Journal of Engineering and Applied Sciences 13 (3): 739-745, 2018
ISSN: 1816-949X

Chaos-Based Speech Steganography and Quantum One Time Pad

[1]Zaid A. Abod, [2]Hussein A. Ismael and [2]Alharith A. Abdullah
[1]College of Food Science, Al-Qasim Green University, Babil, Iraq
[2]College of Information Technology, University of Babylon, Babil, Iraq

Abstract: This research introduces chaos-based speech steganography and quantum cryptography methods that are respectively based on (LSB) or Least Significant Bit and (QOTP) or Quantum Onetime Pad. In the schemes suggested, for scrambling and selection, two chaotic maps have been used, standard map and Lorenz map. The standard chaotic map is used as key two times, one time for scrambling a text message and second time for selecting the position where the text message will be hidden. As for the Lorenz map, it is used as key to select the frames in which the text message is hidden. Then, the data are embedded based on the indices for the ordered sequence of the host speech LSB's samples. Finally, encrypting the embedded data by using one of the quantum cryptography mechanisms which is quantum one-time pad. For the scheme proposed an analysis is discussed. It deals with the key generation drawbacks and distributions for quantum one-time pad through the use of the chaotic map and the quantum laws concepts. The proposed method satisfies the main requirements of steganography, robustness, hidden data capacity and perceptual transparency. Results of the experiments, signal-to-noise ratio, waveform analysis and others, showed that the stego-speech has high qualities. The analyses showed the effectiveness of the method suggested and as a result it can be used for securing communication.

Key words: Least significant bit, speech steganography, steganography, quantum cryptography, quantum one time-pad, chaotic maps

INTRODUCTION

Cryptography is a wide science and always sophisticated by looking for new ideas that help in the evolution of this science. The idea of combining quantum cryptography and steganography are emerging and the goal of these techniques is to provide confidentiality, authenticity, non-repudiation, integrity and data security. Quantum cryptography and steganography are hybrid system where the steganography is considered the arts of invisible communications are achieved by hiding secret data inside carrier files such as an audio. After secret data being hidden, the carrier files must appear unsuspicious so that, the existences of the data embedded is hidden. On the other hand, the new technology of using properties of quantum for performing cryptography algorithms is quantum cryptography quantum computer power that it will be developed in the near future and will help to intercept any secret information and communication. So, the solution for this problem is the combining the quantum cryptography with steganography will increase the privacy of today's information from tomorrow's powerful quantum computer.

There are many aspects proposed related to the combination of cryptography and steganography some of them close to our proposed idea. According to Pelosi *et al*., 2016, the researchers combine cryptography and steganography in their researches they introduced classical one-time pad encryption and steganography system, including all software necessary to complete practical communication. Another similar approach but using different cryptography algorithm has been proposed by Laskar and Hemachandran (2012). They used transposition cipher method for the encryption process. This encryption process has been combined with random LSB technique to make the model more secure. In Saini and Verma (2013) proposed methods to integrate steganography and cryptography for secure communications using images file. AES algorithm is used in encryption, then it is concealed into the cover images using the concepts of steganography. The researchers (Ren-Er *et al.* 2014) presented a rapid combine method based on DES encryption and LSB steganography. Another proposed method to integrate steganography and cryptography for securing communications using image files. The RSA algorithm is used in encryption and LSB technique for steganography (Pund-Dange and Desai, 2015). Recently, two models are presented by combining cryptography and steganography. One of them employed a quick response codes for encoding the

Corresponding Author: Zaid A. Abod, College of Food Science, Al-Qasim Green University, Babil, Iraq

encrypted message before hiding it in the image. And the other model used classical hybrid algorithms which is RSA and Diffie-Hellman before hiding it in the image (Karthikeyan *et al*., 2016; Satar *et al*., 2016). Two most related researches to our proposed algorithm are presented in 2016 the first one proposed a hybrid audio steganography and cryptography by using Least Significant Bit (LSB) and AES encryption algorithm (Krishnan and Abdullah, 2016) for the second time, the researcher proposed one-time pad, methods of cryptography that are based on Least Significant Bits (LSB) and chaos based audio steganography (Alwahbani *et al*., 2016).

