Research Journal of

Information Technology

ISSN 1815-7432

Academic Journals Inc.

www.academicjournals.com

Research Journal of Information Technology 4 (4): 220-227, 2012
ISSN 1815-7432 / DOI: 10.3923/rjit.2012.220.227

Graceful Graph For Graceful Security-Towards A Ste (G) Raph

[1]V. Thanikaiselvan, [1]P. Arulmozhivarman, [2]John Bosco Balaguru Rayappan and [2]Rengarajan Amirtharajan
[1]School of Electronics Engineering, VIT University, Vellore-632 014, Tamil Nadu, India
[2]School of EEE, SASTRA University, Thanjavur-613401, Tamil Nadu, India

Corresponding Author: V. Thanikaiselvan, School of Electronics Engineering, VIT University, Vellore-632 014, Tamil Nadu, India

ABSTRACT
The ubiquitous nature of computers with the rapid advent of technology has exponentially increased the need to secure the confidential information from misuse. Digital communications has led to the combination of both cryptography and steganography which were earlier used separately, to provide the optimum security. Steganography has the advantage of hiding the information in the cover in an invisible way such that the secret isn't visible to the naked eye. The proposed methodology implements image steganography using three keys for selecting the sub-band for embedding, selecting the order of the coefficients and deciding the number of bits to be embedded, respectively. Graph theory is made use of to select the order of the coefficients of the Integer Wavelet Transform. This present method offers good imperceptibility along with immaculate triple security with K1, K2 and K3.

Key words: Random image steganography, graph theory, integer wavelet transform, information hiding

INTRODUCTION
Man is generally obsessed with power and aims at attaining and maintaining the position of power which gives him control of everything else. With the world completely being digitized and all documents being generated digitally, power rests with the one who has the right information at the right time. Thus information has become very valuable and its protection from falling into wrong hands is the highest priority (Amirtharajan and Rayappan, 2012a-d).

Information hiding (Hmood *et al*., 2010a, b; Zaidan *et al*., 2010) is the collective term used for the various data security techniques which include Cryptography, Steganography and Watermarking (Stefan and Fabin, 2000). Cryptography is the technique of scrambling the secret message in such a way that it appears gibberish to anyone but the intended user (Schneier, 2007). While the encrypted message is visible to anyone, data hidden using steganography is invisible to the naked eye and aims at hiding the very existence of the message in a cover medium which could be image (Amirtharajan and Rayappan, 2012a-d; Chan and Cheng, 2004), text (Al-Azawi and Fadhil, 2010), audio (Zhu *et al*., 2011) or video files (Al-Frajat *et al*., 2010). Water-marking is used to implement copyright protection. The different characteristics like capacity, imperceptibility and robustness (Zanganeh and Ibrahim, 2011) are being analyzed for the various applications like secret communication, copyright protection and integrity check (Amirtharajan *et al*., 2011).

Image steganography is prevalent over the other steganographic techniques since the vital information is embedded in the image using different techniques making it imperceptible to the naked human eye (Amirtharajan and Balaguru, 2009, 2011; Amirtharajan *et al*., 2012; Cheddad *et al*., 2010; Kumar *et al*., 2011; Luo *et al*., 2008; Padmaa *et al*., 2011; Janakiraman *et al*., 2012a, b). The two main classifications include spatial domain steganography and transform domain (Thanikaiselvan *et al*., 2011a, b, 2012) steganography. The secret data is embedded directly in the image pixels in the former while it is embedded in the coefficients of the transform domain in the latter.

There are numerous review articles are available in steganography, each with unique features: for example, how to design random image steganography by Amirtharajan *et al*. (2012), how to implement secure stego systems in memory constrained devices by Janakiraman *et al*. (2012a,b), a detailed survey on digital image steganography by Cheddad *et al*. (2010) and Rajagopalan *et al*. (2012) discussed in detail about hardware implementations in FPGA. In addition how to combine stego in spread spectrum are available in study of Thenmozhi *et al*. (2012). The aforementioned reviews would explain in detail about steganography and its importance, strength and weakness and possible future directions and dimensions in information hiding.

