Research Journal of Information Technology

ISSN 1815-7432

Academic Journals Inc.

www.academicjournals.com

Research Journal of Information Technology 5 (3): 329-340, 2013
ISSN 1815-7432 / DOI: 10.3923/rjit.2013.329.340
© 2013 Academic Journals Inc.

Rubik's Cube: A Way for Random Image Steganography

[1]Rengarajan Amirtharajan, [2]M. Venkata Abhiram, [1]G. Revathi, [1]J. Bharathsimha Reddy, [3]V. Thanikaiselvan and [1]J.B.B. Rayappan

[1]School of Electrical and Electronics Engineering, SASTRA University, 613401, India
[2]IIM Shillong, Meghalaya, 793 014, India
[3]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

This study proposes an innovative methodology that incorporates the famous Rubik's cube into steganography. Rubik's cube is a pivot mechanism that enables each face to turn independently thus allowing mixing up of colors. By using this mechanism to represent the three planes of a color image (Red, Green, and Blue) the randomness of the stego image can be improved. The pixel intensity values can additionally be used as pointers to indicate the type of shift that needs to be done to the pixels in three planes. This study contains the experimental results that validate the superiority of this methodology compared to other existing ones in terms of imperceptibility, robustness and with reasonable embedding capacity. It is also found to be more resistant to steganalysis.

Key words: Cryptography, data hiding, information security, Rubik's cube, steganography

INTRODUCTION

Human way of communication has come a long way from cave drawings and drums to electronic mails. As more and more information is communicated electronically, new needs, issues and opportunities are born. Authenticity and secret sharing are becoming the prime concerns (Abdulfetah *et al*., 2010; Zaidan *et al*., 2011). Data encryption (Salem *et al*., 2011; Schneier, 2007) and data hiding (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) are so increasingly being used to protect the sensitive data from disclosure when they are transmitted over an insecure channel.

Imperceptibility and high embedding capacity coupled with robustness are the three main criteria that decide the performance of any stego algorithm (Amirtharajan and Rayappan, 2012a-d; Amirtharajan *et al*., 2012). Imperceptibility and embedding capacity are the two main concerns of steganography while robustness is the prime concern of water marking (Amirtharajan *et al*., 2012; Abdulfetah *et al*., 2010; Stefan and Fabin, 2000; Zeki *et al*., 2011).

Data can be hidden in a grayscale (Amirtharajan and Rayappan, 2012a) or color (Gutub, 2010; Padmaa *et al*., 2011) image because slight changes to colors of pixels are imperceptible to the eye

(Amirtharajan and Rayappan, 2012a-d). The principle of LSB substitution can be used to induce these changes, that is to embed data into the cover image. The modified image is known as stego image (Chan and Cheng, 2004). Given a color image each pixel is represented by three bytes. Each byte represents a color component, typically red, green, and blue (Padmaa *et al.*, 2011). Furtive information, in bits, is veiled by laying it as LSBs in pixel bytes. The least significant bit is either a 0 or 1. The former is also the same. Hence, typically no more than half LSBs get altered through bits shrouding.

An improvement to basic LSB substitution is to hide a bit in a pixel only if the pixel satisfies certain conditions (Zanganeh and Ibrahim, 2011) or after randomization of the pixel (Zhao and Luo, 2012). Hmood *et al.* (2010a, b) described the capacity of information hiding and an overview about steganography. Luo *et al.* (2011) explains secret sharing and data hiding for clandestine information adopting block truncation coding in compressed images. Several methods are available in the literature for different cover objects (Bender *et al.*, 1996; Cheddad *et al.*, 2010; Janakiraman *et al.*, 2012a, b; Rajagopalan *et al.*, 2012; Thenmozhi *et al.*, 2012) like text (Al-Azawi and Fadhil, 2010; Xiang *et al.*, 2011), image (Amirtharajan and Rayappan, 2012a-d; Amirtharajan *et al.*, 2012; Luo *et al.*, 2011; Mohammad *et al.*, 2011), audio (Zhu *et al.*, 2011) and video (Al-Frajat *et al.*, 2010). Nevertheless a method is seldom considered for data hiding in scrambled images.

This study advises an unequalled model for image steganography in which Rubik's cube theory is practised to scramble an image and then secret data entrenching is entitled using cyclic pixel indicator and LSB substitution.

