Integration of Hash -Crypto- Steganography for Efficient Security Technique

Saleh Saraireh, Jaafer Al-Saraireh, and Mohammad Saraireh

***Abstract*—**The exchange of data over wired and wireless communication networks is influenced by various security attacks and threats. This issue requires the implementation of secure system to provide confidentiality and data integrity to ensure secure data exchange. In this paper integration between different security algorithms is proposed to satisfy confidentiality and data integrity of the transmitted data.

Data encryption, hashing algorithm and steganography technique are used to protect data transmission over communication channels. The proposed approach combines these techniques together to obtain a secure and strong communication system. The proposed technique provides confidentiality, data integrity; scalability, low complexity and high speed by using a symmetric cryptographic technique namely, filter bank block cipher, DWT based steganography, and MD5 hashing algorithm.

The propose algorithm performance is evaluated and analyzed using different images. Simulation results show that confidentiality and integrity are achieved as reflected from the obtained high peak signal to noise ratio (PSNR) and high perceptual quality of the histogram analysis.

***Keywords*—**Block Cipher, Hashing, Histogram, MD5, steganography.

I. Introduction

With the growth of communication technology and the internet, which facilities the data exchange between the users. The confidential secret data transmission over communication channel has also increased dramatically. To be able to protect secret data transmission over general communication channel. Both cryptography and steganography techniques would be the most useful methods to maintain the security of secret data transmission[1].

Cryptography and Steganography are two techniques used to provide information security, but there are set of differences between these techniques. The cryptography is used to convert readable secret data to unreadable data to provide confidentiality security services. While steganography is used to hide message in other data carrier such as image, text, video and audio to transmit it in a secure manner over the communication network [2][3].

The cryptographic algorithms and protocol can be classified as: symmetric, asymmetric. The shared key in symmetric technique is used to provide the confidentiality service, by converting the blocks or streams of plain text of any size into cipher text which is unreadable [4]. Public and private key are used in asymmetric encryption technique to provide confidentiality for secret data. To provide the transmitted data from any modification or change, the data integrity technique is used [5].

Steganography is one of the security techniques that embedded a message into particular carrier data, such as text, image, audio or video [6]. The main idea is to use multimedia for carrying the encrypted confidential data. Then the stego media is sent to the receiver over a public communication channels. Since the stego media is very similar to the original, unexpected user will not easily notice stego media [1].

The image steganography technique is classified into two domains: image/spatial domain and transform/frequency domain [7]. In image domain technique the message embedded in the intensity of the pixel directly [7]. In transform domain the image is transformed and then secret data is hidden in the image [7].

The images are classified into three groups: Binary (or white and black), Gray Scale, and RGB. In white and black image each bit in the image has one-bit value for pixel. When the value of bit is zero in pixel this represent black, while one value is used for white pixel [7]. In the gray scale image, each pixel in the image is represented by 8 bits. The value for 8 bits ranging from 00000000 to 11111111. A black pixel is represented by 00000000 and white is represented by 11111111.

In the RGB image 24 bits are used to represent the colors. The red color is represented from bit 1 to 8, green color represented from bit 9 to 16, and blue color represented from bit 17 to 24 [7].

The hashing algorithms are used to provide the data integrity security service. These algorithms are one-way functions that compute the hash value of fixed size to input message of variable length. Hash function $h = H(m)$, computed hash value h for a variable length block of message m as input.

The structure of this paper consist the following sections. In section II the literature and related work are presented. Section III introduces the methodology and the proposed system the

Saleh Saraireh is with the Communication Engineering Department, Boulder, AL – Hussien Bin Talal University, Jordan, (corresponding author to provide phone: 00962779741368; fax: 0096232372573; e-mail: saleh.s.saraireh@ahu.edu.jo, saleh_53@yahoo.com).

Jaafer Al-Saraireh, is with the Computer Science Department, Princess Sumaya University for Technology, Amman, 11941 Jordan. (e-mail: j.saraireh@psut.edu.jo).

Mohammad Saraireh is with the Computer Engineering Department, Mutah University, Karak, (e-mail: m_srayreh@mutah.edu.jo).

details. The simulation results and discussion are covered in section IV. Section V presents the conclusion of this research.

II. RELATED WORK

To improve the security of data transmission over a communication channel, a several methods have been proposed [2], [6], [8 – 16]. The ID3v2 tag space was used in a steganography by Galiah and Salman [8] and the message was encrypted by using McEliece cryptosystem. The public key was used in this method and inserted into MP3 file format. This method provides better security for data, but can't provide maximum capacity.