So far there are good numbers of article in images steganography by adapting spatial and frequency domain but none would offer cryptic effect by adapting graph theory approach in IWT. Hence, this study offered a maiden effort to improve the security by carefully selecting the IWT coefficients and adaptively varying the number of bits to be embedded.

MATERIALS AND METHODS

Block diagram for the proposed methodology is shown in Fig. 1. Initially, the histogram modification (EI-Safy *et al*., 2009; Thanikaiselvan *et al*., 2011a, b, 2012; Amirtharajan and Rayappan, 2012c) has been adapted on the cover image to avoid overflow errors. Later, the cover image has been sub divided into 16×16 sub blocks. Then, apply Integer Wavelet Transform (IWT), to transform intensity variations into transformed coefficients. Here, Key 1, Key 2 and Key 3 would be used to select the sub bands, coefficient selection using graph theory and number of bits for data embedding, respectively.

Graceful graph for random path: Graph theory is basically the study of points and lines and analyzes the ways in which a set of Points called the Vertices (V) can be connected by lines or arcs called as the Edges (E). A graph is represented as G (V,E). In the Steganographic point of view, pixels or coefficients are considered as the Vertices while the traversal path between two pixels is the Edge. Graceful graphs play an important role for random traversing in steganographic algorithms.

Steps for generation of a graceful tree:

Step 1: p and q value will be selected based on the number of edges, i.e., p+q = Total number of edges
Step 2: Select a number (a), a∈{6, 7, 8, 9}
Step 3: Generate a sequence R1. R1 = {1+a.2+a,……………, p+a}
Step 4: Jumble the sequence R1 to get new sequence R2
Step 5: Generate a sequence R3 with Q number of elements:

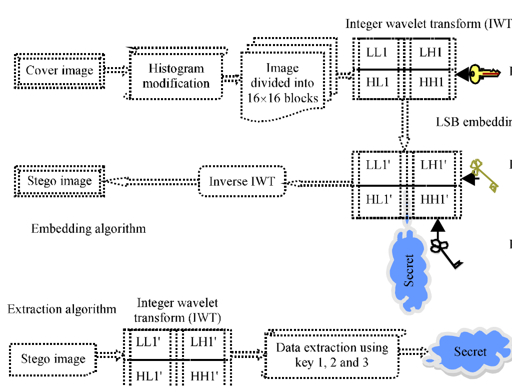

Fig. 1: Block diagram representation of the proposed method

- **Condition 1:** Sequence should be started with 9 and ended with 0, i.e., Descending order sequence
- **Condition 2:** Total number of elements in this sequence is q. Numbers of a number is taken by own

Step 6: Concatenate R2 and R3 and form a sequence S2
Step 7: Generate a sequence S1, where, S1 is {1, 2,……………, p+q}
Step 8: Adding the elements of S1 and S2 to form a new sequence
Step 9: Draw a graceful tree using the sequence S2 and (S1+S2)

Take the first element in the S2 and (S1+S2), Connect these elements and give label as 1.

Example:

Let p = 23, q = 40, a = 9 and p+q = 63
R1 = {10, 11……………… 31, 32}
R3 = {30, 19, 20, 10, 11, 13, 14, 32, 28, 23, 24, 12, 15, 18, 17, 16, 21, 31, 22, 29, 27, 25, 26}
R3 = {9^9, 8^4, 7^4, 6^5, 5^4, 4^1, 3^1, 2^5, 1^4, 0^3}, where, 8^4 represents 4 times of 8

The remaining steps are shown in Fig. 2.

Random path selection: Random path for steganography can be obtained from the Graceful Tree. Figure 3 shows graceful tree, Here Nodes are numbered from 0-63, Then Red coloured number (label) is given to all the edges represents the traversing path for embedding. Label 1 connects the node 30 and 31, Therefore data can embedded in the 30th and 31st pixel in the image. In this study, each Sub-band size is 8×8 which consists of 64 elements. We need to consider 64 pixels as 64 nodes. Numbering will be given as per raster scan procedure i.e., 0-63. Above generated tree is also consisting of 64 nodes and data will be embedded into the randomly selected pixels by tracing all the labels.