In this study, we developed the idea of combining the cryptography and steganography by using quantum cryptography and chaotic maps which relies on quantum laws. We combine a complete steganography system with the quantum cryptography based on Quantum One-Time Pad (QOTP) encryption and Least Significant Bit (LSB) substitution adaptive steganography technology. The hybrid system is tested and shown to be resistant to many common security analysis attack.

Chaotic maps: Chaos theory is a phenomenon which has inevitability latency rules behind irregular appearances. It can be considered one of the hardest nonlinear problems. The original of chaos has started in mathematics and physics and expanded into engineering. The mathematics has described that theory as 'random' which it is a result of the simple systems inevitability affected by the initial-conditions of these systems. Currently, there is a considerable interest in the study and applications of chaotic systems and its importance in multidisciplinary fields such as cryptography, chemistry, physics, engineering, neurophysiology, etc. Chaos has a set of important properties including the sensitive, the deterministic, the irregular, the long-term prediction and the property of non-linear. The studies in the last century focused on the use of chaotic in cryptography so as to get features from which to achieve the security of the system designer based on this phenomenon (Ismael and Sadkhan, 2017). The following subsection introduces standard map and Lorenz chaotic map briefly that have been used for the suggested system.

Standard Map (SM): This map is 2 a D chaotic map. It can be described mathematically as follows:

$$x_t = x_{t-1} + k \sin y_{t-1} \bmod 2\pi \quad (1)$$

$$y_t = y_{t-1} + x_{t-1} \bmod 2\pi \quad (2)$$

Where:

x_n and y_n = Within the period $[0, 2\pi]$

k = Parameter of system with values ($k \geq 18.9$)

It is considered chaotic with this value of 'k' parameter (Pierre *et al*., 1984).

Lorenz Map (ZM): It is the most famous chaotic map. It has been appearing in 1963 by Edward Lorenz. It is considered a simple model for convection of atmospheric. It is an ordinary differential equation. It is a 3-Dimension map. It can be detailed mathematically (Pierre *et al*., 1984):

$$\dot{x}(n) = \sigma(y(n) - x(n)) \quad (3)$$

$$\dot{y}(n) = rx(n) - y(n) - x(x)z(n) \quad (4)$$

$$\dot{z}(n) = x(n)y(n) - bz(n) \quad (5)$$

where, 'θ', 'r' and 'p' are parameters with values (10, 28, 8/3), respectively. They are constants. And x(0) y(0) and z(0) are Lorenz map initial values.

LSB steganography: The Least Significant Bit (LSB) substitution is the simple and well-known steganography method (Johnson and Jajodia, 1998). This method used with images and audio where it replaces the least significant bits directly through embeds messages into the cover image or cover audio. To increase the capacity of hiding, it can be used up to four significant bits (1 bit for each for red, green, blue and alpha color channels, respectively) per pixel with images and in audio the data embedding in the inactive frames of low bit rate audio streams. It has a known weak points, i.e., the values of the sample asymmetrically change. When the LSB of the values of cover medium sample are equal to the message bit no changes are made. Otherwise, the values 2n are changed to 2n+1 or 2n+1 is altered to 2n (Swain and Lenka, 2014). There are many improvements and modifications that have been proposed to strengthen this technique such as adaptive techniques that alter payload distribution based on image and audio characteristics. If the message is encrypted first and then embedded, the level of the security will be improved.

Quantum one-time pad: The "One-Time Pad" encryption algorithm was invented early and has since, been proven as unbreakable. The ciphertext is proved to be unbreakable when the "one-time pad" condition is satisfied where the "one-time pad" is typically implemented by using exclusive or (XOR) addition to

combine plaintext elements with key elements, the key is completely random and the key cannot be used more than once and this is the conditions of the "one-time pad" to be unbreakable (Pund-Dange and Desai, 2015).

The central problem in "one-time pad" is distributed key where the key should be the same length with the plaintext among N number of users. Classical key distribution protocols are unable to detect an adversary between two legitimate parties. Quantum Key Distribution (QKD) protocol solves this problem. The most commonly used (QKD) protocol is BB84 (Bennett and Brassard, 2014). The security of (QKD) is guaranteed by the laws of quantum. The quantum uncertainty principle explained by Busch *et al.* (2007) allows to securely sharing a secret key among two legitimate parties.

