http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 13 (16): 2544-2551, 2014
ISSN 1812-5638 / DOI: 10.3923/itj.2014.2544.2551

Least Significant Bit but Quantum Bit: A Quasi Stego

Padmapriya Praveenkumar, P. Rajalakshmi, G.U. Priyanga, K. Thenmozhi,
John Bosco Balaguru Rayappan and Rengarajan Amirtharajan
Department of Electronics and Communication Engineering, School of Electrical and
Electronics Engineering, SASTRA University, Thanjavur, Tamil Nadu, India

Abstract: Security has become the most indispensible part of any form of communication. There are different ways through which it is brought about, out of which one of the efficient implementation through steganography and encryption. Steganography conceals the existence of a secret message throughout the communication thereby providing enhanced security. In this study, a methodology has been proposed to perform encryption on an image with the help of Secret Steganography Code for Embedding (SSCE) code. A mapping technique has been proposed to combine quantum truth table and LSB based embedding. The SSCE has been employed to provide encryption, followed by quantum table before embedding the secret data. The proposed methodology supports both images and text as cover as well as secret data. In the proposed scheme, embedding has been included with encryption to provide security multifold. The implementation was carried out using Visual Basic. NET and results are presented.

Key words: Information security, quantum encryption, quantum steganography, quantum states, SSCE code

INTRODUCTION

In the present scenario, the marked up dependence on technology have lead to vulnerable privacy. This brings out more desire for security to rectify privacy in virtual realm. Hence, the term data encryption evolved simultaneously which was widely used to ensure the protection of information. Encryption is the method that imparts the content of the messages unintelligible to the persons who are not authorized to read it. It is simply the translation of a message into secret code. And to read that encrypted code, you need to have the secret key to decrypt the message.

There is an interesting sub discipline of information hiding called steganography. It is an art of maintaining secrecy of transmission of any message so that it is not even susceptible to an intruder. The term steganography has its provenance from the Greek words, "Stego" means "Cover" and "Graphy" means "Writing". It is otherwise called as concealed writing (Amirtharajan and Rayappan, 2012a-c, 2013; Amirtharajan *et al*., 2013a- j; Cheddad *et al*., 2010). It is a variant cryptography for data security (Praveenkumar *et al*., 2014a-n, 2013a-d, 2012a, b). Whereas, cryptography is a method for maintaining confidentiality or simple privacy of data. Steganography is basically classified into three categories (Ramalingam *et al*., 2014a, b; Rajagopalan *et al*., 2014a-d; Thanikaiselvan *et al*., 2012a-c, 2013a, b, 2014). These are text steganography, image steganography and audio/video steganography. All the three of them have their own specialization and characteristics.

Over the past few years, there had been increasing steganography techniques that are greatly used to ingrain secret messages into multi-media objects. This is because that multimedia objects have high rate of superfluous information which provides a way to add large number of data by carrying out cinch and profound changes that preserve visceral content of the cover. This study effectively implies image steganography (Amirtharajan and Rayappan, 2012a-c; Janakiraman *et al*., 2012a, b, 2013, 2014a, b; Rajagopalan *et al*., 2014a-d).

In image steganography, the information is entirely hidden inside the images. There are various techniques present to perform this operation. The LSB substitution is one of the most simple and straight forward techniques. Here, the message is ingrained into least significant bit plane hence it causes less degradation of the cover. The LSB based techniques stays to be an ambitious task for the steg-analyst to differentiate the cover and stego images, given small changes have been made.

MATERIALS AND METHODS

Quantum gate: Behind every computation, there will be certainly some basic logic. The general classical computations are carried out using basic logic such as 0

Corresponding Author: Padmapriya Praveenkumar, Department of Electronics and Communication Engineering, School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, Tamil Nadu, India

and 1. They can physically be represented by on and off condition. Quantum circuits are quite different from the digital circuits due to certain rules that are new to quantum computations. The quantum bit are generally considered to be a vector in a two dimensional Hilbert space. A fresh quantum computing is found to be a major application in cryptography. For a physical system, its state can be pictured by its wave function which is completely characterized by the state of the system. An electric circuit was constructed using logic gates similarly quantum circuits are constructed using quantum gates. These quantum gates employ many basic operations based on its states (Shaw and Brun, 2011; Qu *et al*., 2010, 2011).