S1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
S2	30	19	20	10	11	13	14	32	28	30	24	12	15	18	17	16	21	31	22	29	27	25	26	9	9	9	9	9	9	9	9	9
S1+S2	31	21	23	14	16	19	24	40	37	33	35	24	28	32	32	32	38	49	41	49	27	47	49	33	34	35	36	37	38	39	40	41

33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
8	8	8	8	7	7	7	7	6	6	6	6	6	5	5	5	5	4	3	2	2	2	2	2	1	1	1	1	0	0	0	0
41	42	43	44	44	45	46	47	47	48	49	50	51	51	52	53	54	54	54	54	55	56	57	58	58	59	60	61	61	62	63	64

Fig. 2: Generation of sequence S1 and S2

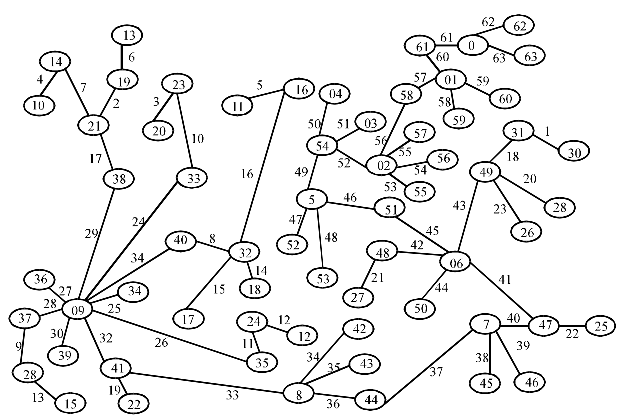

Fig. 3: Adapted graceful tree for the proposed method

Proposed methodology
Embedding algorithm

Step 1: Consider a 256×256 image as the cover image $C_{ij}\in\{0, 1, 2, 3,\ldots, 255\}$
Step 2: Generate the Secret Data in the form of a stream of binary data, $M_{ij}\in\{0,1\}$
Step 3: Convert the pixel values to the range of 15-240 in all the image to restrict the wavelet coefficients within the range of 0-255. $C'_{ij}\in\{15, 16, 17,\ldots 255\}$
Step 4: Convert the image into 16×16 sized non overlapping blocks, B_i; where, $1\le i\le 126$
Step 5: Apply integer wavelet transform to each of the 16×16 blocks (B_i). This will result (sub-bands) in Approximation ($LL1_{pq}$), Horizontal($LH1_{pq}$), Vertical ($HL1_{pq}$) and Diagonal ($HH1_{pq}$) coefficients. where, $1\le p$ and $q\le 8$
Step 6: Select the Sub-band using key-1 for embedding the data:

- Choose the order LH1, HL1 and HH1; if key-1 is 1
- Choose the order HL1, LH1 and HH1; if key-1 is 2
- Choose the order HH1, LH1 and HL1; if key-1 is 3

Step 7: Generate the key-2 using graph theory (graceful graphs) for random selection of coefficients to embed the secret data using above procedure
Step 8: Select key-3(K) for no of bits to be embedded using LSB embedding method (Amirtharajan and Rayappan, 2012c) in the selected co-efficient:

- K = 1, one bit embedding, k = 3, Three bits embedding
- K = 2, Two bits embedding, K = 4, Four bits embedding

Step 9: Repeat the steps 5-8 for all 16×16 blocks
Step 10: Apply Inverse Integer wavelet transform to each 16×16 block and produce the stego image $S'_{ij}\in\{0, 1, 2, 3,\ldots, 255\}$

Extraction algorithm:

Step 1: Receive 256×256 Stego image $S'_{ij}\in\{0, 1, 2, 3,\ldots, 255\}$
Step 2: Convert the image into 16×16 sized blocks, B'_i; where, $1\le i\le 126$
Step 3: Apply integer wavelet transform to each of the 16×16 blocks(B'_i). This will result (sub-bands) in Approximation ($LL1'_{pq}$), Horizontal ($LH1'_{pq}$), Vertical ($HL1'_{pq}$) and Diagonal ($HH1'_{pq}$) coefficients. where, $1\le p$ and $q\le 8$
Step 4: Use key-1 to find the sub band
Step 5: Use key-2 for random selection of coefficients
Step 6: Use key-3 for extraction of secret data from the selected co-efficient
Step 7: Repeat the above procedure for all the 16×16 sized blocks

