Research Journal of Information Technology

ISSN 1815-7432

Academic Journals Inc.

www.academicjournals.com

Research Journal of Information Technology 6 (3): 188-197, 2014
ISSN 1815-7432 / DOI: 10.3923/rjit.2014.188.197

Space Filling Curve for Data Filling: An Embedded Security Approach

Siva Janakiraman, K. Thenmozhi, Sundararaman Rajagopalan, Har Narayan Upadhyay, John Bosco Balaguru Rayappan and Rengarajan Amirtharajan

Department of Electronics and Communication Engineering, School of Electrical and Electronics Engineering, SASTRA University, Tamil Nadu, 613401, Thanjavur, India

Corresponding Author: Siva Janakiraman, Department of Electronics and Communication Engineering, School of Electrical and Electronics Engineering, SASTRA University, Tamil Nadu, 613401, Thanjavur, India

ABSTRACT

Embedded devices have taken a prominent role in today's data communication. Steganography, an ancient method has immense budding to shield electronic data from threats in the modern world. The focus on this study is to make use of Hilbert Space Filling Curve (SFC) to implement random steganography on a single chip embedded device that embeds textual information on grey scale images. The written embedded C program was optimized for in terms of code size and execution time and the results are compared. The results of the proposed method are also compared with a similar methodology hosted on an equivalent embedded device. The main aim of this implementation is to make use of the specialized bit operation capabilities of ARM processor to improve the security level of the embedding algorithm by introducing bit level arbitrariness in the selection of data to be embedded.

Key words: Random image steganography, information hiding, hardware steganography, embedded device

INTRODUCTION

Information security has been in the foreground ever since the parturition of communication. Steganography, an antique method in the modern era shelters the electronic data during its journey between the targets (Amirtharajan *et al*., 2012; Amirtharajan and Rayappan, 2013; Cheddad *et al*., 2010). Hiding of information by itself requires great skill. Greater is the skill needed to protect it from the eagle eyes of eavesdroppers. People who master the art of steganography have found numerous ways (Amirtharajan *et al*., 2013c, g; Wu and Tsai, 2003; Luo *et al*., 2011; Mohammad *et al*., 2011; Thanikaiselvan *et al*., 2012a-c, 2013a, b; Thien and Lin, 2003) to cleverly elude these listeners and continue to protect their information. This technique is broadly classified in domains such as spatial, transform (Amirtharajan and Rayappan, 2012c; Praveenkumar *et al*., 2012a, 2014a-i; Qi and Wong, 2005; Wong *et al*., 2007; Zhang and Wang, 2004) and spread spectrum (Praveenkumar *et al*., 2012b, 2013a, b, 2014j; Thenmozhi *et al*., 2012).

Change in LSB position on any data does not produce perceivable changes to the original information. This fact is made use of in LSB steganography, where, the LSB is replaced with the

bit(s) of a secret message (Janakiraman *et al.*, 2014a). Various random embedding methods have been proposed by several steganography experts till now (Amirtharajan and Rayappan, 2012a; Amirtharajan and Rayappan, 2013; Amirtharajan *et al.*, 2013a, b, d, f, h, i, j). The degree of randomization can be thought of to be directly proportional to the level of security a system provides. Variable data size embedding techniques such as pixel indicator raises the security level at the cost of low payload compared to its equivalent fixed embedding techniques with greater K value (Amirtharajan *et al.*, 2013e; Janakiraman *et al.*, 2012a).

Space Filling Curves (SFC) often plays a role in block based algorithms for the purpose of random traversal (Rajagopalan and Upadhyay, 2011; Rajagopalan *et al.*, 2014a, d) within the cover block (Amirtharajan and Rayappan, 2012d; Zhao and Luo, 2012). These algorithms concentrate only on the way to randomize the place of embedding and still leave the procedure for aligning the extracted data to be chronological. The use of programmable hardware such as, microcontrollers, embedded processors and reconfigurable systems to gain data security through cryptography have been in practice for a long time (Salem *et al.*, 2011; Janakiraman *et al.*, 2012b, 2014b; Rajagopalan *et al.*, 2012a, b). The steganographic hardware systems started gaining its place in the world of data security in recent days through FPGAs (Janakiraman *et al.*, 2013; Ramalingam *et al.*, 2014a, b; Rajagopalan *et al.*, 2014b, c) and embedded devices (Stanescu *et al.*, 2009).