PROPOSED METHOD

In this proposed methodology the pixels are first scrambled and then data is embedded based on their intensity values. For scrambling, the famous Rubik's cube methodology is implemented (Yen and Lin, 2010). The three rows of a face of the Rubik's cube are taken as the three components of the color pixel (Loukhaoukha *et al.*, 2012). For instance, the first row is taken as red, the second row green and third blue. Based on the third and fourth bits of the bytes of a particular component, the other two components are scrambled by rotation. Then by using the first and second bits of a channel as pointer, embedding is carried out in the other two channels. This accounts for improved randomness that can resist any steganalysis (Qin *et al.*, 2010). Embedding capacity is also enhanced as all the three channels are effectively used in hiding data.

A comparison of the original image and the stego image would show an attacker which bits have been modified and may serve as the basis of a successful attack on the hidden data. That is why the original image should be destroyed right after the stego image has been prepared.

This study wishes for a methodology of k = 2 bit embedding derived from the expertise of Rubik's cube. The algorithm comprises of both image scrambling and embedding to pull off the aspiration of secret sharing. Scrambling procedure is defined which involves shifting of bits. The diagram of Rubik's cube and its rotated and scrambled image is shown in Fig. 1.

Pixel indicator technique is used in this paper where indicator channel is cyclically chosen. The proposed block diagram is given in Fig. 2. Here, the secret data is embedded in to cover image which is scrambled using Rubik's cube. The embedded image is descrambled as original image to get stego image. Then the stego image is scrambled using Rubik's cube and then extracted to get the original data.

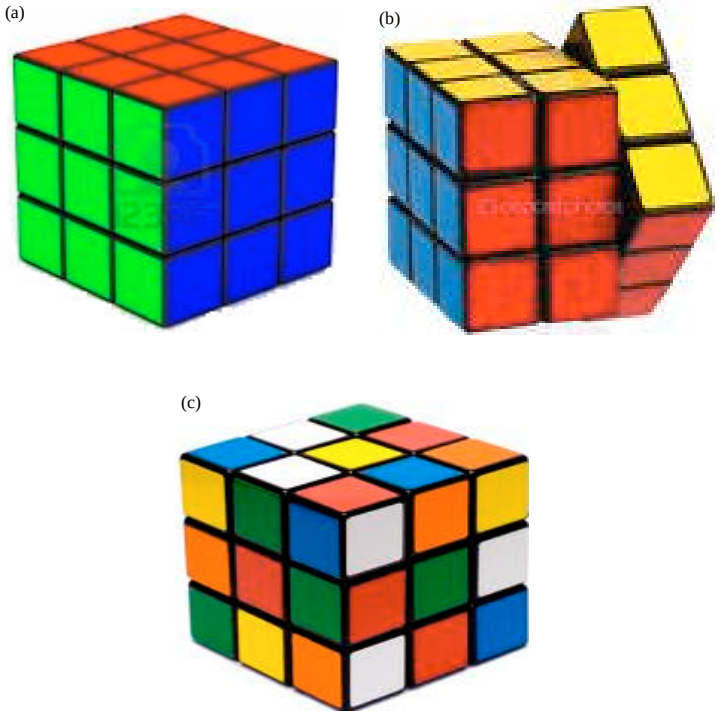

Fig. 1(a-c): (a) Rubik's cube (b) Rotated Rubik's cube and (c) Scrambled Rubik's cube

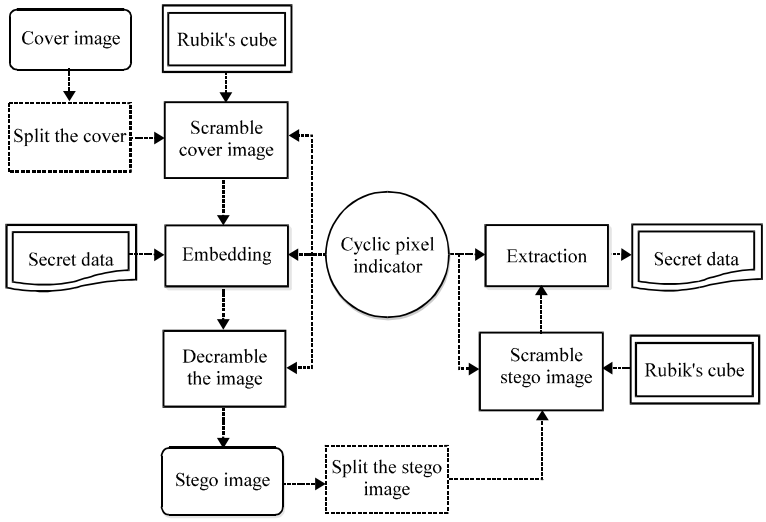

Fig. 2: Block diagram for proposed method

Algorithm for embedding:

- Read the cover image and secret data
- Divide the cover image into Red, Green and Blue planes
- Convert secret data into binary
- Read the number of rows and columns for scrambling using Rubik's cube

Algorithm for embedding: Continue

- Follow cyclic pixel indicator method (Eg: R is 1st plane; G is 2nd plane; B is 3rd plane) and consider 3rd and 4th LSBs in indicator channel for scrambling.