Error metrics: Peak signal to noise ratio is used to evaluate the quality of the stego image which is defined as given below, for an M×N grayscale image:

$$PSNR = 10\times\log_{10}\frac{255\times 255\times M\times N}{\Sigma_{i=1}^{M}\ \Sigma_{i=1}^{N}(C_{i,j}-S'_{i,j})^2}$$

where, $C_{i,j}$ and $S'_{i,j}$ denote the cover image pixels and stego image pixels, respectively.

Table 1: MSE and PSNR values of the proposed method for K = 1 to 4

	K = 1 (49152 bits)		K = 2 (98304 bits)		K = 3 (147456 bits)		K = 4 (196608 bits)	
Image 256×256	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
Lena	0.5611	50.6404	1.7321	45.7450	6.9516	39.7100	30.7481	33.2526
Baboon	0.5683	50.5847	1.6822	45.8720	6.2254	40.1892	24.3811	34.2603
Koala	0.5659	50.6034	1.6931	45.8441	6.3114	40.1296	26.8922	33.8345
Temple	0.5661	50.6019	1.7610	45.6733	7.1179	39.6073	31.3079	33.1743
Tajmahal	0.5665	50.5991	1.7625	45.6695	6.8726	39.7596	29.6305	33.4134
Mahatma	0.5696	50.5751	1.7965	45.5865	7.3159	39.4881	31.6066	33.1330
Rangoli	0.5572	50.6705	1.6907	45.8501	6.3301	40.1167	26.6508	33.8737

RESULTS AND DISCUSSION

To measure the performance of our proposed method several experiments are performed. Seven gray scale images Lena, Baboon, koala, Temple Tajmahal, Mahatma and Rangoli are taken with size 256×256 as cover images and its corresponding stego images for k = 1 to 4 are available in Fig. 4-10. Our proposed method considers 16×16 blocks in the image which does not overlap each other; therefore, sub-band size is 8×8. A sequence of binary number is considered as secret data and they are embedded into the cover image. Using the proposed method the hiding capacity and PSNR for each image with various key-3(K) are tabulated in the Table 1.

Random embedding is achieved by using key-2. Several experiment with different values key-3 in constant embedding have been performed. For example, consider K = 1, then only one bit will be embedded in selected co-efficient. The results of proposed method are shown in Table 1 with embedding capacity and PSNR values for each method with different cover images. Changes due to LSB embedding in these methods are imperceptible to human vision except K = 4. The proposed method has overcome distortions resulted from embedding high-capacity secret data.

The results is shown in Fig. 4-10 represents the observed results, where 4a, 5a-10a are the selected cover images as input to the proposed methodology, Fig. 4b-10b are the corresponding stego images for K = 1, Fig. 4c-10c are the corresponding stego images for K = 2, Fig. 4d-10d are the corresponding stego images for K = 3 and finally Fig. 4e-10e are the corresponding stego images for K = 4, respectively. In all the cases the quality of stego images are good (PSNR is above 33 dB).

From Table 1 and Fig. 4-10, the following are observed and reported. Among all the cover images, baboon has the better image quality (34.26 dB), even for high capacity (196608 bits) is shown in Fig. 5e. The lower PSNR (33.13 dB) has been observed for mahatma as shown in Fig. 10e, Since, Mahatma cover image has more smooth areas than other cover images. Relatively, this cover image could not hide the fact of data hiding. Regardless of the PSNR values variation, all the stego images would escape visual attack, because the value of PSNR is above 33 dB for all the cases. The proposed method is compared with available literature (EI-Safy *et al*., 2009; Thanikaiselvan *et al*., 2011a, b, 2012; Amirtharajan and Rayappan, 2012c), this proposed method offers a comparable imperceptibility (above 33 dB) with reasonable hiding capacity (196608 bits for K = 4 in gray image) and robustness.