The implementation of image steganography on embedded devices such as microcontrollers with ARM7 architecture is obtainable in the literature. The use RGB images as cover, demands interfacing of external memory devices like SRAM for storage of image data. Random image steganography algorithm using grey scale cover images on suitable embedded devices with sufficient on-chip RAM, makes it possible to eliminate the need of external memory (Rajagopalan *et al.*, 2012b).

As the Einstein's words go, "Make things as simple as possible but not simpler". This study organised as follows, after knowing the existing literature, this study provides a simple yet an ingenious way to hide information. The next section of this study intend to make use of Hilbert Space Filling Curve (SFC) to present a three way randomization approach on data embedding sequence to advance the algorithm intricacy and data protection. The algorithm was implemented and tested on LPC2148 microcontroller with ARM7 core to attain the results. The performance metrics of the proposed algorithm on selected hardware with respect to code size and execution time are compared with implementation results of quad block algorithm (Rajagopalan *et al.*, 2012b).

PROPOSED METHODOLOGY

This LSB algorithm (Chan and Cheng, 2004) employs an 8×8 Hilbert curve (Amirtharajan and Rayappan, 2012b, d) as shown in Fig. 1 available in the form of Look-up Table (LUT) accessible from on-chip code memory to facilitate randomness in image steganography. The size of the cover image can be any number of 8×8 blocks with 8-bit grey pixels. In every 8×8 cover block, the 8×8 Hilbert curve dictates the order of pixel selection for data embedding. On considering one bit embedding, the number of secret bytes for full embedding will be 1/8 of the number of cover pixels. This makes the number of secret bytes for every block as 8, when K = 1. At every embedding point within the block, the random number

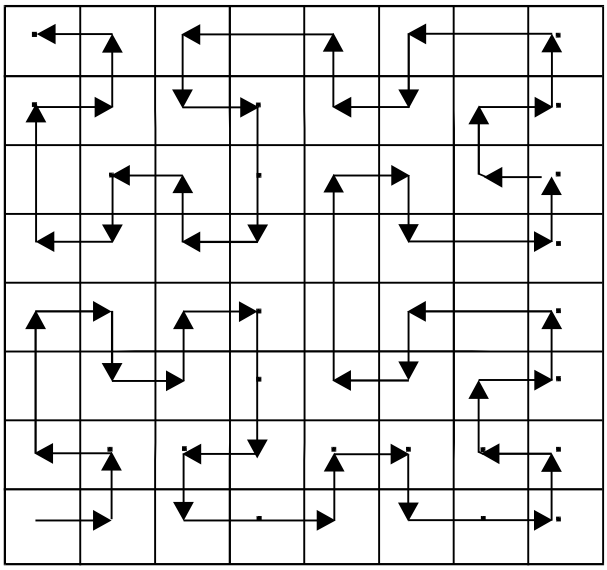

Fig. 1: Hilbert space filling curve (8×8)

obtained from LUT is divided by 8. The Quotient (Q) and Reminder (R) results in a single digit octal value (0-7). This selects the byte and bit positions, respectively in the secret data block corresponding to the cover block.

The embedding procedure given for a single 8×8 block may be continued for any image size with multiple 8×8 blocks. For multi bit embedding with K>1, the number of secret bytes corresponding to each cover block is given by K×8. On multi bit embedding, the byte and bit position of the secret data byte is given by Q+(i×8) and, R, respectively, where, 'i' is referred to as the bit position of the cover pixel in which the secret data bit gets embedded. In the case of embedding, the Hilbert LUT is used to identify the cover pixel and secret data bit to be embedded. During the process of retrieval the Hilbert LUT is used to align the extracted secret data bit of every stego pixel in apposite position so as to get back the original unseen information.

Pseudo code for embedding (K = 1):

```
8×8 cover_ blocks 2 embd = Cover_size/64
while (8×8 cover_ blocks 2 embd! = 0)
{
for (each pixel 't' in 8×8 cover block)
      {
      Cover_byte_pos = Hilbert LUT[t]
      secret_byte_pos = Cover_byte_pos/8
      secret_bit_pos = Cover_byte_pos% 8
Bit 2 embd = Extract_info_bit (secret_byte_pos,
                  secret_bit_pos)
LSB_Embed (Cover_byte_pos, Bit 2 embd)
          } 8×8 cover_ blocks 2 embd--
}
```