  If the bits are

  00 = don't scramble

  01 = scramble 2nd plane

  10 = scramble 3rd plane

  11 = scramble both the planes

  Scrambling procedure:

  In the first pixel of data channel, the first bit is temporarily assigned to a separate variable (Temp) and the subsequent bits are shifted one position right as in Fig. 3. After shifting nth bit to n-1th position, the first bit is placed in the nth position as in Fig. 4. This procedure is followed for scrambling in all the planes. For descrambling the image, the reverse procedure is adopted.
- Merge all the scrambled planes to form a scrambled image and split that image into R, G and B planes again
- Follow cyclic pixel indicator method and consider last 2 LSBs in the indicator channel for embedding

  If the bits are 00, then don't embed

  Else If 01, then embed 2 bits of secret data in 2nd plane

  Else If 10, then embed 2 bits of secret data in 3rd plane

  Else (bits = 11) embed 2 bits of secret data in both the planes
- If all the secret data are embedded, descramble it as original image and then store it as resultant stego image

Algorithm for extraction:

Read the stego image

Split the image into red, green and blue planes

Scramble the image by using 5th step from embedding algorithm

Merge all the scrambled planes to form a scrambled image and split that image into R, G and B planes again

Follow the cyclic pixel indicator method and consider last 2 LSBs in the indicator channel for extraction

