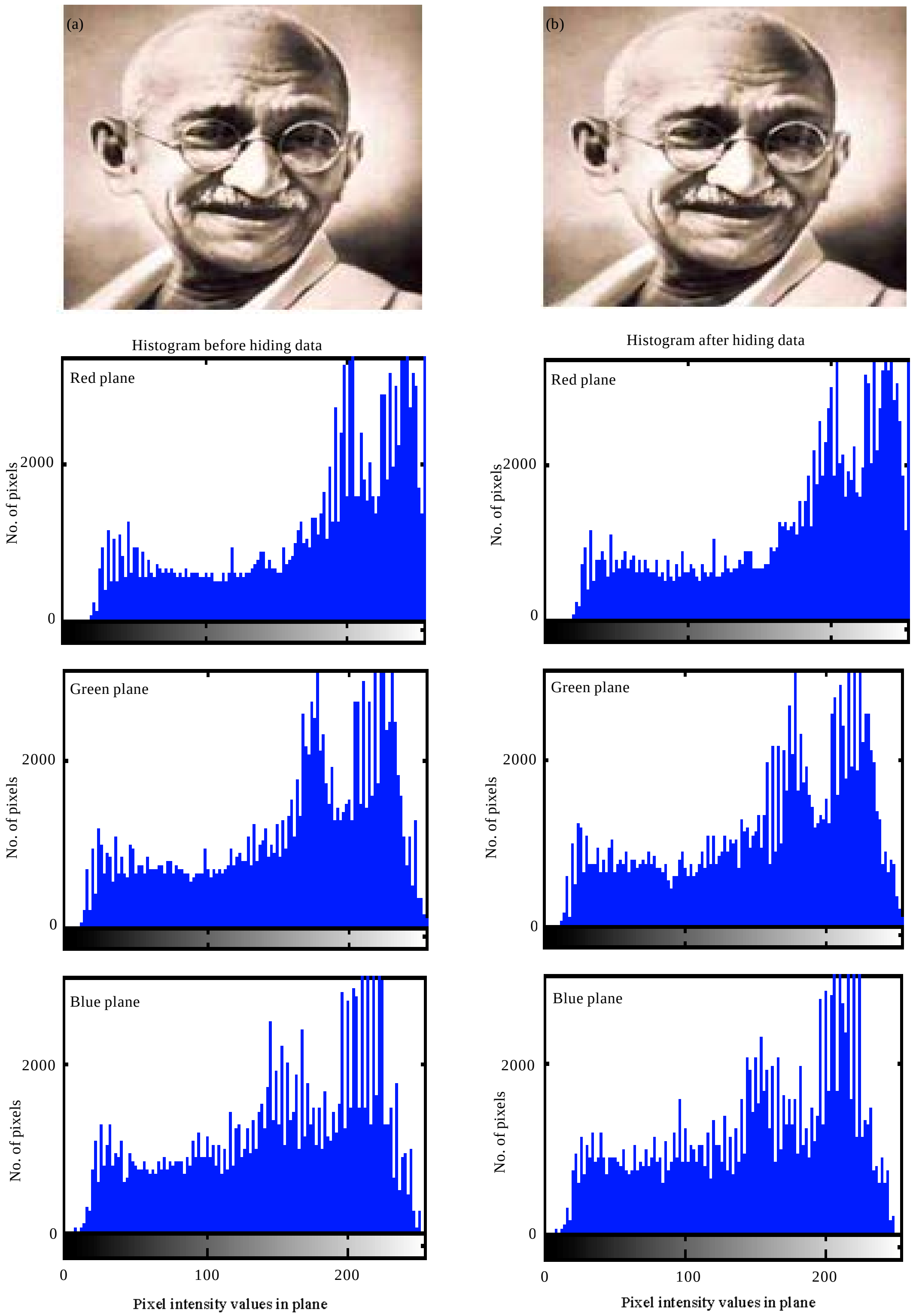

Fig. 9(a-b): (a) Cover and (b) Stego images of Mahatma Gandhi and their corresponding histograms