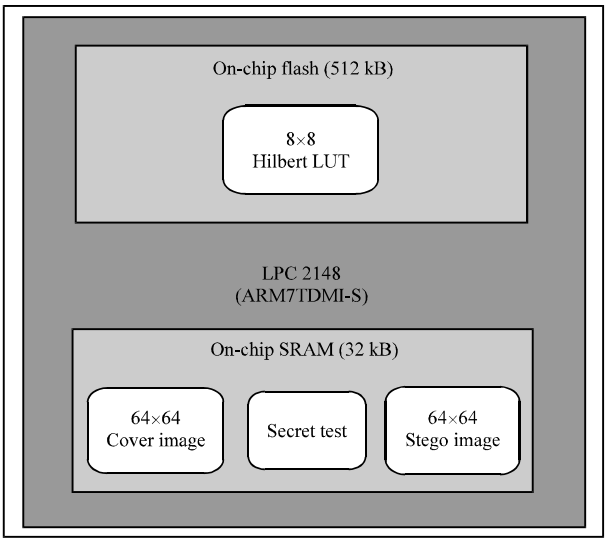

Fig. 2: Basic block diagram of stego implementation on LPC2148

Pseudo code for Retrieval (K = 1):

```
8×8 cover_ blocks 2 extract = Cover_size/64
while (8×8 cover_ blocks 2 extract! = 0)
{
for (each pixel 't' in 8×8 cover block)
        {
        Cover_byte_pos = Hilbert LUT[t]
        secret_byte_pos = Cover_byte_pos/8
        secret_bit_pos = Cover_byte_pos% 8
        secret_bit =
        Extract_info_bit (Cover_byte_pos)
Frame_info_byte (secret_byte_pos,
        secret_bit_pos, secret_bit)
        }
8×8 cover_ blocks 2 embd--
}
```

The existing on-chip data memory of 32 kB is highly sufficient to accommodate the maximum requirement of on-chip SRAM which comes to a value of less than 9 kB. This includes the space to store cover and stego images of 4 kB each in addition to 1536 bytes of secret textual information with maximum embedded bits per pixel (K = 3). Figure 2 shows the basic block diagram of the embedded device (LPC2148) with program and data memory contents used for embedding algorithm.

RESULTS AND DISCUSSION

The grey scale image of size 64×64 is used as cover. A string of english characters (text) is embedded in each cover pixel selected in the order dictated by the Hilbert curve. The tool chain from KEIL MDK µvision4 was used to obtain the implementation results. The code was written using embedded C language and compiled for Philips LPC 2148 microcontroller using ARMCC compiler. The compiler options have been enabled to optimize the code for execution time (Speed)

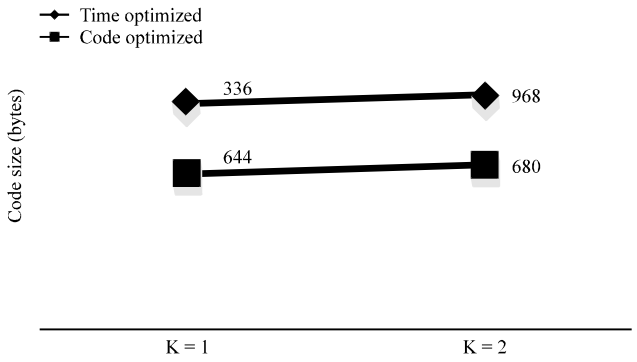

Fig. 3: Code size for embedding algorithm

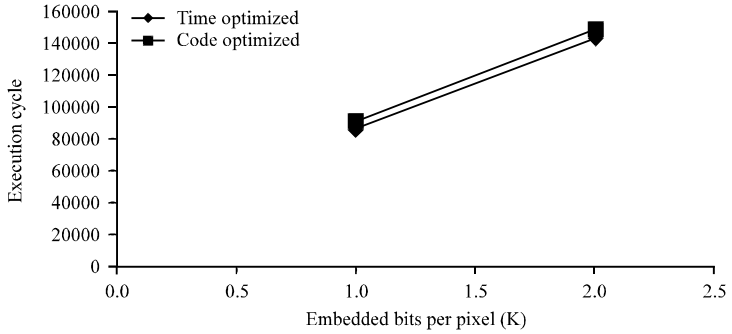

Fig. 4: Execution time for embedding algorithm

and code size (flash memory occupancy). The use of Micro Library (MicroLIB) significantly reduces the code size whereas, the use of same is not suggested for applications that demands speed as its crucial end.