If the bits are 01, then extract 2 bits from 2nd plane

Else if 10, then extract 2 bits from 3rd plane

Else (bits = 11) extract 2 bits from both the planes

Store the original secret data

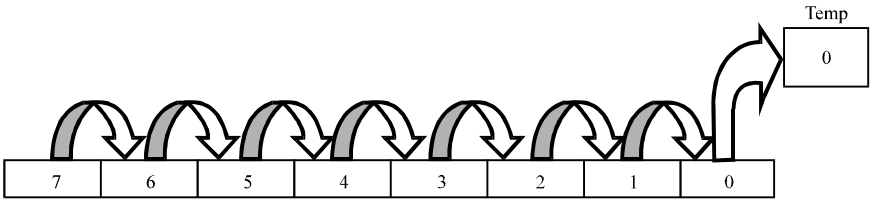

Fig. 3: Move the first bit into the Temp

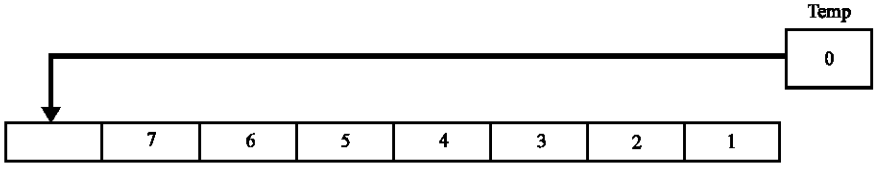

Fig. 4: Return the Temp value to Array

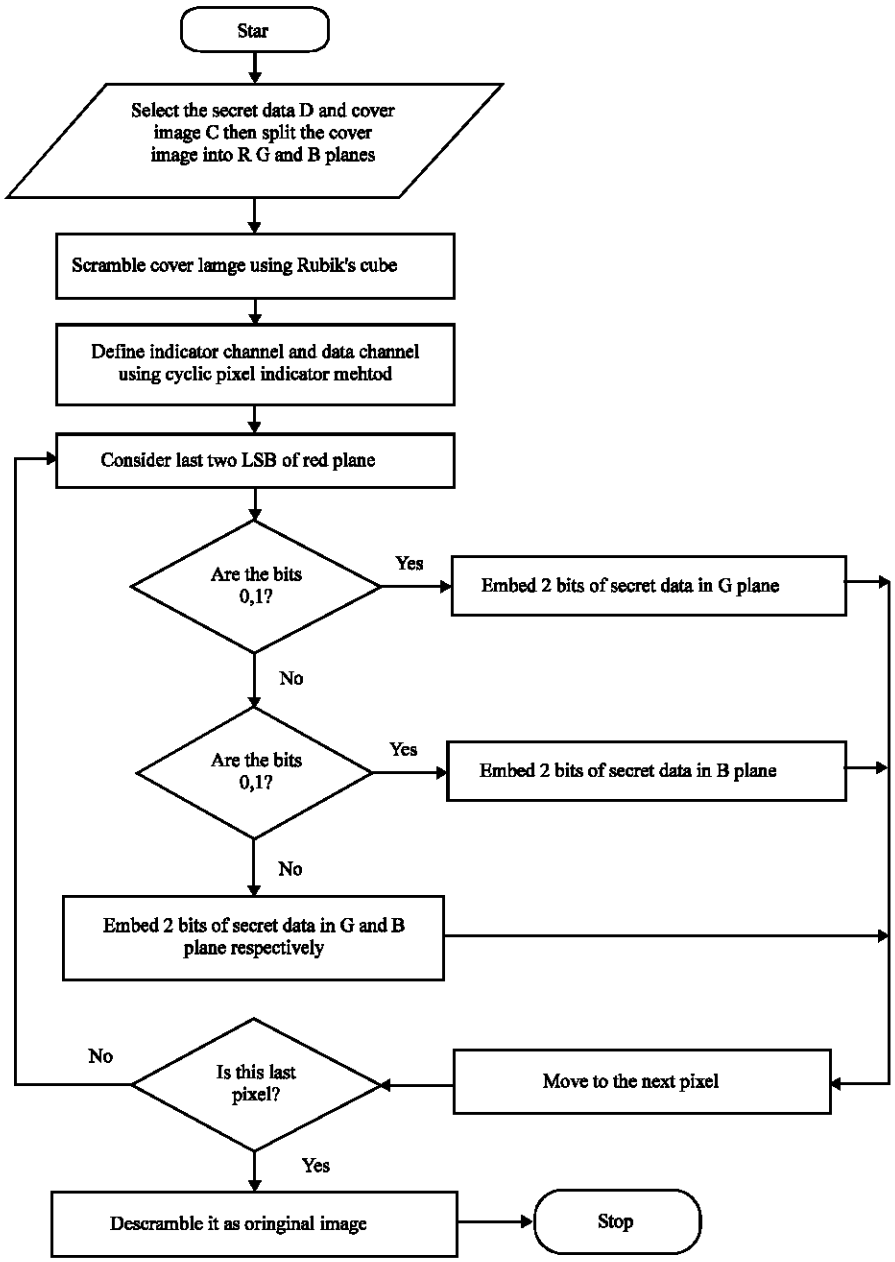

Fig. 5: Flow chart for embedding

The flow chart for embedding and extraction are given in Fig. 5 and 6, respectively. Here embedding and extraction process are explained in step by step manner.

RESULTS AND DISCUSSION

To justify the effectiveness of this study, the algorithm is simulated in MATLAB 7.1 with Lena, Baboon, Mahatma Gandhi and Temple as carrier images are depicted in Fig. 7a-10a with their corresponding stego images and accordingly their histograms are shown in Fig. 7b-10b. All images

