Research Journal of Information Technology

ISSN 1815-7432

Academic Journals Inc.

www.academicjournals.com

Research Journal of Information Technology 5 (2): 87-99, 2013
ISSN 1815-7432 / DOI: 10.3923/rjit.2013.87.99

Pixel Indicated Triple Layer: A Way for Random Image Steganography

R. Amirtharajan, R. Subrahmanyam, Jasti Nithin Teja, Katkuri Mahendar Reddy and J.B.B. Rayappan
School of Electrical and Electronics Engineering, SASTRA University, India

Corresponding Author: R. Amirtharajan, School of Electrical and Electronics Engineering, SASTRA University, India

ABSTRACT

In this study, a secure mode of steganography is projected in which three main entities are exercised. They are Pseudo random generator, Least Significant Bit (LSB) substitution and Optimal Pixel Adjustment Process (OPAP). A popular cliché "All roads lead to Rome" says that there endure countless ways to attain a target. Likewise, this goes very well with Steganography than any other things. Digital epoch of steganography embraces numerous trials to surmount the universal hitch of concealment and refuge in every form of computer communication. This study reveals one more methodology for the same but with unique characteristics. Here, cyclic pixel indicator technique is used wherein two channels are used as data channels and the remaining channel is used as an indicator channel. Red plane is taken as the indicator channel for the first pixel for the subsequent pixels the indicator channels follows a periodic cycle of R, G, B. barring the indicator channel, the other two channels act as the data channels for the corresponding pixels. The pixel intensity determines the bits to be embedded. i.e., LSB's of the indicator channel. If the LSB's of indicator channel say R channel are 00 Embed 1 bit in G and 2 bits in B; in case of 01, embed 2 bits in G and B each. If LSB(R) is 10, 2 are inlayed in G and 3 bits in B. Finally id LSB(R) equals 11 and then 3 bits are ingrained in G and 3 bits in B. A novel 2-key based pseudo random generator is employed which is used to embed data completely in a unique random fashion based on user's choice. Thus, it introduces obscurity, while composite embedding of secret bits will result in additional intricacy. Therefore, this study is yet another practical cum unassailable means for secret sharing. Justification for this study is provided by the analytical results.

Key word: Data security, information hiding, random image steganography, pixel indicator

INTRODUCTION

Information communication through internet is in diverse forms and rivets variety of applications. This, indeed, requires various levels of concealment based on the applications' demand. The electronic transmission faces numerous problems like sham, copyright control, data security, etc. So, the desired information needs to be transmitted safely, first and should endure the attacks of intruders (Salem *et al*., 2011; Schneier, 2007; Stefan and Fabin, 2000). The refuge of such data transfer has been a chief apprehension and has become the study in limelight, probably, forever. The most universal means of doing so is to send the desired data in disguise so that the beneficiary only can avail it (Amirtharajan and Rayappan, 2012a-d). True, this led to the development of information hiding techniques and secret communication methods (Bender *et al*., 1996). The prime bases for the so called methods are cryptography and steganography

(Hmood *et al*., 2010a, b; Rajagopalan *et al*., 2012) and its counter attack called cryptanalysis and steganalysis (Qin *et al*., 2010). While the former (cryptography) deals with text or number alone, the latter (steganography) brings all digital media into play (Cheddad *et al*., 2010).

The place where mathematics and engineering meets is be called cryptography. It is one of the means by which a readable data or text is made unreadable (for the eavesdropper) by encrypting the readable data. A sender transforms an original text (plaintext) into a modified text (cipher text) by means of a cryptographic key using encryption (Schneier, 2007). The receiver performs the reverse operation to retrieve back the original message by decryption. So, a interloper cannot tamper the concealed information. The remarkable cryptosystem services are Confidentiality, legitimacy, Access Control, veracity and Non-repudiation (Schneier, 2007). A good encryption method should thrive for two fundamental attributes, viz., confusion and diffusion (Salem *et al*., 2011). Cryptanalysis is nothing but the attack performed on cipher text. Putting it simple it is the way to crack a cryptosystem. The attacks aim at acquiring key and they may be active or passive. Some of the known cryptographic attacks are Ciphertext Alone attack, Known Plaintext attack, Chosen Plaintext attack (Schneier, 2007).

Steganography exists from long past; some means in history were micro dots (Provos and Honeyman, 2003), invisible inks, shaved head tattoos, wax tablets etc (Kahn, 1983; Stefan and Fabin, 2000). In this day and age, digital images are brought into play as cover files devoid of any suspicion for the reason that their charisma is ubiquitously on the Internet (Cheddad *et al*., 2010; Hmood *et al*., 2010a, b; Gutub, 2010; Amirtharajan *et al*., 2012; Janakiraman *et al*., 2012a, b; Padmaa *et al*., 2011; Zaidan *et al*., 2010). Furthermore, designing steganography algorithms that are statistically unnoticeable and acquiescing a large capacity is the core aspiration of Steganography (Thenmozhi *et al*., 2012). Also, a steganography system is ideally safe if the statistics of the cover image and the stego image are one and the same (Thanikaiselvan *et al*., 2011a, b). For that reason, the embedding capacity is liable to be superior to the robustness (Amirtharajan *et al*., 2012). The former is nothing but the size pertaining to both cover file's size and one which contains secreted message.