A robust method of encryption and steganography was proposed by EdiKresnha and Mukaromah [9]. The ElGamal encryption technique was used to encrypt confidential messages and then embedded in MP3 by diffused confidential message using the spectrum spread technique.

The AES encryption and MD5 hash function were used by Indrayani et al. [6] to improve the security by using MP3. In this approach the MP3 audio was used as cover media and the confidential data was encrypted by using Advance Encryption Standard (AES) algorithm. The secret key was processed using MD5 one-way hash function.

Goudar et al. design a new system to use the TCP/IP header as a stenographic carrier for embedded confidential data [10]. An encryption based of DNA cryptography and steganography was proposed by Mathew [11]. This approach increases the confidential for a sensitive message by providing multilayer security. The secret data encoded to DNA bases, then DNA based AES algorithm was carried out on it. The result of the encryption was embedded in other DNA sequence. A triple layer security was implemented in this method.

To achieve double layer of security a hybrid method was proposed by Hamed et al. [12]. In this approach the secret data converted to DNA format and then applied playfair as classical encryption technique. The encrypted data were embedded in DNA by using LSB technique. In Siddaramappa and Ramesh approach [13], the secret data are converted into DNA bases, then the DNA harmonizing rule applies to DNA based form of data as well as the key. Then the XOR operation is performed between the binary form of the key and data.

In [2] a new technique was proposed to secure image steganography, by using encryption and hash function. This approach uses RSA algorithm and Diffie-Hellman to provide data security. The secret data have been embedded by using LSB stenography.

The RSA encryption algorithm with the LSB steganography method was proposed by [14]. This algorithm was used to encrypt secret messages and then embedded encrypted message with suitable image from the user's library. Therefor; hidden secret message can't be detected through steg-analysis tools.

Masud et al. [15] approach was proposed a novel method that utilized LSB by using a private key. The cover image in this approach is split into Red, Green and Blue matrices and one dimensional array of bit streams of the secret key is generated. Moreover, the Red matrix and the converted secret key are used to make the decision in order to replace the secret data into Blue or Green matrices. To extract the secret data the reverse process is employed.

All previous literature did not consider data integrity service. Data integrity is one of the most important security services that should be satisfied and examined. The paper comes to satisfy the confidentiality and data integrity services.

III. THE PROPOSE APPROACH

It is based on steganography and symmetric encryption techniques to provide the confidentiality, while the hashing algorithm is used to provide the data integrity. To achieve confidentiality, the secret data is encrypted and then embedded through a particular cover object. Furthermore, the data integrity has been implemented by using a hashing algorithm to obtain a hash value for the secret message.

In Figure 1, the flow chart of the proposed approach is presented. The proposed technique contains encryption, hashing and embedding techniques. These operations incorporate to increase the efficiency of the system security. The filter bank symmetric key over finite field GF (2^8) is employed in the encryption process [18]. This cipher is a scalable block cipher, where variable key length and variable plaintext can be used, at the same time; its complexity is less than the complexity of other block cipher.

The hashing process is executed by using message digest algorithm (MD5) which is a hash function that aims to generate 128-bits hash value and it is considered as a fast hashing algorithm [19]. The embedding process of the encrypted data into a cover image is done by employing the discrete wavelet transforms (DWT) based steganography.

The block diagram of a transmitter in the proposed approach is presented in Figure 2; it consists of the following procedures:

Step 1 (generation of hash value): using MD5 hashing function to generate the hash value of the secret message. One MD5 operations is shown in Figure 3. It consists of 64 rounds of these operations, where F is a nonlinear function, $<<<$ denotes a left bit rotation, and $\boxplus$ denotes addition modulo 2^{32}. MD5 processes a variable input string to generate 128 - bit hash value.

Step 2 (concatenation of secret data with hash value): the hash value generated from the MD5 algorithm is concatenated with the secret message to produce the concatenated data.

Step 3 (encryption of the concatenated data): filter bank block cipher with key is used to encrypt the concatenated data, where the analysis filter bank is used to carry out the encryption process.

Step 4 (Embedding the encrypted data to generate the stego image): using DWT based steganography to carry out the embedding or hiding process. The embedding process hides the encrypted data into a particular cover image using

Haar wavelet. In this case, the spatial domain is converted into a frequency domain, where the image is decomposed into the following sub-bands coefficients, namely; horizontal detail, diagonal detail, vertical detail and approximation, then, the encrypted data are embedded into diagonal detail coefficients and vertical detail coefficients.