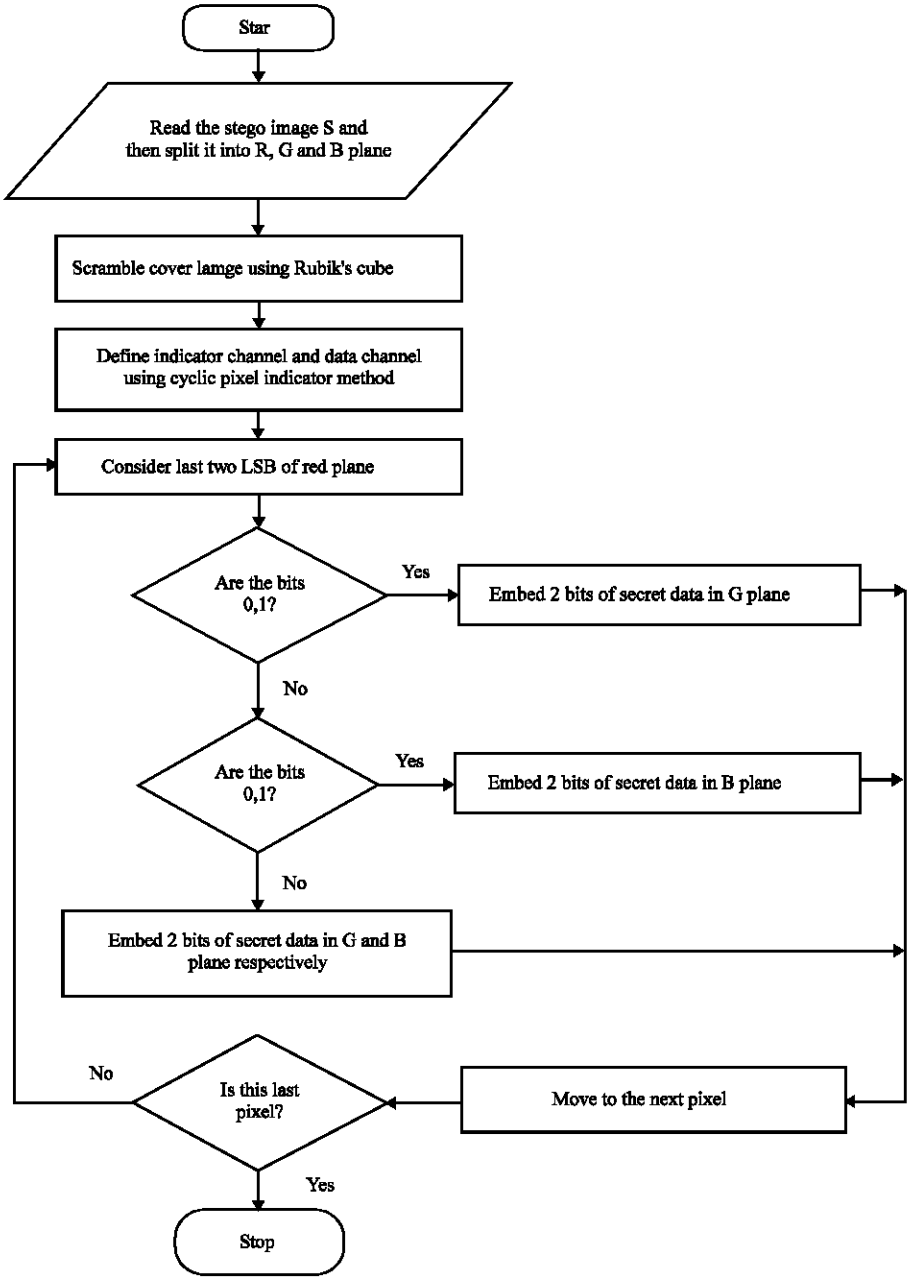

Fig. 6: Flow chart for extraction

are of dimension 256×256×3 and approximately 30-35 kb in size. Here, pixel indicator technique is exploited to appreciate the goodness of the algorithm with the liberality in choosing the indicator for each embedding.

Tabulation for comparative results of MSE, PSNR, BPP and total number of bits embedded are tabulated in Table 1.

Thus, by fixing indicator channel, and based on that 2 bits are embedded in every iteration in each plane. As per the size and dimension of the images, MSE and PSNR values are vary in each

Table 1: Comparative results of MSE, PSNR, BPP and total number of bits embedded

		Channel red		Channel green		Channel blue			
		----------		----------		----------		Bits	No of bits
Cover image	PI Methods	MSE	PSNR	MSE	PSNR	MSE	PSNR	per pixel	embedded
Lena	Proposed	0.4987	51.15	0.2594	53.9904	0.7033	49.6593	1.9958	130798
	Padmaa *et al.* (2011)	1.227	47.24	1.3641	46.782	1.02	48.045	2.114	138549
	Amirtharajan *et al.* (2010)	1.68	45.89	1.57	46.18	1.52	46.31	2.13	139592
	Amirtharajan *et al.* (2011)	1.2906	47.02	1.2374	47.2059	1.2049	47.3213	2.3139	151645
	Amirtharajan *et al.* (2012)	2.4387	44.26	2.3066	44.501	2.3389	44.441	3.9181	256776
Baboon	Proposed	0.4754	51.35	0.2587	54.0024	4.6733	41.4345	1.9858	130144
	Padmaa *et al.* (2011)	4.065	42.04	4.002	42.108	4.2847	41.812	3.657	239262
	Amirtharajan *et al.* (2010)	2.61	43.96	2.65	43.88	2.72	43.77	2.51	164496
	Amirtharajan *et al.* (2011)	46.21	1.5544	46.2151	1.5904	46.1157	2.3975	157121	
	Amirtharajan *et al.* (2012)	2.3702	44.39	2.3255	44.4657	2.3619	44.3981	3.9232	257108
Mahatma Gandhi	Proposed	0.4876	51.25	0.2558	54.0512	3.8500	42.2762	1.9822	131212
	Padmaa *et al.* (2011)	1.348	46.83	2.4212	47.025	1.2478	47.169	2.07	132945
	Amirtharajan *et al.* (2010)	1.34	46.83	1.30	47.07	1.24	47.15	3.0880	135660
	Amirtharajan *et al.* (2011)	42.98	3.2944	42.9530	3.1355	43.1677	2.07	202377	
	Amirtharajan *et al.* (2012)	2.5728	44.03	0.5798	44.2904	2.3595	44.4026	3.9184	256796
Temple	Proposed	0.4673	51.43	0.2569	54.0333	0.8289	48.9458	1.9921	130556
	Padmaa *et al.* (2011)	1.853	45.45	1.766	45.662	1.632	46.003	2.352	154409
	Amirtharajan *et al.* (2010)	1.85	45.45	1.76	45.66	1.63	46.00	2.30	150732
	Amirtharajan *et al.* (2011)	47.65	1.1062	47.6924	1.1240	47.6232	2.4659	161604	
	Amirtharajan *et al.* (2012)	2.3143	44.49	2.3095	44.4957	2.3764	44.3716	3.9240	257160