As a result, countless novel embedding practices have been recommended so as to boost the imperceptibility and swell the capacity of steganography methods. Steganography carrier archives may be of the extension txt, mp3, gif, bmp, wav, jpeg etc. (Al-Azawi and Fadhil, 2010; Al-Frajat *et al*., 2010; Xiang *et al*., 2011; Zanganeh and Ibrahim, 2011; Zhu *et al*., 2011; Zhao and Luo, 2012). Of these jpeg is the universal image format for local convention and internet given that it affords large compression ratio and retain high image quality. Therefore, JPEG compressed images are the mainly apposite cover images used for steganography. Steganography in spatial domain (Luo *et al*., 2011; Mohammad *et al*., 2011) includes Least Significant Bit (LSB) (Chan and Cheng, 2004), Pixel Value Differencing (PVD) and Pixel Indicator (PI) (Janakiraman *et al*., 2012a; Padmaa *et al*., 2011) whereas frequency domain includes Discrete Cosine Transform DCT (Abdulfetah *et al*., 2010), Discrete Wavelet Transform DWT (Abdulfetah *et al*., 2010) and Integer Wavelet Transform IWT (Thanikaiselvan *et al*., 2011a; Amirtharajan and Rayappan, 2012d).

If we roll back, watermarking concept was used around 700 years ago in Italy in the Fabriano town. Watermarking is all about establishing distinctiveness of information to avert illicit use (Stefan and Fabin, 2000). The noteworthy aspects of watermark are that they are supposed to be undividable from the carrier, indiscernible and should stay entrenched even through

transformation (Abdulfetah *et al.*, 2010; Zeki *et al.*, 2011; Zhang *et al.*, 2006). Unlike Steganography, Watermarking has the additional perception of buoyancy against endeavours to confiscate the veiled data (Cheddad *et al.*, 2010).

The common terminologies employed in watermarking are visible and fragile watermarks, labelling and fingerprinting, embedded signatures, bit stream watermarking. Based on the keys, the watermarking techniques are categorized as secret and public. The general properties of robust watermarking schemes are redundancy, keys and imperceptibility as they are applicable to formatted text, image, audio, video 3D models etc. Popular applications of watermarking are to give ownership proof, data tracking, monitoring, fingerprinting etc. (Stefan and Fabin, 2000). Reviewing the available literature suggest to implement a random image steganography method to offer good payload without compromising imperceptibility.

The main goal of this study is to offer a substantive steganographic plot for communication of surreptitious messages through images. It entices most common traits of digital image steganography but constructs the plot very in a different and complex way so as to make steganalysis outrageous. Thus, this is one such method which is easy to realize but hard to attack.

PROPOSED METHOD

This study asserts a diverse pixel indicator technique for both variable capacity and randomization in the cover. Here, Cyclic pixel indicator technique is used wherein two channels were used as data channels and the remaining channel is used as an indicator channel. Red plane was taken as the indicator channel for the first pixel for the subsequent pixels the indicator channels follows a periodic cycle of R,G,B. barring the indicator channel, the other two channels act as the data channels for the corresponding pixels.

The bits needed for embedding is decided by the pixel intensity i.e., LSB's of the indicator channel. If the LSB's of indicator channel, say R channel were 00 Embed k bit in G and k+1 bits in B. Similarly, if LSB(R) is 01, then k+1 bits are embedded in G and k+1 bit in B. If LSB(R) is 10, k+1 bit were embedded in G and k+2 bits in B. Finally id LSB(R) equals 11, then k+2 bits were embedded in G and k+2 bits in B. A novel 2-key based pseudo random generator is employed which was used to embed data completely in a unique random fashion based on user's choice. The proposed methodology's block diagram is given in Fig. 1.

The conditions for embedding in data channels as per the two LSBS of indicator channel are given in Table 1.

ALGORITHM

The processes can be laid down to three block process, apart from the Optimal Pixel Adjustment process incorporated while embedding the data.

Table 1: No. of bits embedded

Last two bits of a pixel of indicator channel (R)	No. of bits embedded(G)	No. of bits embedded(B)
00	K bit	K+1 bits
01	K+1 bits	K+1 bits
10	K+1 bits	K+2 bits
11	K+2 bits	K+2 bits