The proposed embedding algorithm when optimized for code size as given by Fig. 3 results in the reduction of memory footprint around 30% in comparison with its counterpart, the time optimization. The graph results also show that for embedding with K>1, every rise in the value of 'K' makes only a paltry contribution towards the rise of code size. The execution time for the code and time optimized version of proposed embedding algorithm always grows radically with rise in bits embedded per pixel as given in Fig. 4.

The algorithm described in this study (Rajagopalan *et al*., 2012b) has been implemented again on the same hardware LPC2148 with which the proposed algorithm has been implemented. The execution time and clock cycles are analyzed with the KEIL MDK at 60 MHz the maximum operating frequency of LPC2148. The graph on Fig. 5 and 6 depicts the comparison results with two variants of optimization on code size and execution time respectively obtained in the proposed method with respect to the one obtained in this study.

The Fig. 7a and 8a shows the 64×64 cover images taken and Fig. 7b-c, 8b-c gives the stego images with K = 1 and 2, respectively. The quality of the stego image is analyzed for imperceptibility in terms of two error metrics namely Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) are tabulated in the Table 1 for full embedded capacity as given by the following equations:

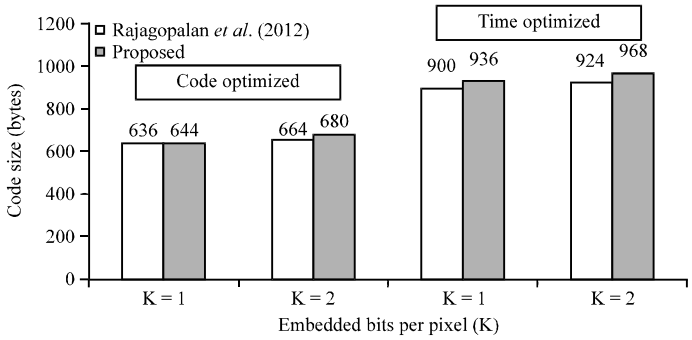

Fig. 5: Code size comparison

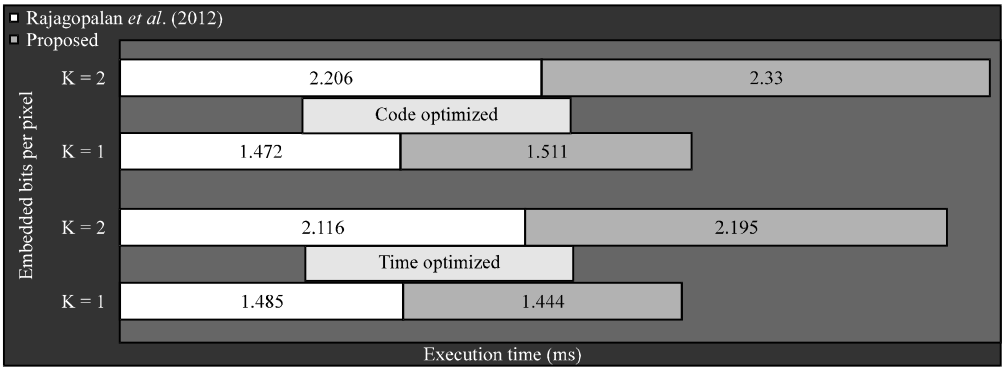

Fig. 6: Speed comparison

Fig. 7(a-c): Peppers, (a) Cover image, (b) Stego image (K = 1) and (c) Stego image (K = 2)

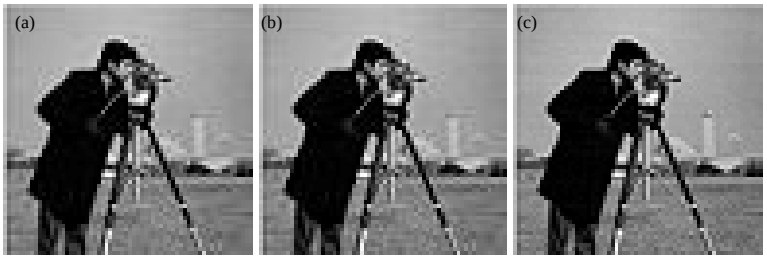

Fig. 8(a-c): Cameraman, (a) Cover image, (b) Stego image (K = 1) and (c) Stego image (K = 2)

Table 1: Error metrics

Image type	Size	K	MSE	PSNR (dB)
Cameraman	64×64	1	0.4941	51.1923
		2	2.4609	44.2198
Pepper	64×64	1	0.5061	51.0884
		2	2.5842	44.0075

$$MSE = \frac{1}{M \times N}\sum_{X=1}^{M}\sum_{Y=1}^{N}(S_{XY} - C_{XY})^2$$

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

Where:

$S_{X,Y}$: Stego pixel value

$C_{X,Y}$: Cover pixel value

C^2_{max}: Maximum intensity value of the pixel (255 for gray scale image)

CONCLUSION

The use of Hilbert LUT provides a tri coat technique for the selection of arbitrary cover pixel, plus bit and byte positions of the data to be embedded. The proposed technique consumes only less than 0.2% of 512 kB code space accessible on the selected embedded device. It offers a great benefit in applications where the code size is decisive, making the algorithm suitable as well for tiny embedded devices such as microcontrollers. Here, a random choice on the selection of cover pixel for embedding was done with the help of LUT in code memory in addition, the selection on secret data byte were also done in a random fashion to improve the security level with a negligible amount of trade-of f in execution cycles. Therefore, further enhancements may be considered by building multiple LUTs on flash memory making ample choices to raise the unpredictability and security.

REFERENCES

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

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., K. Karthikeyan, M. Malleswaran and J.B.B. Rayappan, 2013a. Kubera kolam: A way for random image steganography. Res. J. Inform. Technol., 5: 304-316.

Amirtharajan, R., M.V. Abhiram, G. Revathi, J.B. Reddy, V. Thanikaiselvan and J.B.B. Rayappan, 2013b. 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, 2013c. Why image encryption for better steganography. Res. J. Inform. Technol., 5: 341-351.

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

Amirtharajan, R., K.M. Ashfaaq, A.K. Infant and J.B.B. Rayappan, 2013e. High performance pixel indicator for colour image steganography. Res. J. Inform. Technol., 5: 277-290.

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.D. Roy, N. Nesakumar, M. Chandrasekar, R. Sridevi and J.B.B. Rayappan, 2013g. Mind game for cover steganography: A refuge. Res. J. Inform. Technol., 5: 137-148.

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

Amirtharajan, R., P.S. Priya and J.B.B. Rayappan, 2013i. Pixel indicated user indicator: A muxed stego. Res. J. Inform. Technol., 5: 73-86.

Amirtharajan, R., G. Devipriya, V. Thanikaiselvan and J.B.B. Rayappan, 2013j. High capacity triple plane embedding: A colour stego. Res. J. Inform. Technol., 5: 373-382.

Chan, C.K. and L.M. Cheng, 2004. Hiding data in images by simple LSB substitution. Pattern Recogn., 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.

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

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

Janakiraman, S., S. Rajagopalan, K. Thenmozhi, H.N. Upadhyay and J. Ramanathan *et al.*, 2013. Captivating CODEC Stego (CCS): A cover on camouflage. Res. J. Inform. Technol., 5: 160-170.

Janakiraman, S., J. Chakravarthy, B. Radhakrishnan, K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014a. Cover as key and key as data: An inborn stego. Inform. Technol. J., 13: 1969-1976.

Janakiraman, S., K.V.S.K. Kumar, R.R.K. Reddy, A. Srinivasulu and R. Amirtharajan *et al.*, 2014b. Humming bird with coloured wings: A feedback security approach. Inform. Technol. J., 13: 2022-2026.

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.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012a. Regulated OFDM-role of ECC and ANN: A review. J. Applied Sci., 12: 301-314.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012b. Phase for face saving-a multicarrier stego. Proc. Eng., 30: 790-797.

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., M. Nagadinesh, P. Lakshmi, K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2013b. Convolution and viterbi EN(DE)coders on OFDM hides, rides and conveys message-A neural STEGO. Proceedings of the International Conference on Computer Communication and Informatics, January 4-6, 2013, Coimbatore, pp: 1-5.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2014a. Sub carriers carry secret: An absolute stego approach. J. Applied Sci., 14: 1728-1735.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2014b. Double layer encoded encrypted data on multicarrier channel. J. Applied Sci., 14: 1689-1700.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014c. Purposeful error on OFDM: A secret channel. Inform. Technol. J., 13: 1985-1991.

Praveenkumar, P., G.S. Hemalatha, B. Reddy, K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014d. Secret link through simulink: A stego on OFDM channel. Inform. Technol. J., 13: 1999-2004.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014e. Stego in multicarrier: A phase hidden communication. Inform. Technol. J., 13: 2011-2016.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014f. Inserted embedding in OFDM channel: A multicarrier stego. Inform. Technol. J., 13: 2017-2021.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014g. Data puncturing in OFDM channel: A multicarrier stego. Inform. Technol. J., 13: 2037-2041.