The idea of a "Quantum One-Time Pad" (QOTP) is presented by Boykin and Roychowdhury (2003). The protocol researches by transmitting the quantum particles from receiver to sender where the sender embeds his information and then from sender to the receiver where "quantum one-time pad" is an encryption scheme for qubits.

MATERIALS AND METHODS

In this study, we introduced a new model for two stages steganography: to secure and hide the secret message into the host speech signal using LSB algorithm and secure mechanism: that uses quantum cryptography, prior to sending it via quantum communication channel. This model rely on chaotic maps for the three processes, scrambling, choosing and hiding. The following sections study the two main stages, steganography and encryption.

Message hiding: The secret message is converted into binary bits, before embedding in the host speech signal. The chaotic Standard Map (SM) is used for generating sequences pseudo random numbers, that are used as the keys for scrambling of secret message bits. As well as, the chaotic Lorenz Map (LM) is used as the key for choosing the frames of a speech signal where the speech signal is divided into frames each frame has 256 samples. Furthermore, divide the secret message that produced form previous step into groups where each group has 16 bits and save it in each selected frame. Finally, use the Standard chaotic Map (SM) for selecting locations in the selected frame to embedded the secret message by using the Least Significant Bit (LSB) substitution. The hiding algorithm is detailed as follows:

Algorithm 1; The hiding algorithm:

1: Read speech signal and save it in one-dimensions array
2: Divide the speech signal into frames where each frame has 256 samples
3: Read the secret text message and save it in one-dimension array
4: Calculate the number of characters of secret text message
5: Convert the array of text message to binary system
6: Use the standard chaotic map for scrambling the binary text message.
7: Divide the binary text message that produced form previous step into groups where each group has 16 bits and save the number of groups in variable (no-g)
8: Use the Lorenz chaotic map for selecting number of frames that equal to (no-g)
9: Make the least significant bit "indicator" for the center of the selected frame equal to "1 otherwise "unselected frames" equal to "0"
10: While (j< = no-g)
Begin
Use the standard chaotic map for selecting locations in the selected frame j Hide the group j in the selected frame j by using LSB technique
End

Message encryption: After embedding the message, the output is encrypted using a quantum one-time pad where the key used in the algorithm choosing by using BB84 protocol.

Senders and receivers obtained copies of the initial values and systems parameters for all chaotic maps and generate BB84 protocol for the quantum one-time pad. The encryption algorithms are detailed as follow: the complete our model process as depicted in Fig. 1:

Algorithm 2; The encryption algorithm:

1: Convert the produced data of speech to binary system
2: Convert the produced data of speech from previous step to vectors
3: Apply QOTP by applying a bit flips with the vector and quantum key where key is choosing by using BB84 protocol between sender and receiver
4: The output of the algorithm sends via quantum channel
5: Send the initial values and keys of chaotic maps by using Diffie Hellman exchange key (Steiner *et al.*, 1996)

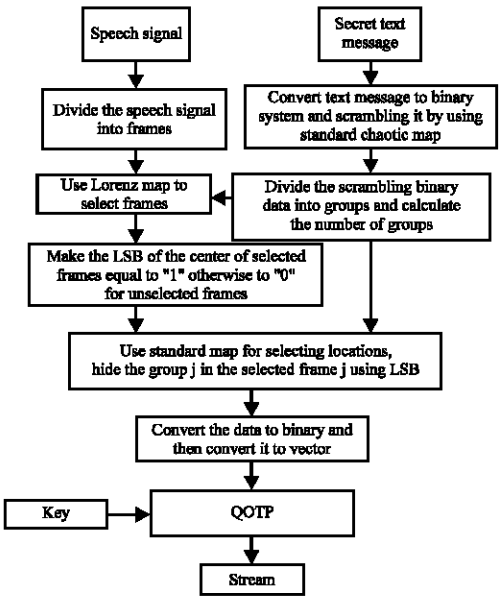

Fig. 1: Block diagram of the proposed model

RESULTS AND DISCUSSION

This part discusses many results of the experiments for demonstrating the effectiveness of the proposed design. The proposed method is implemented using MATLAB Software. All the experimental results were conducted using some WAV sound files.