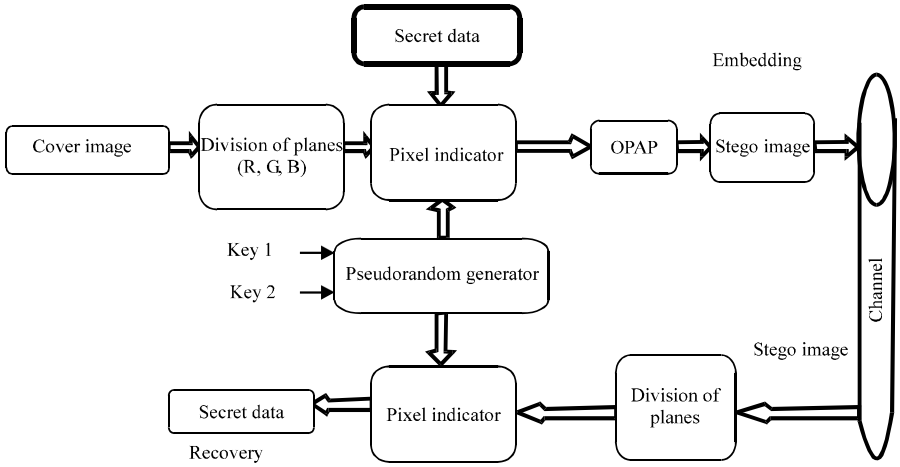

Fig. 1: Block diagram of proposed method

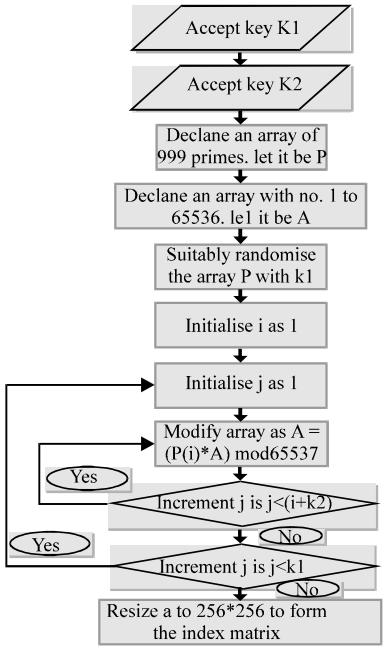

Fig. 2: Flow chart for pseudo random number generator

PSEUDO RANDOM GENERATOR

The sequence employs generation of random sequences which act as the index numbers creating a space filling curve. The curve's routing path is determined by a combination of user defined keys. Fig. 2 represents the flowchart for Pseudo Random Number Generator (PRNG) and Fig. 3 and 4 represent the flowchart for embedding and extraction.

Algorithm for PRNG:

- Accept keys k1 and k2
- Declare an array of 999 primes and let it be P
- Declare an array from 1 to 65536 and let it be A
- Randomize the array P with key k1
- Initialize i as 1
- Initialize j as 1
- Compute A=(P(j)×A)mod65537
- Increment j and check whether j is less than i+k2. If yes go to step 7. If no go to next step
- Increment I and check whether I is less than k1. If yes go to step 6. If no go to next step
- Resize A to index matrix of form 256×256