Qubits are the quantum bits (Qu *et al*., 2010; Martin, 2007; Liao *et al*., 2010) upon which the basic quantum circuits operate. Unlike logic gates which are most often irreversible, the quantum gates are physically and logically reversible. A qubit is a basic or smallest unit for manipulation of quantum circuits. They have two possible states ket|0> and ket|1> which are also known as computational basis states. A logic bit can take either 0 or 1 whereas a quantum bit can take the superposition of both the states. Quantum probability amplitudes are defined by complex number. Qubits are somewhat distinct from Boolean logic and that is the reason why they have excitingly increased expectations.

C-NOT quantum truth table: The operation of controlled gate is represented by "If first bit is true, then perform NOT on the second bit". Where the first bit is the control qubit and the second bit is the target qubit. If control qubit is 0, then target qubit is not changed. If control qubit is set to 1, then target qubit is inverted.

C-NOT gate quantum truth table are given in Table 1. Inverse of a unitary matrix is again a unitary matrix therefore, this gate is logically reversible. This gate is universal. It is the quantum parallel of the universality of the NAND gate. Therefore, this gives logical and physical reversibility. This quantum truth table has been used for mapping.

VB.NET platform: The implementation of this concept was carried out in VB.NET platform. This language has got many striking features. The basic structure of this programming language is facile and especially when it comes to executable code. It is an integrated, Interactive Development Environment (IDE). This VB-IDE stays to be a cornerstone for Rapid Application Development (RAD) which braces the use of graphical user interfaces. This is

Table 1: Quantum truth table

C-NOT	<00>	<01>	<10>	<11>
<00>	1	0	0	0
<01>	0	1	0	0
<10>	0	0	0	1
<11>	0	0	1	0

mainly made of use in this study. It has also got 'Intelligence' technology which shows a popup window about the types of constructs.

Now, if the message is embedded into the LSB of the cover image, the resultant LSB plane will provide attention and will clearly turn over the message. Hence, it is strongly ratified to maintain a randomness of LSB, for which encryption can be performed. And this encrypted message should be randomly inserted into a subset of pixels. Then encryption is accomplished using SSCE code. In order to boost up the security level, quantum mapping concept is also used ahead of embedding the message into cover.

The secret image to be trespassed via a communication channel is first selected as given in Fig. 1. It is encrypted using SSCE code. A secret key is generated which has to be used at the receiver for decryption. Then a random matrix is chosen according to the size of input image. The quantum truth table is mapped to this random matrix from top left till the end. The encrypted messages are replaced by 0's present in the mapped matrix. A suitable cover image is chosen. This table of encrypted message contents is then embedded into the cover image. The LSB based substitution has been carried out here. Thus, a stego image has been formed.

At the receiver side, the message was extracted from the LSB plane of stego image. And the decryption was performed using the secret key for SSCE code. Thus, the resultant gives the secret image which was originally transmitted.

Algorithm of the proposed scheme:

- Get an input secret image of size N×N
- Encrypt the image by modifying each pixel value by its corresponding SSCE values
- The next step is to declare a ones matrix of dimension (N+N/2)×(N+N/2)
- Map the quantum truth table, shown in Fig. 1, to the above ones matrix
- Then replace 0's in the above mapped matrix by the pixel values of encrypted image
- Convert the matrix into an array and then convert each value in to 8-bit binary representation