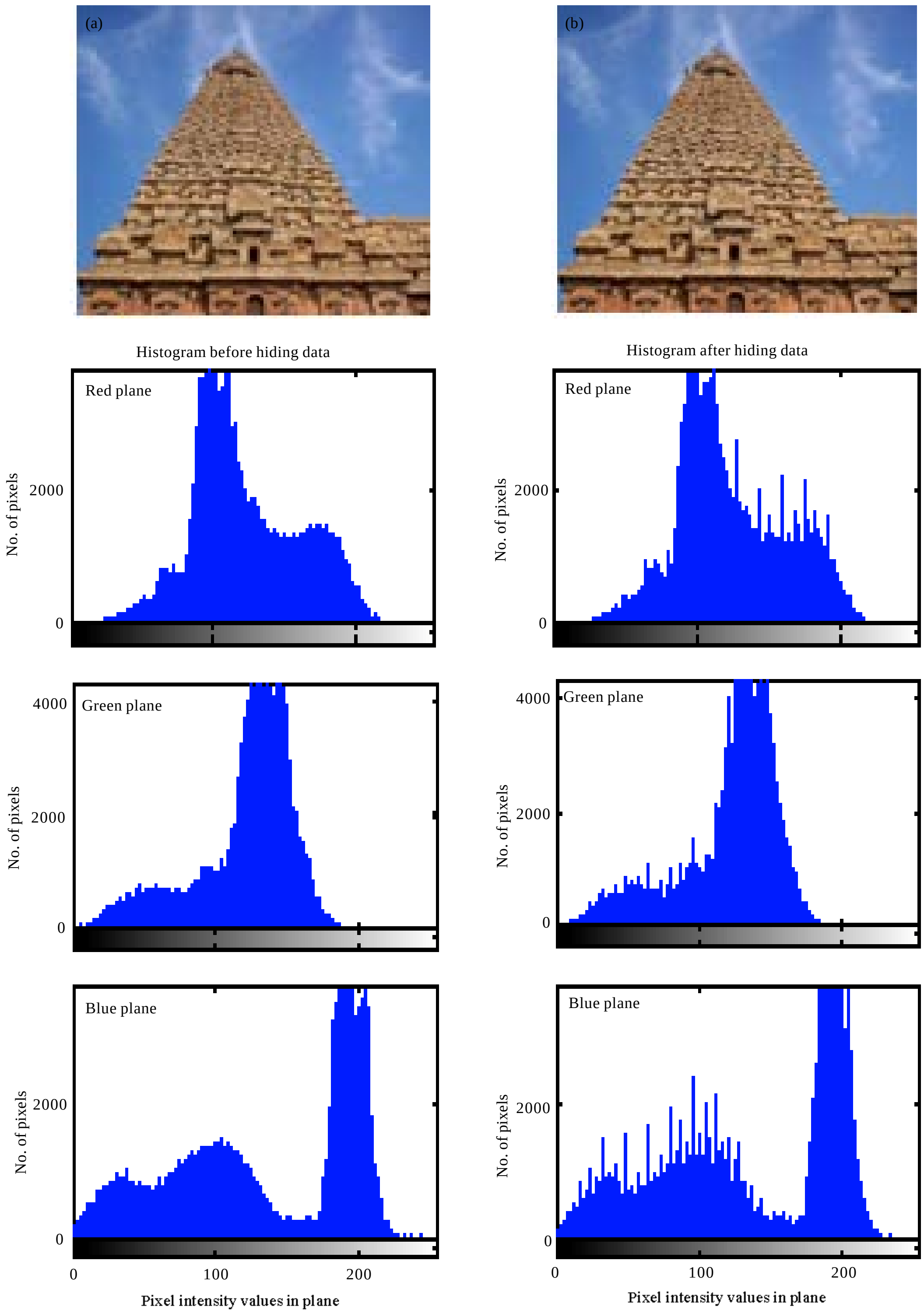

Fig. 10(a-b): (a) Cover and (b) Stego images of Temple and their corresponding histograms exhibit high PSNR. In general, PSNR of above 38 dB is rendered good. So, all these images possess high PSNR, which indicates high imperceptibility; that is the images are prone to visual attack and escape it. Thus one cannot sense the hidden data in the images. Conversely, MSE is very low. But Baboon has relatively high MSE of all. In turn it has the highest embedding capacity. Relatively decent BPP is obtained in all images. Also, high embedding capacity highlights this routine. Indicator is cyclically selected in method 2, where each plane will have a chance of being the indicator. The images possess high BPP and also embedding capacity is also high. Approximately, 2.6445 bits are embedded in each plane which is determined to be fair. Thus, method 2 gives anticipated results and is best. This method exhibit higher imperceptibility, security and is highly robust to steganalytic attacks.

Comparison of existing methods with proposed method: In pixel indicator method (Padmaa *et al*., 2011), any one of the colour planes is assumed to be the indicator and data is embedded accordingly. In pixel authorised by pixel with pixel indicator method (Amirtharajan and Rayappan, 2012c), Hilbert SFC and Moore SFC traversing path based steganography techniques are applied. Here a block of 4x4 pixels are taken and the above methods are implemented on it by adapting a common traversing path for the sender and receiver. Then the entire cover image is taken for secret bit embedding by considering it as multiple 4×4 blocks to cover up the entire $2^8\times2^8\times3$ pixels. The pixel indicator method here is used to select a particular channel as an indicator. Then data embedding in other channels is done based upon the last two bits of the indicator.

CONCLUSION

In this proposed method, Cryptography, Visual Cryptography and Steganography are put together to enhance the security and robustness. The method minimizes the perceptibility of the introduced distortion. Compared with Pixel indicator and Pixel authorized by pixel to trace with Pixel indicator methods, our proposed method makes stego-image so strong. Four parameters namely MSE, PSNR, BPP and embedding capacity are used as metrics for comparison. Visual cryptography with steganography will provide minimum MSE and maximum PSNR and moderate embedding capacity. These parameters decide the imperceptibility and robustness of a stego-image. This method provides better resistance against various forms of attacks.