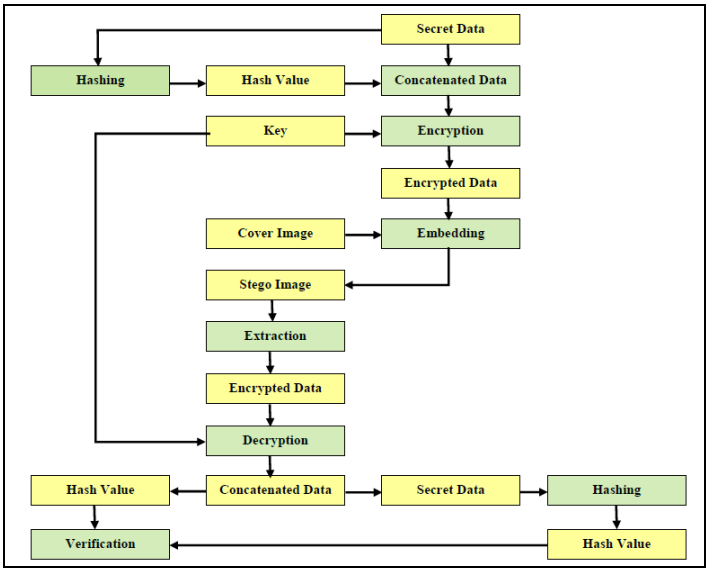

Fig. 1 Flow chart of the proposed approach

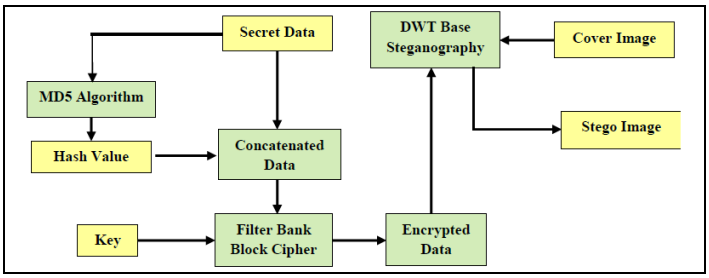

Fig. 2 Transmitter Block Diagram

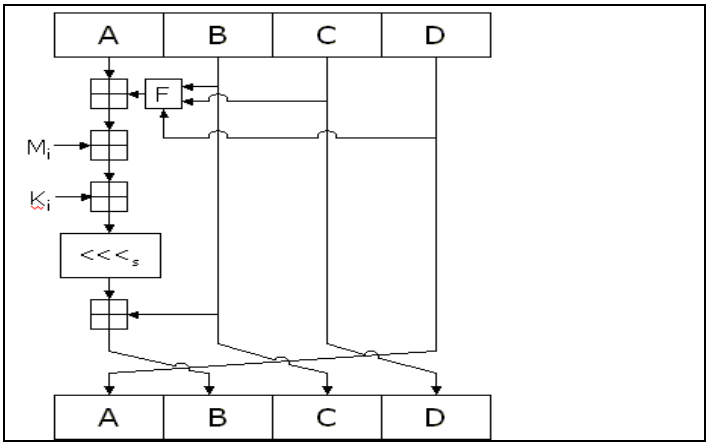

Fig. 3 MD5 Hashing Algorithm

The receiver block diagram in the proposed algorithm is presented in Figure 4. It consists of the following procedures:

Step 1 (Extracting the encrypted data from the stego image): using DWT based steganography to extract the encrypted data from the stego image, where it can be retrieved from vertical detail coefficients and diagonal detail coefficients.

Step 2 (Decryption the encrypted data to generate the concatenated data): synthesis filter bank block cipher is used to decrypt the data to generate the concatenated data; the same key used for encryption is used for decryption.

Step 3 (Separating the concatenated data): the concatenated data are separated into secret message and the hash value, so the original secret data is recovered.

Step 4 (Data integrity verification): to examine the data integrity, the retrieved hash value is compared with a hash value generated at the receiver using the MD5 hashing algorithm for the retrieved secret message, if the hash values are the same, then the data integrity is satisfied, otherwise it is not satisfied.