Praveenkumar, P., R. Deepak, K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014h. Reversible steganography on OFDM channel: A role of cyclic codes. Inform. Technol. J., 13: 2047-2051.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014i. Reversible steganography on OFDM channel-a role of RS coding. Inform. Technol. J., 13: 2052-2056.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014j. Spread and hide-a stego transceiver. Inform. Technol. J., 13: 2061-2064.

Qi, X. and K. Wong, 2005. An adaptive DCT-based mod-4 steganographic method. Proceedings of the IEEE International Conference on Image Processing, Volume 2, September 11-14, 2005, Genoa, Italy, pp: II-297-II-300.

Rajagopalan, S. and H.N. Upadhyay, 2011. Stego system on chip with LFSR based information hiding approach. Int. J. Comput. Appl., 18: 24-31.

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

Rajagopalan, S., S. Janakiraman, H.N. Upadhyay and K. Thenmozhi, 2012b. Hide and seek in silicon: Performance analysis of Quad block Equisum Hardware Steganographic systems. Proc. Eng., 30: 806-813.

Rajagopalan, S., Y. Ravishankar, H.N. Upadhyay, J.B.B. Rayappan and R. Amirtharajan, 2014a. Modeling combo PR Generator for Stego Storage Self Test (SSST). Inform. Technol. J., 13: 1936-1944.

Rajagopalan, S., P.J.S. Prabhakar, M.S. Kumar, N.V.M. Nikhil, H.N. Upadhyay, J.B.B. Rayappan and R. Amirtharajan, 2014b. MSB based embedding with integrity: An adaptive RGB Stego on FPGA platform. Inform. Technol. J., 13: 1945-1952.

Rajagopalan, S., K. Pravallika, R. Radha, H.N. Upadhyay, J.B.B. Rayappan and R. Amirtharajan, 2014c. Stego on song-an amalgam of VI and FPGA for hardware info hide. Inform. Technol. J., 13: 1992-1998.

Rajagopalan, S., H.N. Upadhyay, S. Varadarajan, J.B.B. Rayappan and R. Amirtharajan, 2014d. Gyratory assisted info hide-a nibble differencing for message embedding. Inform. Technol. J., 13: 2005-2010.

Ramalingam, B., R. Amirtharajan and J.B.B. Rayappan, 2014a. LCC-LSB-FPGA stego-A reconfigurable security. J. Applied Sci., 14: 2139-2148.

Ramalingam, B., R. Amirtharajan and J.B.B. Rayappan, 2014b. Stego on FPGA: An IWT approach. Sci. World J., 10.1155/2014/192512

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.

Stanescu, D., V. Stangaciu, I. Ghergulescu and M. Stratulat, 2009. Steganography on embedded devices. Proceedings of the 5th International Symposium on Applied Computational Intelligence and Informatics, May 28-29, 2009, Timisoara, pp: 313-318.

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. Wavelet Pave the Trio travel for a secret mission: A stego vision. Global Trends Inf. Syst. Software Appl., 270: 212-221.

Thanikaiselvan, V., P. Arulmozhivarman, R. Amirtharajan and J.B.B. Rayappan, 2012c. Horse riding and hiding in image for data guarding. Proc. Eng., 30: 36-44.

Thanikaiselvan, V., P. Arulmozhivarman, S. Subashanthini and R. Amirtharajan, 2013a. A graph theory practice on transformed image: A random image steganography. Sci. World J., 10.1155/2013/464107

Thanikaiselvan, V., K. Santosh, D. Manikanta and R. Amirtharajan, 2013b. 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.

Thien, C.C. and J.C. Lin, 2003. A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function. Pattern Recogn., 36: 2875-2881.

Wong, K., X. Qin and K. Tanaka, 2007. A DCT-based Mod4 steganographic method. Signal Process., 87: 1251-1263.

Wu, D.C. and W.H. Tsai, 2003. A steganographic method for images by pixel-value differencing. Pattern Recogn. Lett., 24: 1613-1626.

Zhang, X. and S. Wang, 2004. Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security. Pattern Recognit. Lett., 25: 331-339.

Zhao, Z. and H. Luo, 2012. Reversible data hiding based on Hilbert curve scan and histogram modification. Inform. Technol. J., 11: 209-216.