Wave form and spectrogram analysis: To analyze the proposed method, a waveform of the cover speech signal and stego-speech signal are visualized and compared. Figure 2 shows an example to embed a message: 60 bytes in a cover file which is one of the tested file with sampling rate 8 kHz, 16 bits for each sample, 480,000 samples and 60 sec duration. The larger number of characters to be hidden in the speech sign is equal to (3750 chars) and the Chaotic maps parameters using for example initial condition and parameters values as follows: Lorenz $x_0 = 0$, $y_0 = 4$, $z_0 = 6$, $z_0 = 10$, $\sigma = 28$, $r = 8/3$ and Standard $x_0 = 0.1$, $y_0 = 0.2$, $k = 18.9$. These parameters represent the keys for hiding secret message. Figure 2 and 3 show that there is no obvious difference between the cover speech signal and the corresponding stego-speech. In addition to Fig. 4 and 5 show also that with spectrogram there is no difference between the cover speech signal a nd the c orresponding stego-speech.

Table 1 produces the percentages difference between the covers audio and the stego-speech when a message with a different size is embedded in the host speech, it is very small.

Signal to noise ratio: Signal-to-Noise Ratio (SNR) is a common measurement for the speech signal quality that is measure the noise in the signal. It is given by the following Eq. 6:

$$SNR(s(i), sn(i)) = 10\log_{10}\frac{\sum_{i=1}^{i=N} s(i)^2}{\sum_{i=1}^{i=N} s(i)-sn(i)^2} \quad (6)$$

Where:

N = The samples total number
s(i) = The original (cover) signal amplitude
sn(i) = Reconstructed signal the amplitude
SNR = High values mean high data precision, low values on the other hand indicate large amount of noise

SNR is used in this research for measuring the difference between the original speech signal (cover) and the stego-speech signal. We embedded different text messages and we compute the SNR for them as shown in (Table 2). And we noticed that the values of SNR are very large with the large embedded messages and this indicates high quality and accuracy of the stego files see Table 2. In addition, there are no significant degradations of the speech signal file quality when the size of the messages is raised (Pelosi *et al*., 2016).

Peak signal to noise ratio: Table 3 shows, it is clear that the PSNR values are very large even large messages are embedded which indicate high precision and quality of the stego file. Also, there is no significant degradation of the speech signal file quality when the message size is increased.