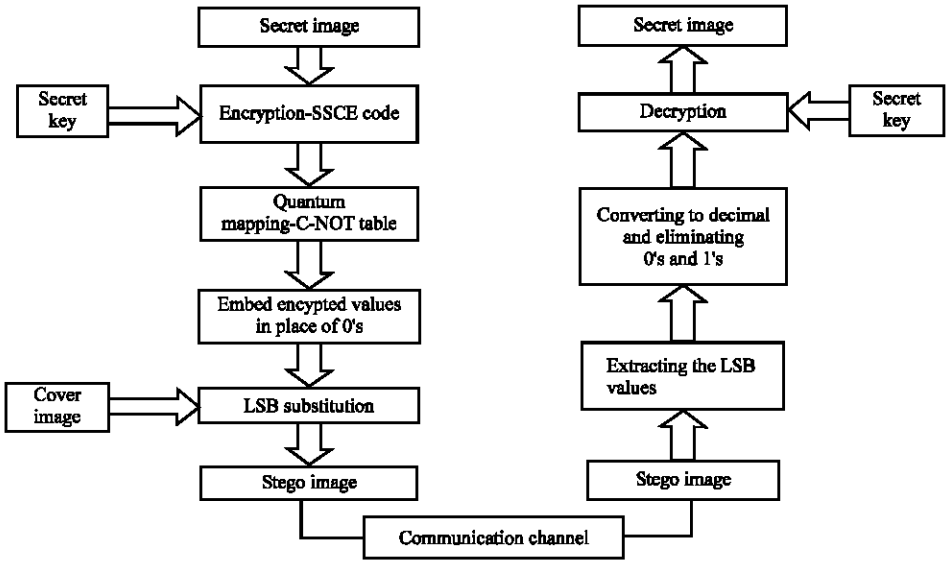

Fig. 1: Proposed methodology

- Get a cover image into which the secret image should be hidden
- Convert each pixel of cover image into 8-bit binary representation
- Now replace the LSB of each pixel of cover image by a bit in binary array
- Then convert back the values to decimal and display that as image
- So that stego image which contains secret information will be transmitted through the communication channel
- At the receiver side, after receiving the stego image, its converted in to binary in order to retrieve the LSB bits.
- After retrieving, the values are converted back to decimal
- From the extracted decimal values, excluding 0's and 1's remaining values are stored in a matrix and they are converted back to original values using the SSCE value
- Then, finally secret message was extracted

RESULTS AND DISCUSSION

The proposed methodology was implemented using ten images and implemented using VB.NET platform for both images and text. One of the sample secret image, cover image and its corresponding outputs are shown below. A secret input image was taken and analyzed for better results. The following are the output at various stages of the process. Figure 2 shows the output window

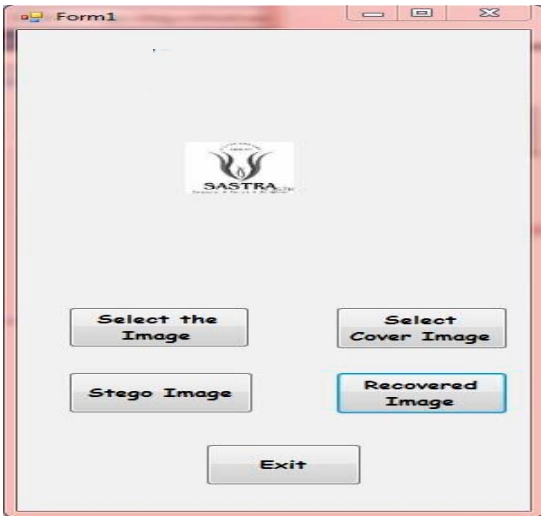

Fig. 2: Secret input image

of the input image on the screen. Figure 3 shows the encrypted output image after the encrypting the original image with the SSCE code (Qu *et al*., 2010, 2011; Liao *et al*., 2010). Figure 4 shows the cover image into which the encrypted image is to be embedded. Figure 5 shows the stego image that has hidden information.

Finally, Fig. 6 shows the extracted image from which the original secret image was decrypted at the receiver side as given in Fig. 7. This same concept can also be implemented for text data. The message and cover can be taken as text data. The algorithm resembles as that for