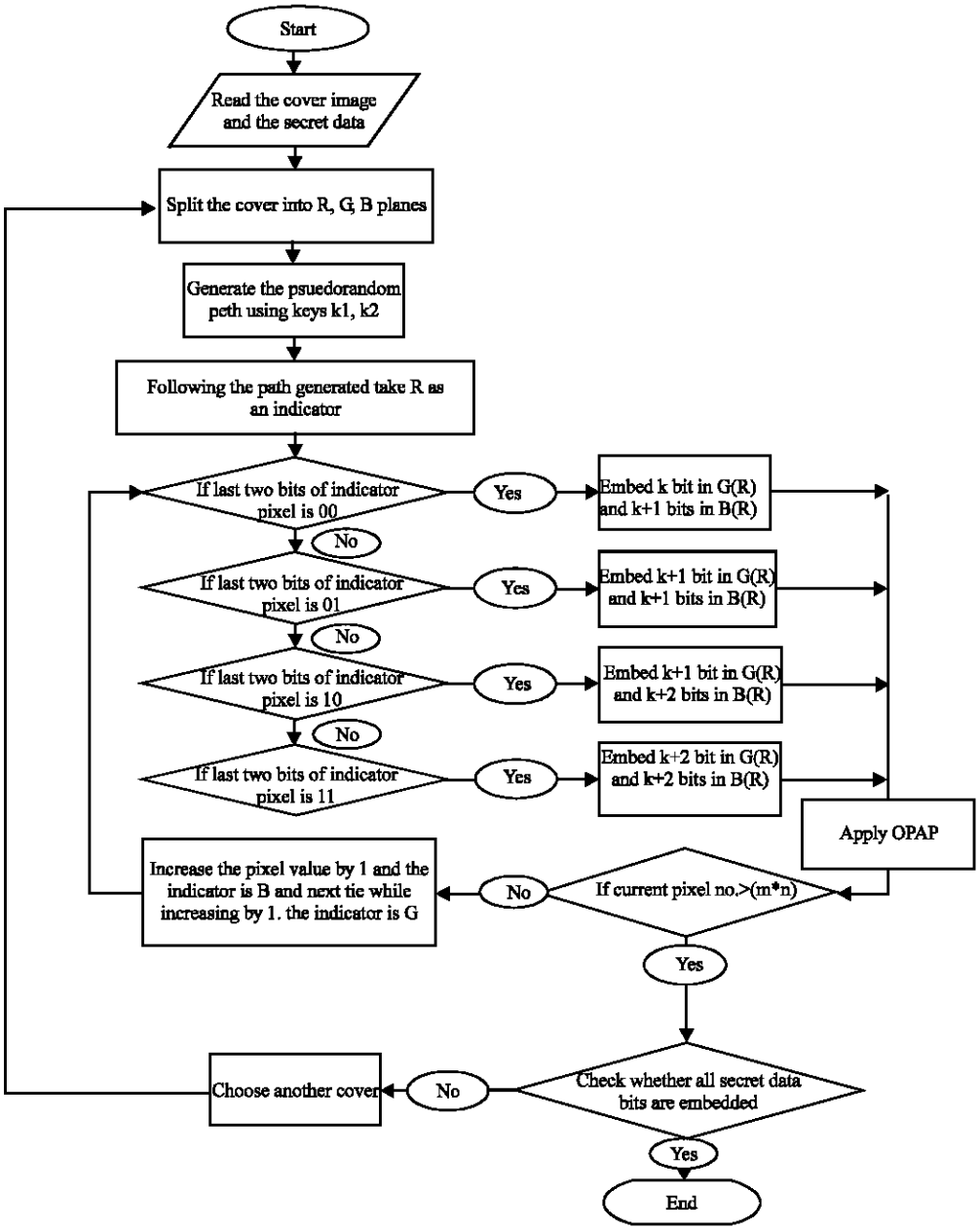

Fig. 3: Flowchart for embedding

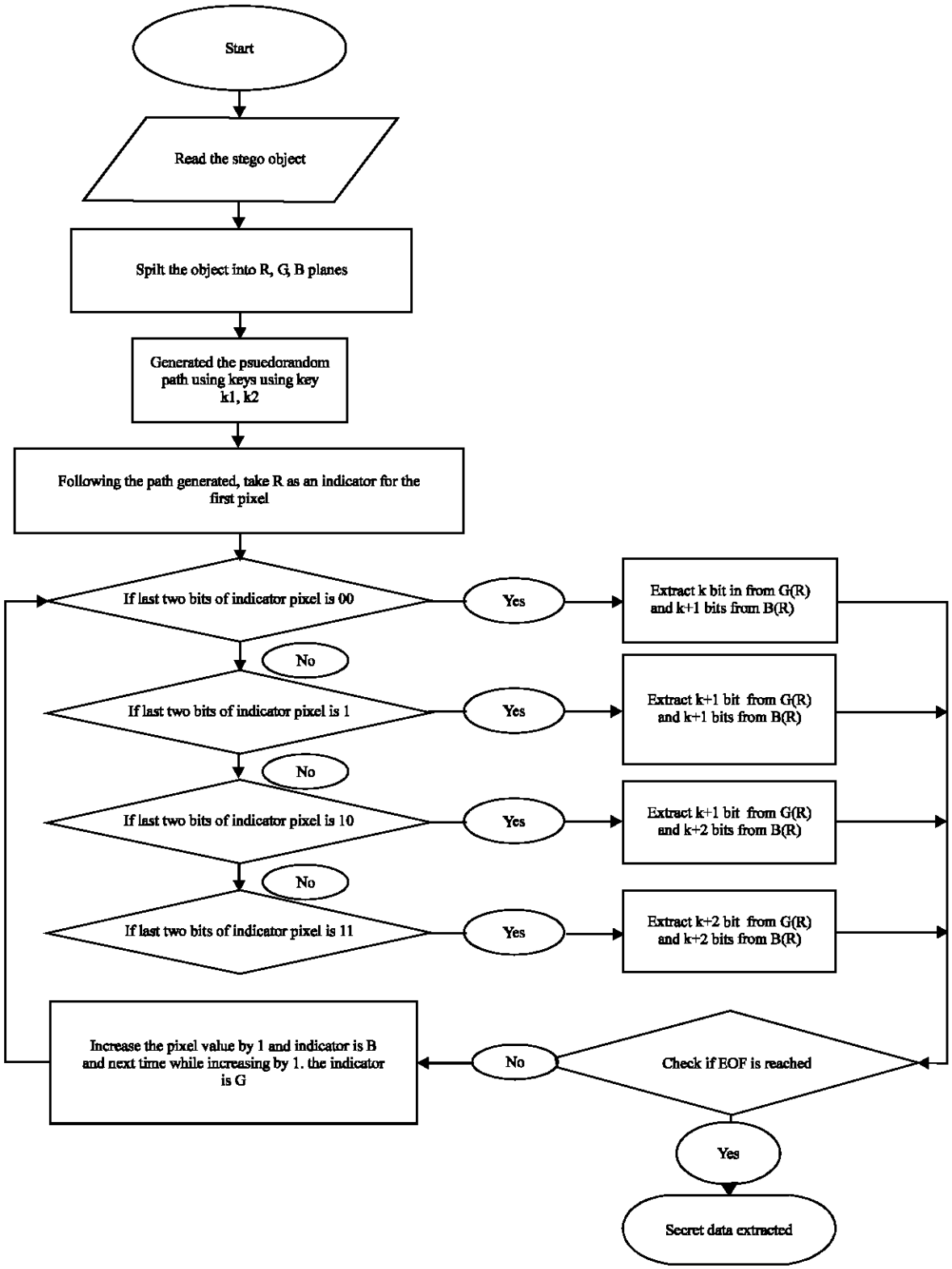

Fig. 4: Flowchart for extraction

EMBEDDING ALGORITHM

This process aims at embedding the secret data as follows.