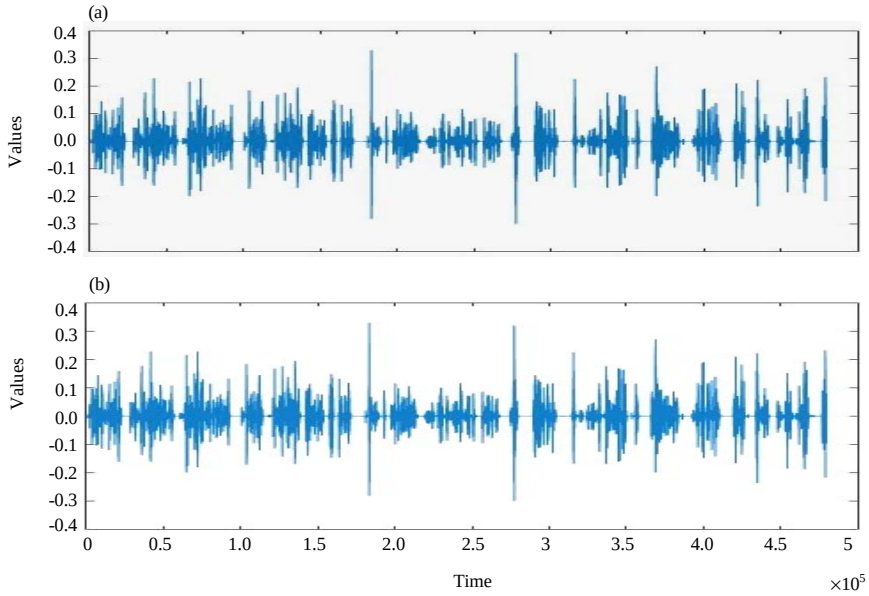

Fig. 2: Waveform of cover and stego-speech signal for message of 60 bytes

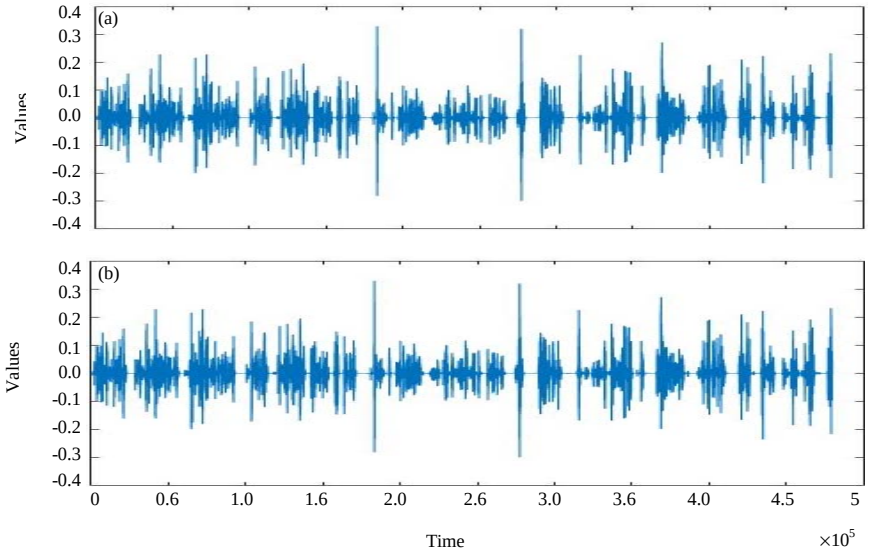

Fig. 3: Waveform of cover and stego speech signal for message of 100 bytes

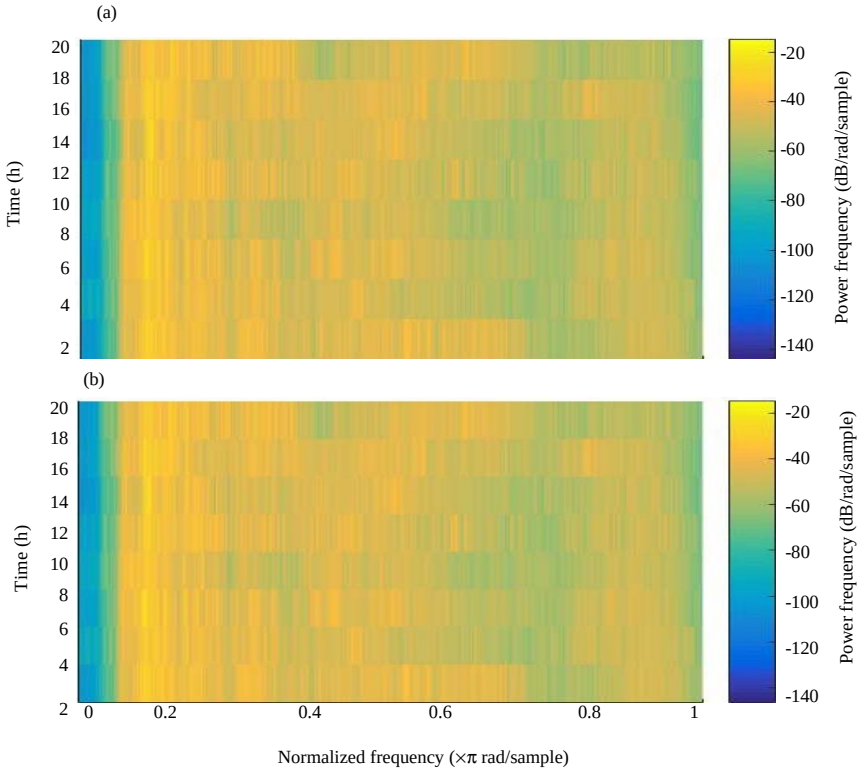

Fig. 4: Spectrogram of cover and stego speech signal for message of 60 bytes

Mean-squared error: Table 4 shows it is clear that the MSE values are very small that refers to a high quality and precision of the stego file. Furthermore, there are no significant degradations of the speech signal file quality when the size of the message is raised.