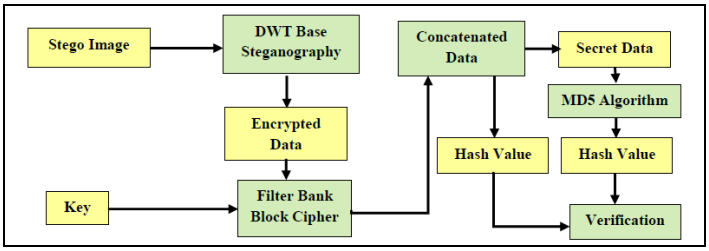

Fig. 4 Receiver Block Diagram

IV. Simulation Results and Discussion

The performance analysis of the proposed approach is discussed in this section. A set of the cover image is employed to examine the performance of the proposed approach. The proposed approach is applied on four grayscale cover images with dimension of 256 × 256 pixels.

$$PSNR = 10\log\left(\frac{M^2}{MES}\right) \quad (1)$$

Where M is the maximum sample number, and MES is the mean square error.

The perceptual quality and similarity between the original images and the stego images is measured through PSNR. PSNR is an important metric to measure such differently.

As summarized in the table (1), the minimum value of PSNR is 63.168 dB, and the average value is 65.527 dB, and the standard deviation is 2.470. Note that, the value of PSNR is a great value; consequently, the corruption due to the embedding of the secret data over the cover image is very low. High PSNR reflects high perceptual quality, accordingly, the human will not distinguish between the stego and the original image, since the human can distinguish the difference between two images if PSNR less than 36dB.

Table 1: PSNR Results

Image	PSNR (dB)
Rose	66.218
Legs	63.168
Bird	64.030
House	68.694

The statistical features of the stego and the cover images can be analyzed and compared by drawing their histograms. To ensure the resistivity of the steganographic technique against the statistical attack, the histogram of stego and its corresponding cover image should not have any significant change. As shown in the Figures 5, 6, 7, and 8, it can be noted that, there is no change of values in terms of pixels and size between the stego and cover images. Accordingly, it is very difficult for the attackers to detect the difference between the original images and the stego images. This means that, the proposed algorithm improves the protection of secret data and establishes a secure communication channel.

The proposed algorithm avoids the following attacks:

1) Collision attack: the proposed algorithm avoids the collision attack by using the MD5 hash function which is a collision resistance algorithm.
2) Visual attacks: it has been avoided by using DWT based steganography, this was proved from the histograms and PSNR analysis.
3) Integrity: the proposed algorithm uses the MD5 hash function; it protects the data from any alteration during the transmission, and a verification process is done at the receiver to ensure the data integrity.

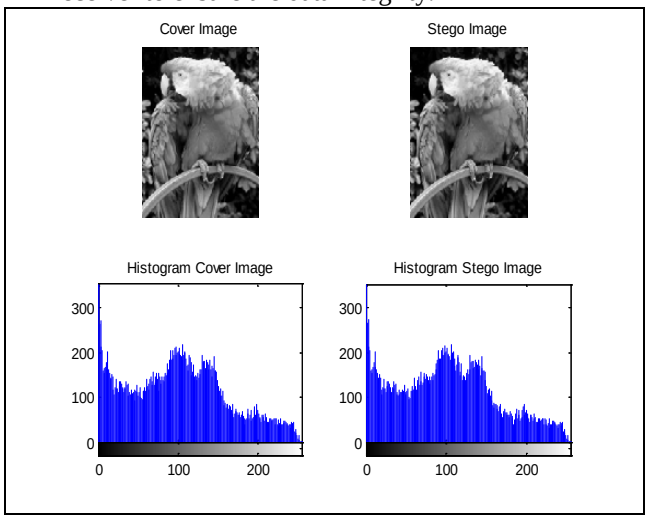

Fig. 5 Histogram analysis of bird cover image.

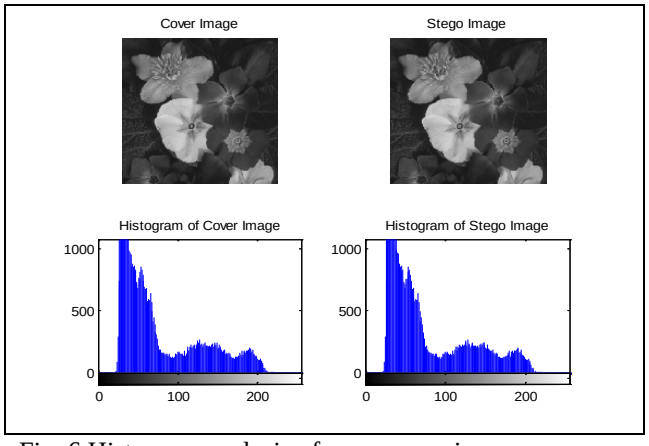

Fig. 6 Histogram analysis of roses cover image.