plane. If we take Lena image, Green plane has the highest PSNR of 53.9904 and minimum of 49.6593 in Blue plane. If all four images are likened, Temple plane offers relatively high PSNR in all of its 3 planes. Approximately, BPP witnessed in these images is found to be 0.6660 which is fairly straight for constant bit embedding. More or less 130677 bits are embedded in each plane which says about the efficiency of the algorithm.

In order to make the readers understand this libretto apart from analytical results, histograms and stego images are also portrayed. One can notice that covers and their corresponding stegos remain identical without giving a clue about secret sharing. As a result, they possess far above the ground imperceptibility which is what needed the most in a steganographic run. Moreover, encryption algorithm is designed by taking Rubik's cube fundamentals. This would create more complexity along with security as well.

This study is justified in terms of steganalysis also to prove the performance. One such attack is Chi-square which generally tests the competence of any algorithm by giving pictorial representation. Here, for performance analysis sake, Mahatma Gandhi image is exposed to the test and graphical results are obtained in Fig. 11.

The two curves represent cover and stego images. Before 50 rows the probability of embedding gradually minimizes to zero that clears the fact that the stego seems as if it contains no secret hidden in it. However, more care is taken in bringing up the obscurity, which is revealed in the graph given. In general, probability of 1 is when all rows undergo embedding and 0 if none.

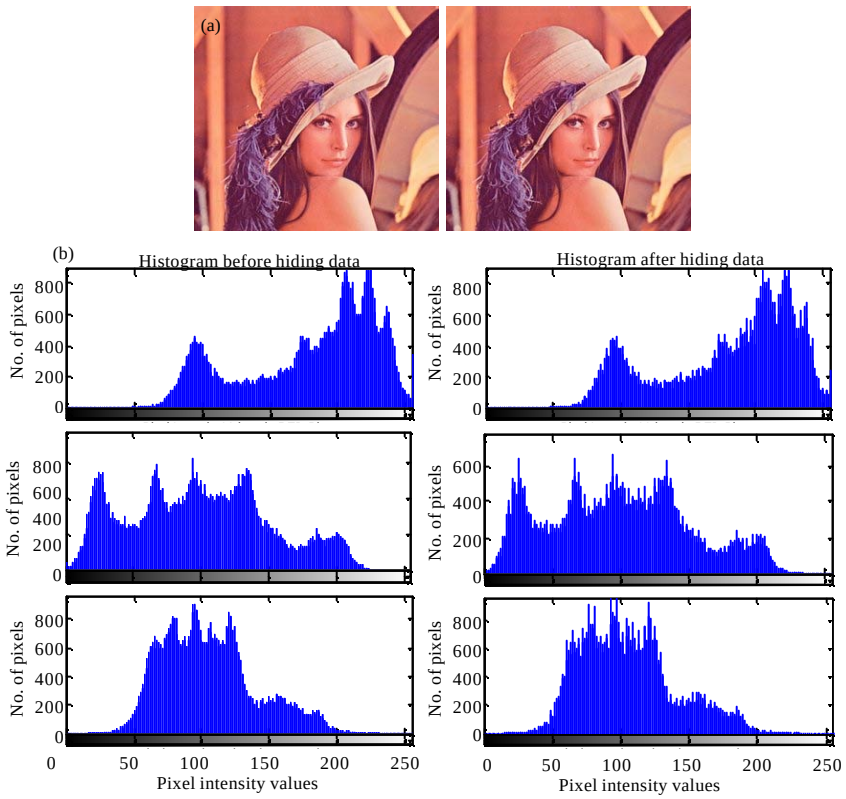

Fig. 7(a-b): (a) Lena cover image and its corresponding stego image and (b) Subsequent histograms for cover and stego images