Security key: BB84 is a security protocol used in quantum one-time pad and proven unconditionally secure against unlimited resources and provided that by using the idea of photon polarization and each bit encoded with random photon polarization. So, based on quantum laws the attacker cannot intercept the quantum channel

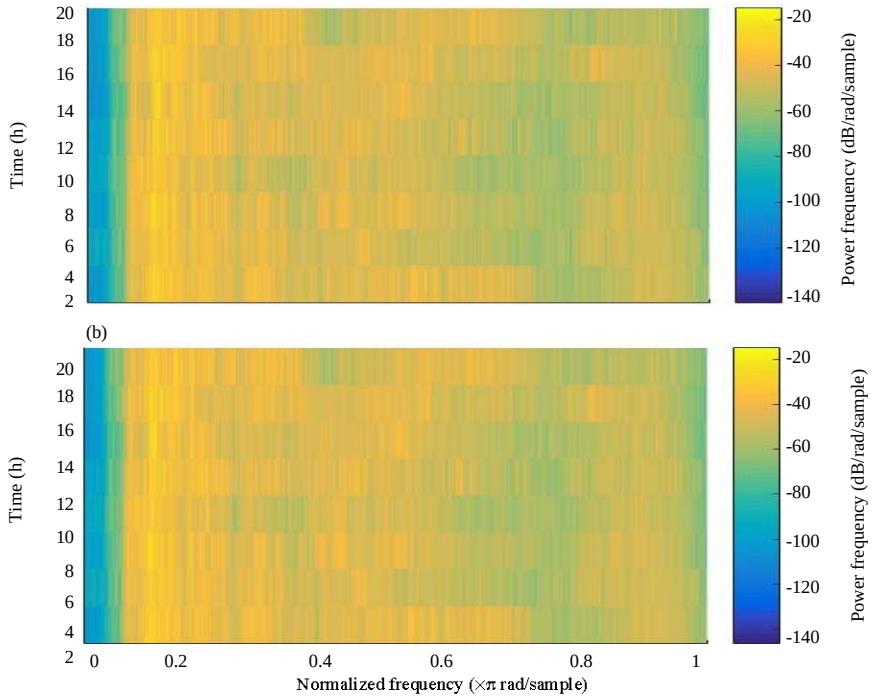

Fig. 5: Spectrogram of cover and stego speech signal for message of 100 bytes

Table 1: Percentage Difference in the cover with different message size

Message size (bytes)	Difference (%)
60	0.25146
100	0.28708
200	0.36312
500	0.63125
1000	1.04850
2000	1.83540
3750	3.32920

Table 2: SNR in the cover with different message size

Message size (bytes)	SNR
60	81.2666
100	80.6911
200	79.6707
500	77.2692
1000	75.0654
2000	72.6339
3750	70.0479

Table 3: PSNR values for different message size

Message size (bytes)	PSNR
60	116.3043
100	115.7289
200	114.7084
500	112.3070
1000	110.1031
2000	107.6717
3750	105.0856

between the receivers and senders, therefore, the channels of communications used by the sender and the receiver are trusted. For all the keys that used in the chaotic maps exchange it by used the Diffie Hellman exchange algorithm and it is determine the value of security and confidentiality.

Table 4: MSE in the cover with different message size

Message size (bytes)	MSE
60	2.3419e-12
100	2.6737e-12
200	3.3819e-12
500	5.879e-12
1000	9.7653e-12
2000	1.7094e-11
3750	3.1005e-11

CONCLUSION

In this research, we have presented a complete "Quantum One-Time Pad" (QOTP) encryption and steganography system based on chaotic maps algorithms including all software necessary to complete practical communication. This is first time combine between steganography system and quantum encryption where in this model, the Least Significant Bit (LSB) responsible for embedding the secret message into speech signal while "Quantum One-Time Pad" (QOTP) is responsible for encrypting and decrypting the stego-specch. This model is robust because extracting data without knowing the architecture of the proposed technique and extracting data is difficult because all the classical data convert it to quantum bits (Qubits). Where the eavesdropper cannot get the information from the cover speech signal he still could not read the secret message because it is in the form of quantum ciphertext.

RECOMMENDATIONS

The experimental result showed the efficiency of the hybrid model proposed. For steganography, the chaotic maps give us high random sequences. Thus, it will increase the complexity of system. For encryption, the quantum key that used in quantum one-time pad algorithm gives us high privacy based on quantum laws. Furthermore, the final results of the ratio of the signals to noise, ratio of the peak signal to noise and mean squared error indicate that the stego-speech has high quality and the hybrid model system is strong.