1. Read the cover image and the secret data.
2. Split the cover image into red, green and blue planes.
3. Generate the pseudo random path using keys k1 and k2.
4. Follow the pseudo random path generated and for the first pixel (with respect to the generated path),the indicator is taken as red.
5. If the last two bit of the pixel indicator is 00, then embed k bit in green and k+1 bits in blue.
6. If the last two bit of the pixel indicator is 01, then embed k+1 bits in green and k+1 bits in blue.
7. If the last two bit of the pixel indicator is 10, then embed k+1 bits in green and k+2 bits in blue.
8. If the last two bit of the pixel indicator is 11, then embed k+2 bits in green and k+2 bits in blue.
9. Apply optimum pixel adjustment process after embedding.
10. Check whether the current pixel number is less than no. Of Rows × Columns. If yes, go to next step. Else check whether all data bits are entered. If yes go to end. If no print choose another cover.
11. Now go to the next pixel and take green as the pixel indicator. Instead of green embed in red. For the 3rd (next) pixel take blue as indicator and instead of blue embed in red. Follow the cycle by choosing red as indicator for next pixel
12. Go to step 5
13. End the program

EXTRACTION ALGORITHM

This algorithm retrieves the secret data from the image efficiently.

1. Start the program
2. Read the stego image
3. Split the image into red, green and blue planes
4. Generate the pseudo random path using keys k1 and k2
5. Follow the path generated and take red as an indicator for the first pixel
6. If the last two bits of the pixel indicator is 00, then extract k bit from green and k+1bits from blue
7. If the last two bits of the pixel indicator is 01, then extract k+1bits from green and k+1bits from blue
8. If the last two bits of the pixel indicator is 10, then extract k+1bits from green and k+2 bits from blue
9. If the last two bits of the pixel indicator is 11, then extract k+2 bits fromgreen and k+2 bits from blue
10. Check for the end of function of the secret data. If yes end the program. If no, go to next step
11. Now go to the next pixel and take green as the pixel indicator. Instead of green extract it from red. For the 3rd (next) pixel take blue as indicator and instead of blue extract if from red. Follow the cycle by choosing red as indicator for next pixel
12. Go to step 6
13. End the program

RESULTS AND DISCUSSION

The results had excelled as far imperceptibility and randomness was concerned. We considered images Temple, Baboon and Mentor of 256×256×3 pixels color image as cover image and its stego image. To prove the efficiency of the algorithm under any cover, 2 practical images had been used. Cover image of Temple and its stego output with histograms of the image are given in Fig. 5. Graphical results for comparison of MSE and embedding capacity of Temple image is given in Fig. 6. Similarly, the cover and stego images of Baboon and Mentor along with the histograms are shown in Fig. 7 and 8. Graphical results for comparison of MSE and embedding capacity of Mentor image is given in Fig. 9. An example of randomized image is depicted in Fig. 10. MSE and PSNR values of the images Temple, Baboon and Mentor are given in Table 2, 3 and 4, respectively.

It's evident from all tables 2 to 4, each cover and a plane have its own embedding capability. While LSBs of the indicator determines maximum embedding, intensity values decides the