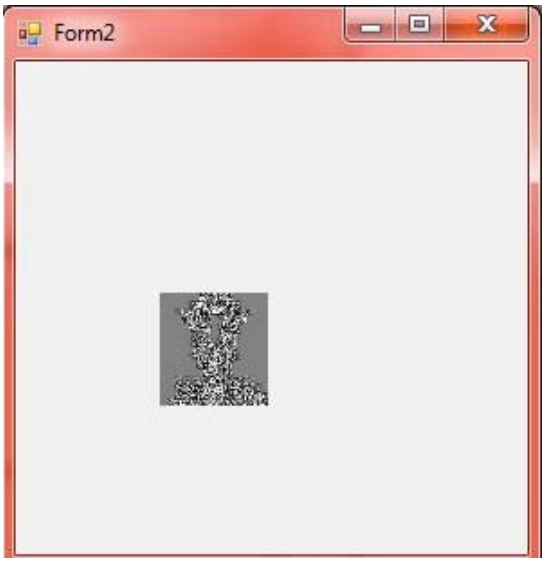

Fig. 3: Encrypted image of secret input image

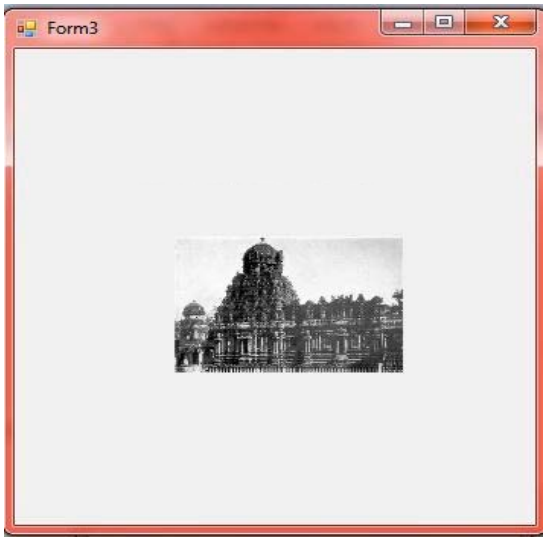

Fig. 4: Cover image

images except a few steps at embedding the encrypted value into cover. While, using images simple LSB substitution was carried out, instead in text, a concept of quantum states are used.

The information is shuffled using the 4 quantum states. They are 00 Rectilinear Vertical, 01-Rectilinear Horizontal-Diagonal Left circular polarization and 11-Diagonal Right circular polarization. Then the changes were made in the cover text using variations made in articles of the passage. The embedding was performed using the following rule as given in Table 2.