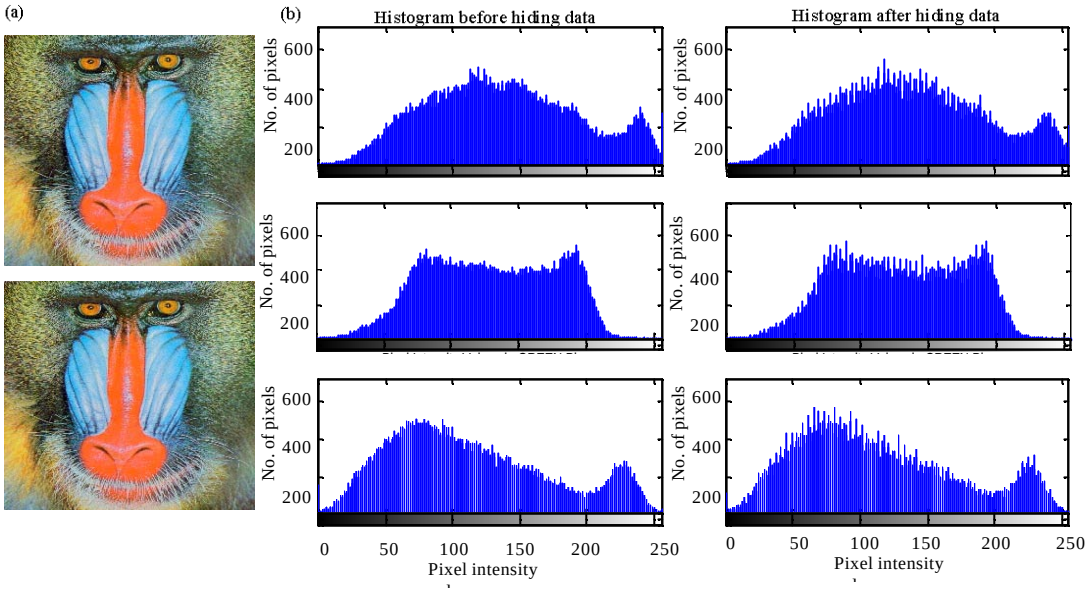

Fig. 8(a-b): (a) Baboon cover image and its corresponding stego image and (b) Subsequent histograms for cover and stego images

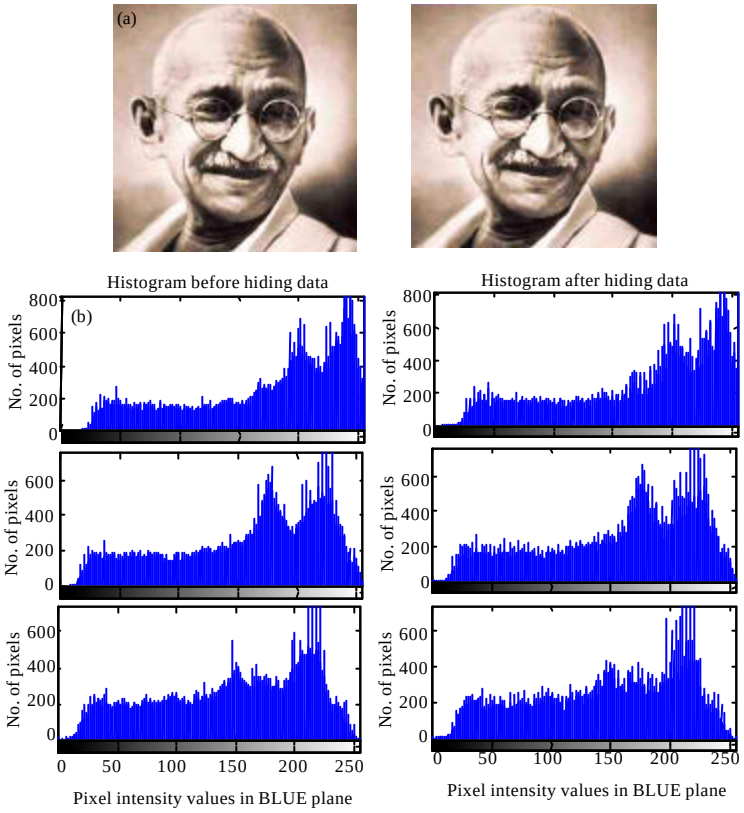

Fig. 9(a-b): (a) Mahatma Gandhi cover image and its corresponding stego image and (b) Subsequent histograms for cover and stego images