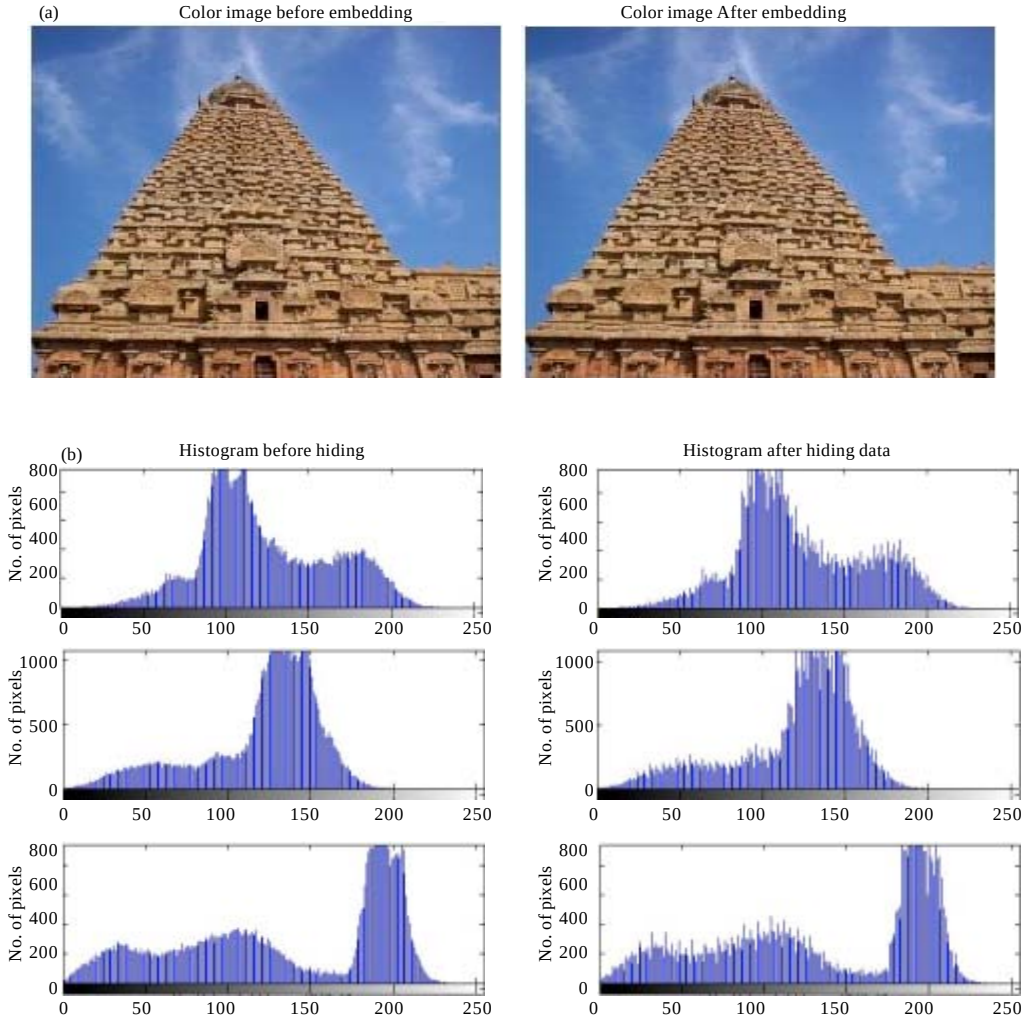

Fig. 5(a-b): (a) Cover and Stego images of temple (b) Histogram of temple image

Table 2: MSE and PSNR values for temple

Bits embedded	7.227	14454	21681	28908	36135
MSE					
Red	0.0978	0.1974	0.2962	0.3944	0.4919
Green	0.1255	0.2457	0.3710	0.4974	0.6243
Blue	0.1509	0.3029	0.4561	0.6076	0.7563
PSNR					
Red	58.2288	55.1767	53.4148	52.1709	51.2124
Green	57.1430	54.2273	52.4376	51.1640	50.1769
Blue	56.3440	53.3176	51.5400	50.2948	49.3438

counterpart. Various testing has been done for on these covers producing more than sufficient results and are presented in Fig 5 to 9, Cover, Stego and histogram of Temple, Baboon and Mentor respectively.