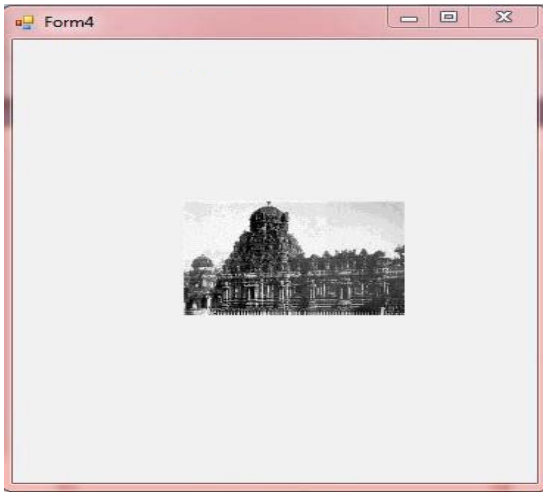

Fig. 5: Stego image

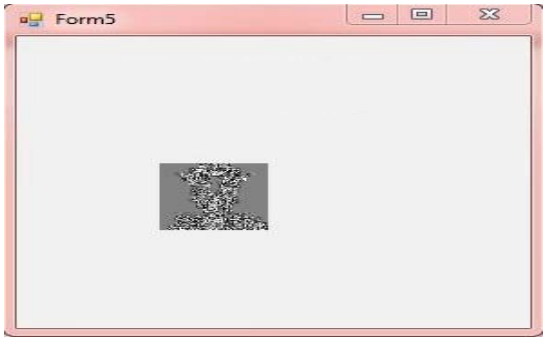

Fig. 6: Extracted image

Fig. 7: Recovered secret image

Table 2: Embedding table for text

Words		Bit sequence
a	Consonant	00
an	Vowel	11
a	Vowel	10
an	Consonant	01

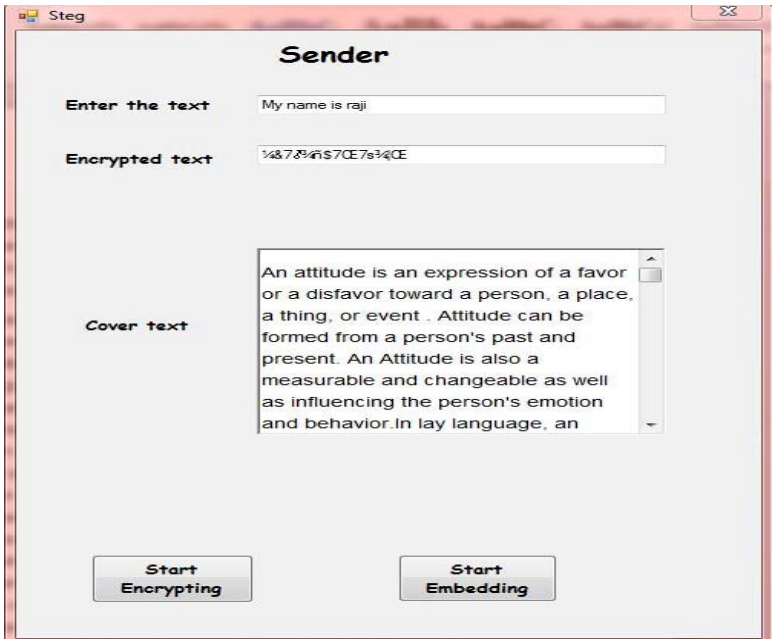

Fig. 8: Output of text based steganography on sender side

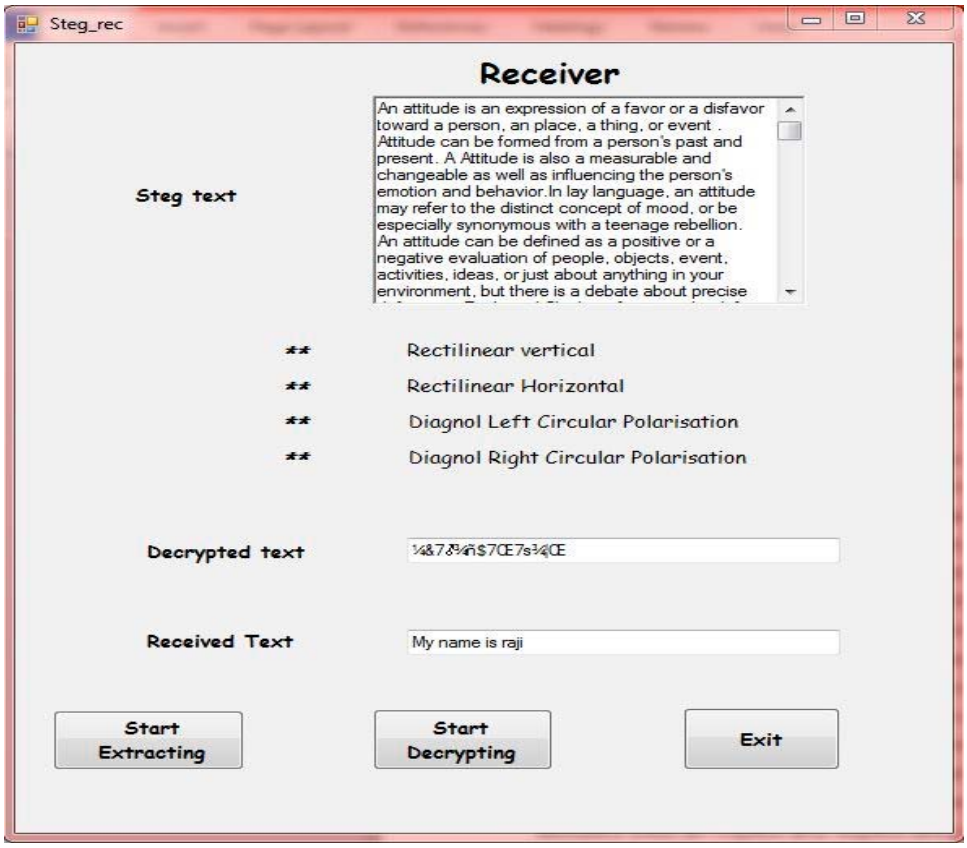

Fig. 9: Output of text based steganography on receiver side

Using the above mentioned procedure, the text of various lengths were taken as input and corresponding cover text were chosen to analyze the result of text steganography. Figure 8 and 9 shows the embedding and the extraction at the transmitter and at the receiver side consider text as cover and secret data, respectively.

CONCLUSION

In the proposed scheme, SSCE codes are initially used for encryption, followed by quantum table for shuffling and LSB based embedding was done considering images as cover and secret. Then, text based steganography was done where four quantum states were involved to shuffle the text and table for performing text based embedding was considered. In total, this method supports both images and text as cover as well as secret data. In addition, this method scheme, embedding has been included with encryption to provide security multifold. The implementation was carried out using Visual Basic. NET and results are presented.

REFERENCES

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. 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. and J.B.B. Rayappan, 2013. Steganography-time to time: A review. Res. J. Inform. Technol., 5: 53-66.

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

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

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

Amirtharajan, R., M.V. Abhiram, G. Revathi, J.B. Reddy, V. Thanikaiselvan and J.B.B. Rayappan, 2013d. Rubik's cube: A way for random image steganography. Res. J. Inform. Technol., 5: 329-340.

Amirtharajan, R., P. Archana and J.B.B. Rayappan, 2013e. Why image encryption for better steganography. Res. J. Inform. Technol., 5: 341-351.