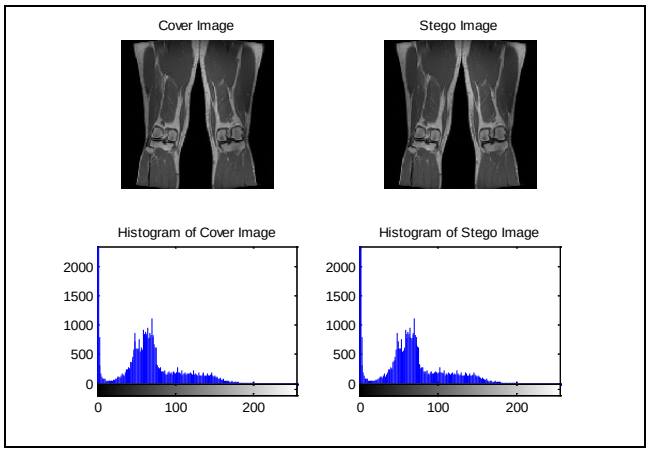

Fig. 7 Histogram analysis of legs cover image.

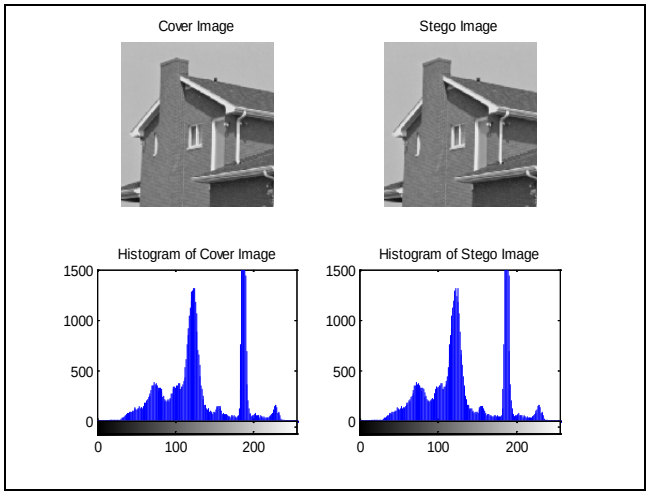

Fig. 8 Histogram analysis of house cover image.

V. Conclusion

The proposed algorithm is a mutual security algorithm; it combines many security techniques to obtain a robust algorithm that satisfies confidentiality and data integrity. This mutual security algorithm uses DWT based steganography and symmetric filter bank block cipher to improve the confidentiality, where the filter bank block cipher encrypts the secret data and DWT based steganography hides the encrypted data into a cover image.

MD5 hash function is employed in this paper to assure the data integrity. The results obtained in terms of PSNR values and histograms for a set of cover images reflect the effective performance of the proposed algorithm. The PSNR values and histograms guarantee the invisibility of the hidden data over the cover images; this ensures data protection and the resistivity of the algorithm against threats and attacks.

References

[1] H.-H. Chang, Y.-C. Chou, C.-C. Tseng, and T. K. Shih, "A High Payload Steganography Scheme for Color Images Based on BTC and Hybrid Strategy," *J. Comput.*, vol. 26, no. 2, pp. 46–55, 2015.

[2] E. P. Singh and E. P. S. Saini, "A Novel Approach to Robust and Secure Image Steganography Based on Hash and Encryption," *Int. J. Eng. Sci. Res. Technol.*, vol. 5, no. 3, pp. 194–201, 2016.

[3] H. Kayarkar and S. Sanyal, "A Survey on Various Data Hiding Techniques and their Comparative Analysis," *ACTA Tech. Corviniensis*, vol. 5, no. 3, pp. 35–40, 2012.

[4] J. Al-Saraireh, "HVM: A method for improving the performance of executing SQL-query over encrypted database," *J. Theor. Appl. Inf. Technol.*, vol. 95, no. 14, pp. 3394–3402, 2017.

[5] J. Al-Saraireh, "An efficient approach for query processing over encrypted database," *J. Comput. Sci.*, vol. 13, no. 10, pp. 548–557, 2017.