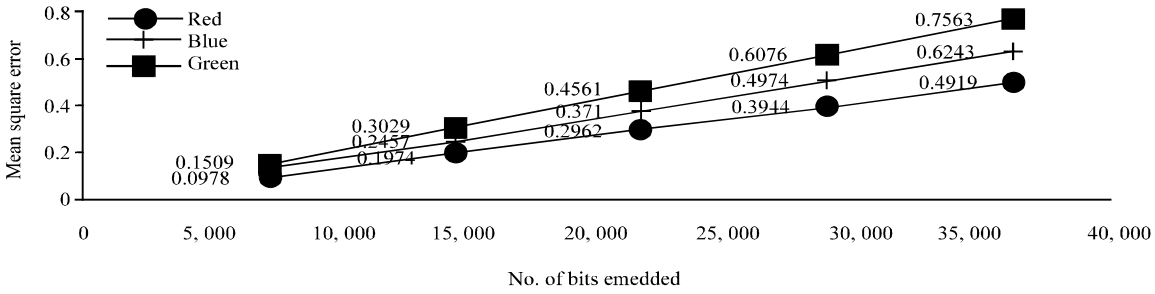

Fig. 6: MSE vs. number of bits for the temple cover image

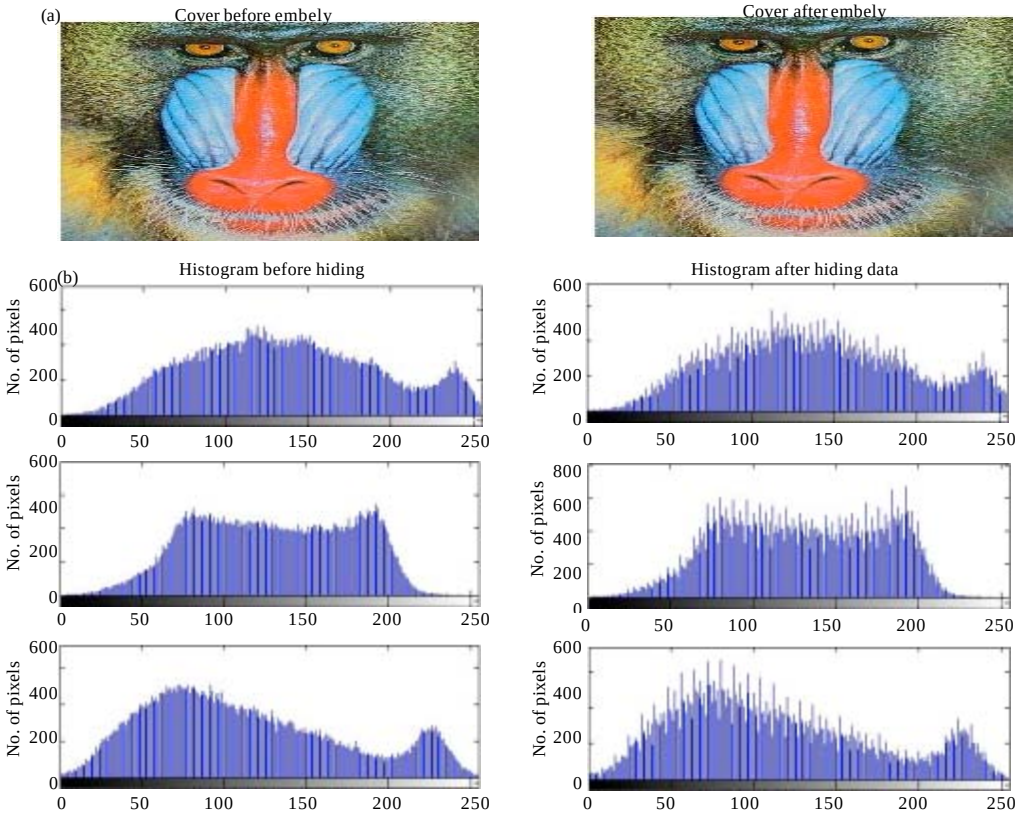

Fig. 7(a-b): (a) Cover and Stego images of Baboon (b) Histogram of Baboon image before and after hiding data

Table 3: MSE and PSNR values for baboon

Bits embedded	7.227	14454	21681	28908	36135
MSE					
Red	0.0985	0.1972	0.2965	0.388	0.4952
Green	0.1247	0.2493	0.3721	0.5016	0.6229
Blue	0.153	0.3043	0.46	0.6084	0.7655
PSNR					
Red	58.196	55.1813	53.4103	52.242	51.1831
Green	57.1711	54.1629	52.4247	51.127	50.1866
Blue	56.2837	53.298	51.5028	50.2888	49.2914

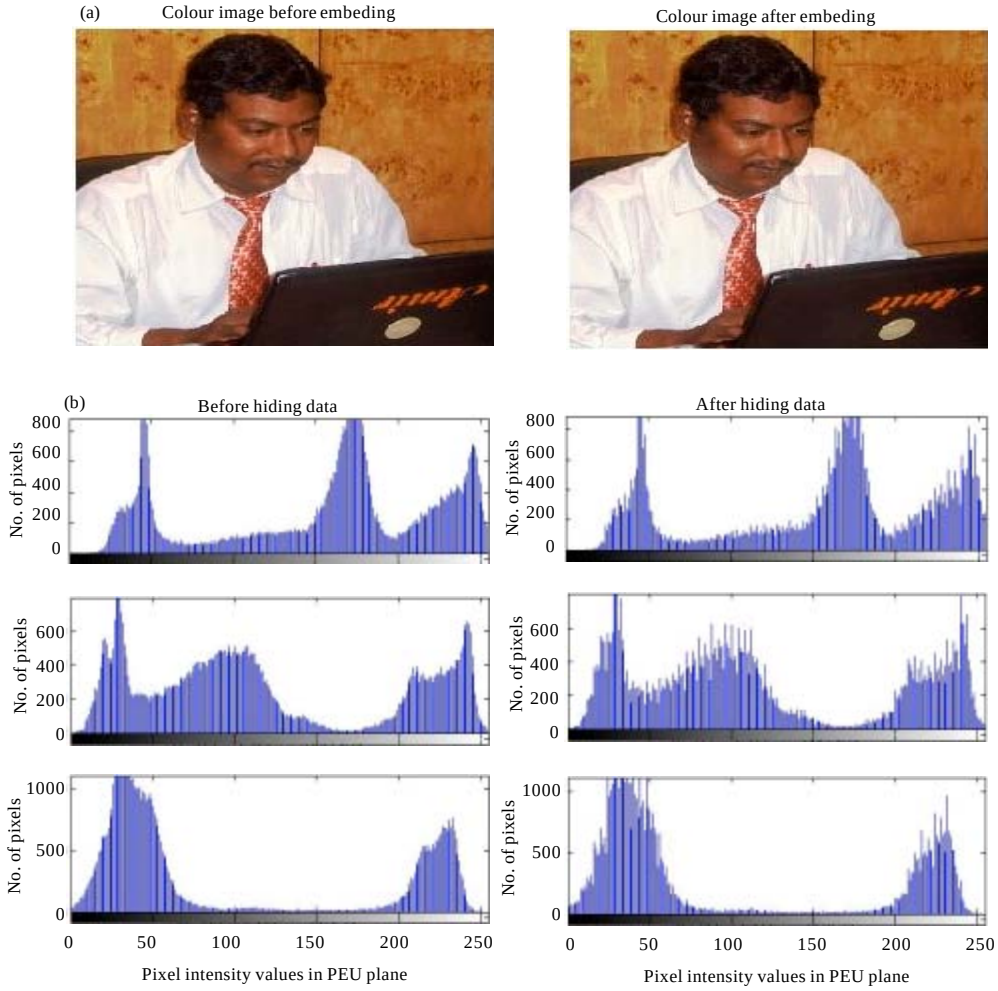

Fig. 8(a-b): (a) Cover and Stego images of Mentor (b) Histogram of Mentor image before and after hiding data