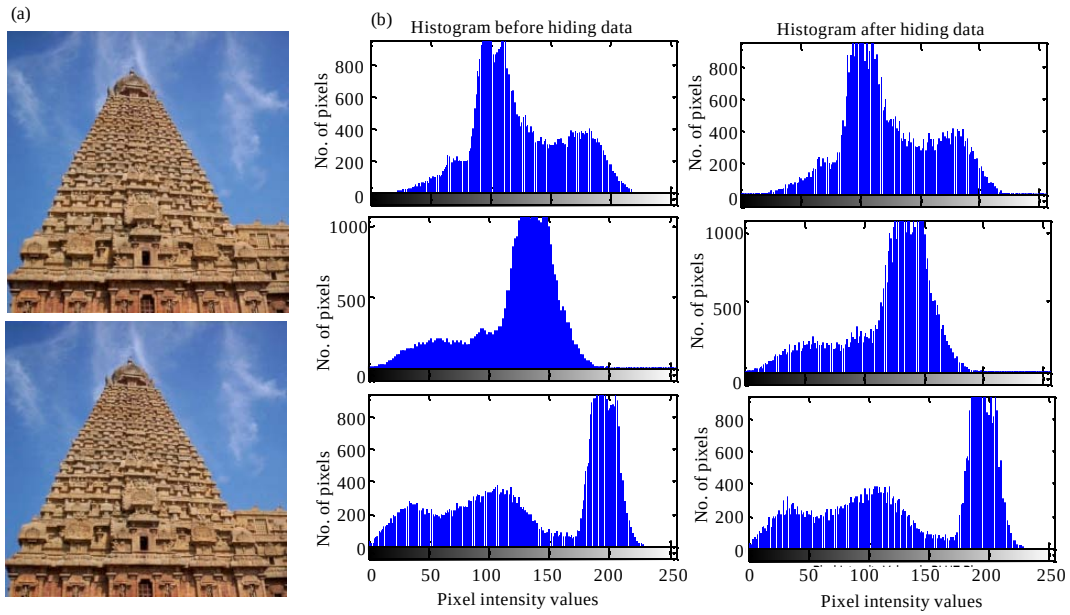

Fig. 10(a-b): (a) Temple cover image and its corresponding stego image and (b) Subsequent histograms for cover and stego images

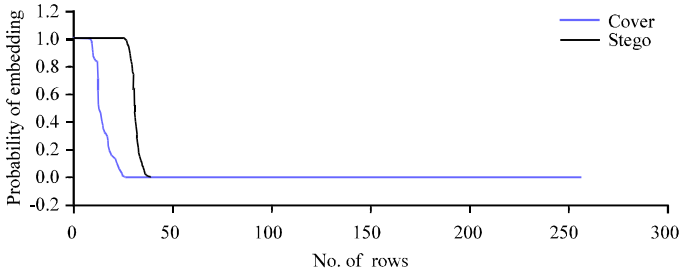

Fig. 11: Graphical results for Mahatma Gandhi against chi square test

CONCLUSION

Rubik's cube is a 3-D mishmash riddle, which has lent itself in discovering numerous theories and concepts in mathematics and engineering. This paper takes the idea of Rubik's cube and formulates it in an image steganographic scheme. Secret data undergoes manipulation on some grounds of cryptography and further follows steganographic principles to share the secret. The experimental values show that this is one benevolent model for hiding secret in images. It also has the possibility of practical realization apart from owning secrecy and anonymity. The study is also tested against Chi-square to give good reason for. Thus, this study proposes a beneficial steganographic method when equated with previously available ones.

REFERENCES

Abdulfetah, A.A., X. Sun, H. Yang and N. Mohammad, 2010. Robust adaptive image watermarking using visual models in DWT and DCT domain. Inform. Technol. J., 9: 460-466.

Al-Azawi, A.F. and M.A. Fadhil, 2010. Arabic text steganography using kashida extensions with huffman code. J. Applied Sci., 10: 436-439.

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

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

Amirtharajan, R., 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.

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

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

Cheddad, A., J. Condell, K. Curran and P.M. Kevitt, 2010. Digital image steganography: Survey and analysis of current methods. Signal Process., 90: 727-752.

Gutub, A.A.A., 2010. Pixel indicator technique for RGB image steganography. J. Emerging Technol. Web Intell., 2: 56-64.

Hmood, A.K., B.B. Zaidan, A.A. Zaidan and H.A. Jalab, 2010a. An overview on hiding information technique in images. J. Applied Sci., 10: 2094-2100.

Hmood, A.K., H.A. Jalab, Z.M. Kasirun, B.B. Zaidan and A.A. Zaidan, 2010b. On the Capacity and security of steganography approaches: An overview. J. Applied Sci., 10: 1825-1833.

Janakiraman, S., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012a. Firmware for data security: A review. Res. J. Inform. Technol., 4: 61-72.

Janakiraman, S., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012b. Pixel forefinger for gray in color: A layer by layer stego. Inform. Technol. J., 11: 9-19.

Loukhaoukha, K., J.Y. Chouinard and A. Berdai, 2012. A secure image encryption algorithm based on Rubik's cube principle. J. Electrical Comput. Eng., Vol. 2012. 10.1155/2012/173931

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.

Yen, E. and L.H. Lin, 2010. Rubik`s cube watermark technology for grayscale images. Expert Syst. Appl., 37: 4033-4039.

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.