STEGANALYSIS

Steganalysis is the blind detection of a secret data in the Stego image (Qin *et al*., 2009, 2010; Xia *et al*., 2009). In this proposed method maximum PSNR is 50 dB and minimum PSNR is 34 dB which says that this is highly robust against Human visual Attack.

Here, embedding is done in the wavelet transform domain, so that secret data cannot be detected in the spatial domain. And the random traversing is used in each sub-band. Therefore, this is highly robust against Blind steganalysis technique. Numbers of iterations are needed to hack the information from this stego image:

$$\text{Total iteration} = (3!\times 4\times 3\times 8!)\times 256$$

Fig. 4(a-e): (a) Selected Lena cover and corresponding stego images for (b) K = 1, (c) K = 2, (d) K = 3 and (e) K = 4

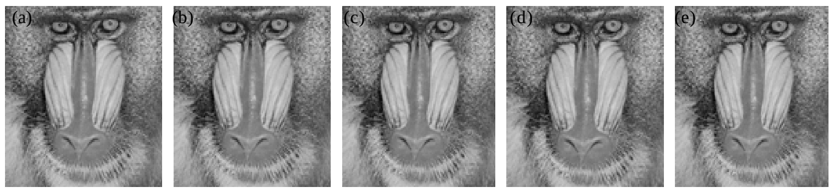

Fig. 5(a-e): (a) Selected baboon cover and corresponding stego images for (b) K = 1, (c) K = 2, (d) K = 3 and (e) K = 4

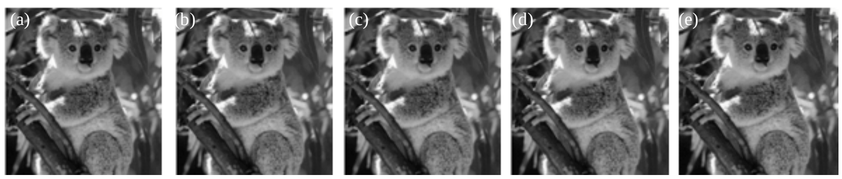

Fig. 6(a-e): (a) Selected koala cover and corresponding stego images for (b) K = 1, (c) K = 2, (d) K = 3 and (e) K = 4

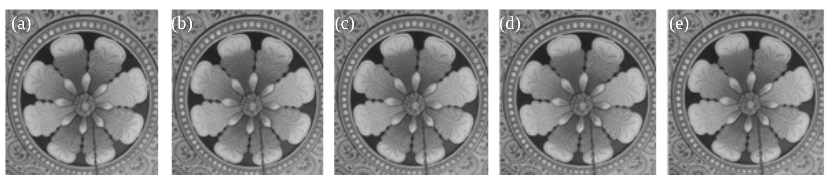

Fig. 7(a-e): (a) Selected rangoli cover and corresponding stego images for (b) K = 1, (c) K = 2, (d) K = 3 and (e) K = 4

Fig. 8(a-e): (a) Selected temple cover and corresponding stego images for (b) K = 1, (c) K = 2, (d) K = 3 and (e) K = 4

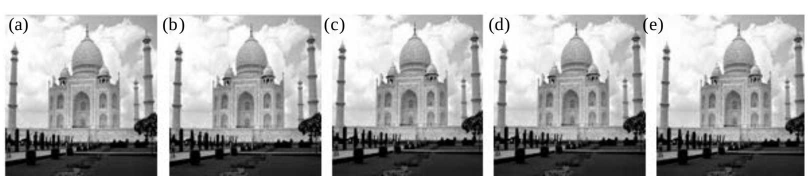

Fig. 9(a-e): (a) Selected tajmahal cover and corresponding stego images for (b) K = 1, (c) K = 2, (d) K = 3 and (e) K = 4