[6] R. Indrayani, H. A. Nugroho, R. Hidayat, and I. Pratama, "Increasing the security of MP3 steganography using AES Encryption and MD5 hash function," in *Proceedings - 2016 2nd International Conference on Science and Technology-Computer, ICST 2016*, 2017, pp. 129–132.

[7] R. K. Sheth and R. M. Tank, "Image Steganography Techniques," *Int. J. Comput. Eng. Sci.*, vol. 1, no. 2, pp. 10–15, 2015.

[8] A. Galih Salman and B. Kanigoro, "Steganography Application Program Using the ID3v2 in the MP3 Audio File on Mobile Phone," *J. Comput. Sci.*, vol. 10, no. 7, pp. 1249–1252, 2014.

[9] P. E. Kresnha and A. Mukaromah, "A Robust Method of Encryption and Steganography Using ElGamal and Spread Spectrum Technique Based on MP3 Audio File," in *Proceeding Conference on Applied Electromagnetic Technology (AEMT)*, 2014, pp. 11–15.

[10] R. M. Goudar, P. N. Patil, A. G. Meshram, S. M. Yewale, and A. V Fegade, "Secure Data Transmission by using Steganography," *Inf. Knowl. Manag.*, vol. 2, no. 1, pp. 1–7, 2012.

[11] S. Mathew, "An Encryption based on DNA cryptography and Steganography," in *2017 International conference of Electronics, Communication and Aerospace Technology (ICECA)*, 2017, pp. 162–167.

[12] G. Hamed, M. Marey, S. A. El-Sayed, and M. F. Tolba, "Hybrid technique for steganography-based on DNA with n-bits binary coding rule," in *Proceedings of the 2015 7th International Conference of Soft Computing and Pattern Recognition, SoCPaR 2015*, 2016, pp. 95–102.

[13] V. Siddaramappa and K. B. Ramesh, "Cryptography and bioinformatics techniques for secure information transmission over insecure channels," in *Proceedings of the 2015 International Conference on Applied and Theoretical Computing and Communication Technology, iCATccT 2015*, 2016, pp. 137–139.

[14] M. Juneja and P. S. Sandhu, "Designing of robust image steganography technique based on LSB insertion and encryption," in *ARTCom 2009 - International Conference on Advances in Recent Technologies in Communication and Computing*, 2009, pp. 302–305.

[15] S. M. Masud Karim, M. S. Rahman, and M. I. Hossain, "A new approach for LSB based image steganography using secret key," in *14th International Conference on Computer and Information Technology, ICCIT 2011*, 2011, pp. 286–291.

[16] S. S. Saraireh, and M. S. Saraireh, "Filter Bank Block Cipher and LSB Based Steganography for Secure Data Exchange," *Int. J. Commun. Antenna Propag.*, vol. 7, no. 1, p. 1, Feb. 2017.

[17] S. Saraireh, "A SECURE DATA COMMUNICATION SYSTEM USING CRYPTOGRAPHY AND STEGANOGRAPHY," *Int. J. Comput. Networks Commun.*, vol. 5, no. 3, 2013.

[18] S. Saraireh and M. Benaissa, "A Scalable Block Cipher Design using Filter Banks and Lifting over Finite Fields" In IEEE International Conference on Communications (ICC), 2009, Dresden, Germany.

[19] Y. Sasaki and L. Wang, "Improved Single-Key Distinguisher on HMAC-MD5 and Key Recovery Attacks on Sandwich-MAC-MD5," International Conference on Selected Areas in Cryptography, Springer, Berlin, Heidelberg, 2014, pp. 493–512.

Saleh Saraireh is Associate Professor at Al – Hussien bin Talal University in Jordan. I got the PhD from the University of Sheffield, UK, in communication engineering. Also I hold a Master degree in Communication Engineering and a Bachelor degree in electrical engineering from Mutah University, Jordan. My research area related to wireless communication, digital signal processing and cryptography and security.

Jaafer Al Saraireh is Associate Professor of Computer Science at Princess Sumaya University for Technology (PSUT), Amman, Jordan. He received his BSc in Computer Science from Mu'tah University in 1994, MSc in Computer Science from University of Jordan in 2002, and PhD in Computer Science from Anglia Ruskin University, United Kingdom in 2007. His research interests include computer networks security, database security and mobile network security.

Mohammad Saraireh is a professor at the Faculty of Engineering, Computer Engineering Department, Mutah University, Jordan. His area of expertise is in quality of service in wireless computer networks and computer Networks, artificial intelligence applied to computer networks, communication systems, security and network security.