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

Amirtharajan, R., R. Subrahmanyam, J.N. Teja, K.M. Reddy and J.B.B. Rayappan, 2013g. Pixel indicated triple layer: A way for random image steganography. Res. J. Inform. Technol., 5: 87-99.

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

Amirtharajan, R., S.D. Roy, N. Nesakumar, M. Chandrasekar, R. Sridevi and J.B.B. Rayappan, 2013i. 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, 2013j. Pixel indicates, standard deviates: A way for random image steganography. Res. J. Inform. Technol., 5: 383-392.

Cheddad, A., J. Condell, K. Curran and P. McKevitt, 2010. A hash-based image encryption algorithm. Opt. Commun., 283: 879-893.

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.

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., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014a. Audio fingerprint indicator in embedded platform: A way for hardware steganography. J. Artif. Intell., 7: 82-93.

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

Liao, X., Q.Y. Wen, Y. Sun and J. Zhang, 2010. Multi-party covert communication with steganography and quantum secret sharing. J. Syst. Software, 83: 1801-1804.

Martin, K., 2007. Steganographic Communication with Quantum Information. In: Information Hiding, Furon, T., F. Cayre, G. Doerr and P. Bas (Eds.). Springer, Berlin Heidelberg, ISBN: 978-3-540-77369-6, pp: 32-49.

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

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

Praveenkumar, P., K. Thenmozhi, M.N. Dinesh and R. Amirtharajan, 2013a. Fixing, padding and embedding: A modulated stego. Int. J. Eng. Technol., 5: 2257-2261.

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, 2013c. Can we reduce PAPR? OFDM+PTS+SLM+STEGO: A novel approach. Asian J. Sci. Res., 6: 38-52.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2013d. OFDM with low PAPR: A novel role of partial transmit sequence. Res. J. Inform. Technol., 5: 35-44.

Praveenkumar, P., R. Hemalatha, R. Uma, K. Madhumisha, K. Thenmozhi and R. Amirtharajan, 2014a. Image Zoning→encryption. Res. J. Inform. Technol., 6: 368-378.

Praveenkumar, P., G. Ashwin, S.P.K. Agarwal, S.N. Bharathi, V.S. Venkatachalam, K. Thenmozhi and R. Amirtharajan, 2014b. Rubik's cube blend with logistic map on RGB: A way for image encryption. Res. J. Inform. Technol., 6: 207-215.

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

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

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

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

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2014j. Coded crypted converted hiding (C^3H)-a stego channel. J. Applied Sci., 14: 1786-1797.

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

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

Praveenkumar, P., R. Amirtharajan, R.S. Janani, K. Thenmozhi and J.B.B. Rayappan, 2014m. Multi (Carrier+Modulator) adaptive system: An anti fading stego approach. J. Applied Sci., 14: 1836-1843.

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

Qu, Z.G., X.B. Chen, X.J. Zhou, X.X. Niu and Y.X. Yang, 2010. Novel quantum steganography with large payload. Opt. Commun., 283: 4782-4786.

Qu, Z.G., X.B. Chen, M.X. Luo, X.X. Niu and Y.X. Yang, 2011. Quantum steganography with large payload based on entanglement swapping of χ-type entangled states. Opt. Commun., 284: 2075-2082.

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

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

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

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

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.

Shaw, B.A. and T.A. Brun, 2011. Quantum steganography with noisy quantum channels. Phys. Rev. A: Atomic Mol. Opt. Phys., Vol. 83. 10.1103/ PhysRevA.83.022310.

Thanikaiselvan, V., P. Arulmozhivarman, J.B.B. Rayappan and R. Amirtharajan, 2012a. Graceful graph for graceful security-towards a STE (G) Raph. Res. J. Inform. Technol., 4: 220-227.

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

Thanikaiselvan, V., P. Arulmozhivarman, R. Amirtharajan and J.B.B. Rayappan, 2012c. Wavelet Pave the Trio travel for a secret mission: A stego vision. Global Trends Inform. Syst. Software Applic., 270: 212-221.

Thanikaiselvan, V., K. Santosh, D. Manikanta and R. Amirtharajan, 2013a. A new steganography algorithm against chi square attack. Res. J. Inform. Technol., 5: 363-372.

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

Thanikaiselvan, V., S. Subashanthini and R. Amirtharajan, 2014. PVD based steganography on scrambled RGB cover images with pixel indicator. J. Artif. Intell., 7: 54-68.