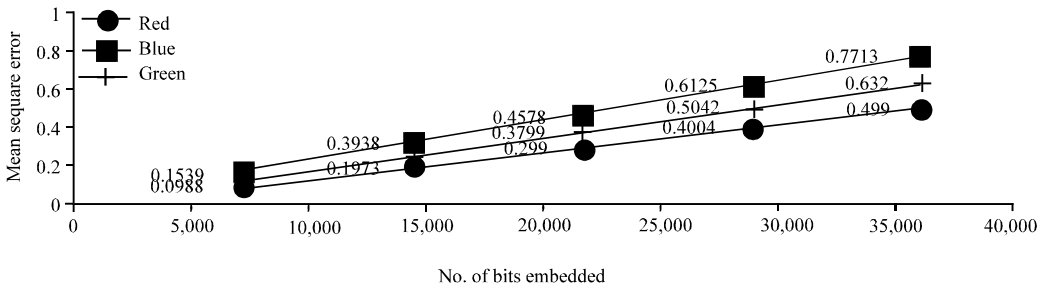

Fig. 9: MSE vs. Number of bits for the Mentor cover image

Also, the pseudo random method with the two key systems has shown very good strength with high randomness visible in Fig. 10. Since this routine has PSNR of 48dB and above it exhibits more than enough imperceptibility and capacity.

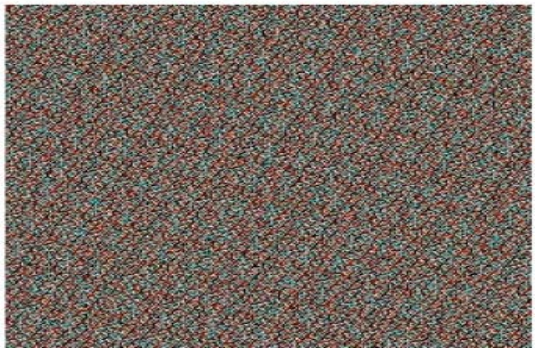

Fig. 10: Sample of randomized image for team.jpeg

Table 4: MSE and PSNR values for mentor.jpeg

Bits embedded	7.227	14454	21681	28908	36135
MSE					
Red	0.0983	0.1973	0.299	0.4004	0.499
Green	0.1252	0.2534	0.3799	0.5042	0.632
Blue	0.1528	0.3038	0.4578	0.6125	0.7713
PSNR					
Red	58.2056	55.1794	53.374	52.1057	51.1498
Green	57.1564	54.0925	52.3338	51.1049	50.1237
Blue	56.2895	53.3049	51.5244	50.26	49.2586

CONCLUSION

Inclusion of the randomization algorithms in no way have raised suspicion or compromised the imperceptibility of the image, setting up new benchmarks for stego system that aim to supersede the present algorithm. The results have also affirmed our conclusions. The one way pseudo random algorithm makes it difficult for any system to back track the entire algorithm even if routing pattern for any key is discovered.

LIMITATIONS AND FUTURE ENHANCEMENTS

The work has presented itself to be adept not just in imperceptibility but also at randomness. However, this is due to customization of the algorithm that is fixed to a particular dimension. The application of the algorithm to a generic image dimension is a daunting task. This is owing to the fact that the Strength of the pseudo random algorithm is dependent on prime numbers which make it foolproof. Building a generic algorithm requires higher computing specifications and takes up a lot of executing time.

The Future benchmarks that could outperform the algorithm could aim to accomplish a certain properties. Constructing an algorithm that could route data to suppress the Mean Square Error would not only do the job of rerouting the data in a random fashion but also act as complex stego tool. However, proposing such an algorithm could compromise over the security of the one way function against backtracking, making it a reversible function. Discovery of newer high capacity techniques could replace the model and when merged with the present algorithm could give even better results.

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, 2012e. 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.

Kahn, D., 1983. The Codebreakers: The Story of Secret Writing. Macmillan, New York.

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.

Provos, N. and P. Honeyman, 2003. Hide and seek: An introduction to steganography. IEEE Secur. Privacy, 1: 32-44.

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., P. Arulmozhivarman, R. Amirtharajan and J.B.B. Rayappan, 2011a. Wave (let) decide choosy pixel embedding for stego. Proceedings of the International Conference on Computer, Communication and Electrical Technology, March 18-19, 2011, India, pp: 157-162.

Thanikaiselvan, V., S. Kumar, N. Neelima and R. Amirtharajan, 2011b. 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.

Zhang, Y.H., B.S. Kang and X.F. Zhang, 2006. Image encryption algorithm based on chaotic sequence. Proceedings of the 16th International Conference on Artificial Reality and Telexistence-Workshops, November 29-December 1, 2006, Hangzhou, China, pp: 221-223.

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.