ACKNOWLEDGMENT

The first author expresses her sincere gratitude to Dr. R. Amirtharajan Associate Professor/ECE School of Electrical and Electronics Engineering, for his guidance in providing technical and linguistic support for fructifying the 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.

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

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

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

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

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

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

Amirtharajan, R., J. Qin and J.B.B. Rayappan, 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., S. Sulthana and J.B.B. Rayappan, 2013g. Seeing and believing is a threat: A visual cryptography schemes. Res. J. Inform. Technol., 5: 435-441.

Amirtharajan, R., S. Sulthana, P.S. Priya, G. Revathi, A.K. Infant and J.B.B. Rayappan, 2013h. Seeable visual but not sure of it-A visual cryptographic perspective for TAMIL characters. Int. J. Eng. Technol., 5: 2000-2007.

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

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

Chang, C.C., J.Y. Hsiao and C.S. Chan, 2003. Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy. Pattern Recogn., 36: 1583-1595.

Chang, C.C. and H.W. Tseng, 2004. A steganographic method for digital images using side match. Pattern Recognition Lett., 25: 1431-1437.

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.

Hou, Y.C., 2003. Visual cryptography for color images. Pattern Recognit., 36: 1619-1629.

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.

Noar, M. and A. Shamir, 1995. Visual Cryptography. In: Advance in Cryptography, DeSantis, A. (Ed.). Springer, Netherlands, pp: 1-12.

Padmaa, M. and Y. Venkataramani, 2010. ZIG-ZAG PVD-a nontraditional approach. Int. J. Comput. Appl., 5: 5-10.

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.

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., 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.

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.

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.