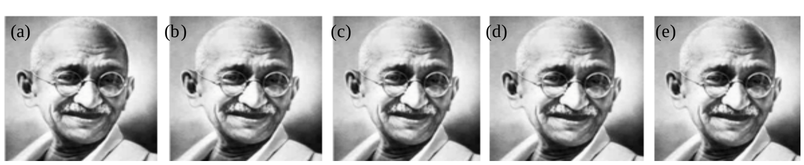

Fig. 10(a-e): (a) Selected mahatma cover and corresponding stego images for (b) K = 1, (c) K = 2, (d) K = 3 and (e) K = 4 where, First 3 factorial inform as which sub-band to be selected first. Then next 4 represent the Key-3, Furthermore (3×8!) represents 3 times of random traversing, Finally 256 represents, total number of 16×16 blocks.

CONCLUSION

The following three objectives must be considered for steganography, initially high payload; second one is imperceptibility and third one is robustness. The Proposed method provides high capacity with small error because of key-3, Here key-3 is directionally proportional to a payload. Embedding is done in the transform domain and it gives good imperceptibility. By referring the Table 1, proposed method embeds 196608 bits with 34 dB. High robustness is achieved through wavelet transform, key-1 and key-2. Finally, this method provides triple security. Thus, various wavelets can be used to get good imperceptibility and Adaptive embedding method can be used to improve the data hiding capacity.

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. and R.J.B. Balaguru, 2009. Tri-layer stego for enhanced security-a keyless random approach. Proceedings of the IEEE International Conference on Internet Multimedia Services Architecture and Applications, December 9-11, 2009, Bangalore, India, pp: 1-6.

Amirtharajan, R. and R.J.B. Balaguru, 2011. Covered CDMA multi-user writing on spatially divided image. Proceedings of the Wireless ViTAE Conference, February 28-March 3, 2011, IEEE, Chennai, India, pp: 1-5.

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 2011 IEEE 5th International Conference on Internet Multimedia Systems Architecture and Application (IMSAA), December 12-14, 2011, Bangalore, Karnataka, India.

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.

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.

EI-Safy, R.O., H.H. Zayed and A. EI-Dessouki, 2009. An adaptive steganographic technique based on integer wavelet transform. Proceedings of the International Conference on Networking and Media Convergence, March 24-25, 2009, Cairo, pp: 111-117.

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.

Kumar, P.P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2011. Steg-OFDM blend for highly secure multi-user communication. Proceedings of the 2nd International Conference on Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology, February 28-March 3, 2011, IEEE, Chennai, India, pp: 1-5.

Luo, G., X. Sun and L. Xiang, 2008. Multi-blogs steganographic algorithm based on directed hamiltonian path selection. Inform. Technol. J., 7: 450-457.

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. Sun, X. Xiang and Z. Xia, 2009. Steganalysis based on difference statistics for LSB matching steganography. Inform. Technol. J., 8: 1281-1286.

Qin, J., X. Xiang and M.X. Wang, 2010. A review on detection of LSB matching steganography. Inform. Technol. J., 9: 1725-1738.

Rajagopalan, S., R. Amirtharajan, H.N. Upadhyay and J.B.B. Rayappan, 2012. Survey and analysis of hardware cryptographic and steganographic systems on FPGA. J. Applied Sci., 12: 201-210.

Schneier, B., 2007. Applied Cryptography: Protocols, Algorithm and Source Code in C. 2nd Edn., 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.

Thanikaiselvan, V., P. Arulmozhivarman, A. Rengarajan and J.B.B. Rayappan, 2012. Authenticated wireless image sensor secret network: Graph guided steganography. Proceedings of the International Conference on Advances in Engineering, Science and Management, March 30-31, 2012, Nagapattinam, Tamil Nadu, India, pp: 279-284.

Thenmozhi, K., P. Praveenkumar, R. Amirtharajan, V. Prithiviraj, R. Varadarajan and J.B.B. Rayappan, 2012. OFDM+CDMA+Stego = Secure Communication: A Review. Res. J. Inform. Technol., 4: 31-46.

Xia, Z., X. Sun, J. Qin and C. Niu, 2009. Feature selection for image steganalysis using hybrid genetic algorithm. Inform. Technol. J., 8: 811-820.

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.

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.