REFERENCES

Alwahbani, S.M.H. and H.T.I. Elshoush, 2016. Chaos-Based Audio Steganography and Cryptography Using LSB Method and One-Time Pad. In: Proceedings of SAI Intelligent Systems Conference (IntelliSys) 2016, Bi, Y., S. Kapoor and R. Bhatia (Eds.). Springer, Berlin, Germany, ISBN:978-3-319-56991-8, pp: 755-768.

Bennett, C.H. and G. Brassard, 2014. Quantum cryptography: Public key distribution and coin tossing. Theor. Comput. Sci., 560: 7-11.

Boykin, P.O. and V. Roychowdhury, 2003. Optimal encryption of quantum bits. Phys. Rev. A, Vol. 67,

Busch, P., T. Heinonen and P. Lahti, 2007. Heisenberg's uncertainty principle. Phys. Rep., 452: 155-176.

Chirikov, B.V., 1971. Research concerning the theory of non-linear resonance and stochasticity. CM-P00100691, CERN Library, Geneva, Switzerland. http://inspirehep.net/record/898561/files/CM-P00100691.pdf.

Ismael, H.A. and S.B. Sadkhan, 2017. Securityenhancement of speech scrambling using triple Chaotic Maps. Proceedings of the 2017 Annual Conference on New Trends in Information and Communications Technology Applications (NTICT'17), March 7-9, 2017, IEEE, Baghdad, Iraq, ISBN:978-1-5386-2963-5, pp: 132-137.

Johnson, N.F. and S. Jajodia, 1998. Exploring steganography: Seeing the unseen. Computer, 31: 26-34.

Karthikeyan, B., A.C. Kosaraju and S. Gupta, 2016. Enhanced security in steganography using encryption and quick response code. Proceedings of the International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET'16), March 23-25, 2016, IEEE, Chennai, India, ISBN:978-1-4673-9339-3, pp: 2308-2312.

Krishnan, S. and M.S. Abdullah, 2016. Enhanced security audio steganography by using higher least significant bit. J. Adv. Res. Comput. Appl., 2: 39-54.

Laskar, S.A. and K. Hemachandran, 2012. High capacity data hiding using LSB steganography and encryption. Int. J. Database Manage. Syst., 4: 57-68.

Pelosi, M.J., G. Kessler and M.S.S. Brown, 2016. One-time pad encryption steganography system. Proceedings of the Annual Conference on Digital Forensics, Security and Law (ADFSL'16), May 25, 2016, Embry-Riddle Aeronautical University, Florida, Arizona, USA., pp: 130-154.

Pierre, B., Y. Pomeau and C. Vidal, 1984. Order within Chaos. Wiley and Sons, New York, USA.,.

Pund-Dange, S. and C.G. Desai, 2015. Secured data communication system using RSA with mersenne primes and Steganography. Proceedings of the 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom'15), March 11-13, 2015, IEEE, New Delhi, India, ISBN:978-9-3805-4415-1, pp: 1306-1310.

Ren-Er, Y., Z. Zhiwei, T. Shun and D. Shilei, 2014. Image steganography combined with DES encryption pre-processing. Proceedings of the 2014 16th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA'14), January 10-11, 2014, IEEE, Zhangjiajie, China, ISBN:978-1-4799-3435-5, pp: 323-326.

Saini, J.K. and H.K. Verma, 2013. A hybrid approach for image security by combining encryption and steganography. Processings of the 2nd International Conference on Image Information (ICIIP'13), December 9-11, 2013, IEEE, Shimla, India, ISBN:978-1-4673-6099-9, pp: 607-611.

Satar, S.D.M., N.A. Hamid, F. Ghazali, R. Muda and M. Mamat *et al*., 2016. Secure image steganography using encryption algorithm. Proceedings of the Annual International Conference on Intelligent Computing, Computer Science and Information Systems (ICCSIS'16), April 28-29, 2016, Hotel Mercure Pattaya Ocean Resort, Pattaya, Thailand, pp: 43-46.

Steiner, M., G. Tsudik and M. Waidner, 1996. Diffie-Hellman key distribution extended to group communication. Proceedings of the 3rd ACM Conference on Computer and Communications Security, March 14-15, ACM Press, New Delhi, India, pp: 31-37.

Swain, G. and S.K. Lenka, 2014. Classification of image steganography techniques in spatial domain: A study. Intl. J. Comput. Sci. Eng. Technol., 5: 219-232.