Enhancing Medical Data Security via Combining Elliptic Curve Cryptography and Image Steganography

Eshraq S. Bin Hureib[1†] and Prof. Adnan A. Gutub [2††]

University of Umm Al-Qura, University of Umm Al-Qura, Makkah, Saudi Arabia

Abstract
This paper explores methods through which secret information is encrypted then and hided so as to increase the level of security in medical health data from being hacked[19]. This is done through combining two method Elliptic curve cryptography and image steganography. On first stage, text would be encrypted through using ECC. On second stage, steganography would be used so as to conceal the text inside an image [2, 24]. Selecting ECC, which is an algebraic structure of elliptic curves over finite fields, is considered as being a desired choice for being public key [12] [16]. Furthermore, it can be used in many type of media they use it in medical record system and in field such as CT scan, and MRI scan [1]. Selecting Image Steganography, which is a technique that helps many organizations, institutions to hide the encrypted information, obscures privacy information from a person which is not authorized to get the access of that of it. The technique can be used by any person, group of persons or organization to hide and protect their important business information or nation's secrets, or laboratory secrets or the important defines information.

Key words:
Elliptic curve cryptography, Image Steganography, encryption, hiding, information.

1. Introduction

In the fast moving and high technology world of today, protection, security and hiding of private and secret information have become an important part of everyone's life [3]. In this paper an attempt is made to combine the technique of image steganography with the curve cryptography to hide and protect the secret message. This attempt can ensure more realistic, reliable and high standard safety, security and privacy to the secret messages and the codes [11]. For the aim of encryption data, ECC is used as an effective alternative for traditional crypto systems such as AES, DES, and RSA. Using of ECC is done because of its pros as it needs less computational power, low level of memory and modest network connectivity, and low ability in communication bandwidth [17]. In this study, the elliptic curve over characteristic 2 (binary finite field), GF (2m) will be examined in relation to encryption of information so as to strengthen the security of medical data [12, 14, 16]. Nonetheless, encryption the information might not be sufficient to protect and secure the data transferred between two recipients. This is due to the parallel development in the ways of encryption and decryption the data [16]. As such, no matter the level of development in the ways of encryption, the decryption science would develop at the same level.

Therefore, it might be a logical step trying to hide the encrypted information so no person can detect the encrypted information as indicated in a number of studies [13] [18] [5]. Based on this analysis, the implementation of image steganography, which is adopted for hiding the data, should be done in tandem with ECC [9]. Likewise, developing secure and robust steganography way that is immune against detectability needs integrating the two processes of encrypting and hiding the data. As a result, both methods of cryptography (ECC) and steganography should be recognized.

Therefore, there is a requirement to investigate in one process the methods in which the data should be encrypted and hided. The outline of this study would be as follows: section 2 highlights the main differences between encryption method of ECC and hiding method of image steganography. section 3 would examine theoretical background. This includes exploring ECC in subsection 3.1. followed by a detailed examination of steganography in subsection 3.2. Then, section 4 provides a detailed description the idea, procedure, algorithm and implementation tests. Section 5 suggests potential improvements to the literature based on the findings of this study. Finally, section 6 summarizes of the whole research.

2. Differences between Steganography and Cryptography

Table 1: Steganography and Cryptography

Basis	Steganography	Cryptography
Basic	It is a form of cover writing	It is a form of secret writing
Objective	To hide the presence of an information	To protect and secure the data
Easy and popular	Steganography is not easy to use and is not much popular	Cryptography is easy to use and is much popular

Manuscript received August 5, 2020
Manuscript revised August 20, 2020

Alternations	The main message is not altered	The main message is altered
Feasibility	Can be stored to hide information of all types such as text, images, videos, audios, etc	Only text messages can be protected

3. Theoretical Background

This section explores the two methods of ECC and image steganography followed in this research.

3.1 Elliptic Curve Cryptography

Elliptic curve cryptography is a technique to protect the secret data through the use of keys. ECC is based on the theory of Elliptic curve [14]. The Elliptic curve theory is used to make smaller and faster effective keys of cryptography [16]. It provides better security and protection the secret protected data. Elliptic curve cryptography uses the elliptic curves to design the elliptic keys [8]. Elliptic curve can be defined by equation:

$$Y2 = X3 + AX + B \quad (1)$$

This coded and equated data is encrypted by only using the private key which private key holder possesses.

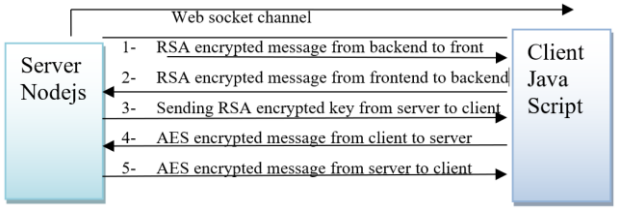

Fig. 1 Public key and Private key generated

Fig. 1. Shows the example of how public and private keys are generated for the client and the server. Based on ideas of [25], it is how the encrypted client-server communication takes place in the technique of cryptography.

3.2 Steganography

Steganography is the technique in which the secret information or the secret data is hided in such a way that its presence cannot be detected. This is the reason why steganography is known as covered writing [2]. The purpose of steganography is not just to protect the protection but also to hide it in such a way that no one can recognize or find out the presence of the hidden secret information. The main aim of this technique or technology is to hide the presence of any of the hidden information [6].

The person who is not authorized to get the access of the information should not even know that if any hidden information is present or not [10]. Message, carrier and the password are the three main components of the steganography. The message is the secret text, image or the video or the audio that had to be protected through the technique of steganography[21]. The carrier is the path or the medium through which the secret and the covered message is transferred. The password is the stego-key through which the secret data is protected and can be disclosed.

Model of steganography as shown in Fig. 2.

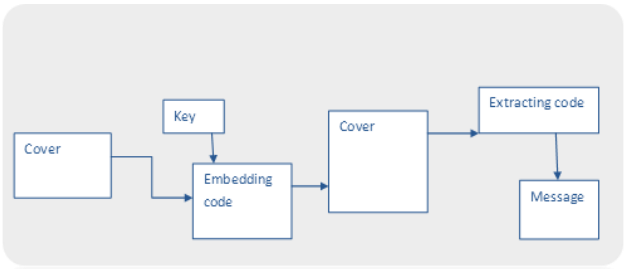

Fig. 2 Model of Steganography

3.2.1 Steganography is Categorized into Three types:

(i) Text: this is the most commonly used type of steganography technique [13].

(ii) Audio/video: This type of steganography is the most difficult and complex type of steganography [22]. Under this secret message is hidden in an audio or the visual files. The audio/video steganography too has its various types such as Least Significant Bit coding, Parity coding, etc. [18].

(iii) Image: The most widely used method of Steganography is the images as the cover page. Images are formed by collection of various pixels that contains the different light intensives [21]. Most widely the images of eight bit and twenty four bit pixels are used. The image steganography too has its various types such as least significant bit insertion, encrypt and scatter, masking and filtering, etc.[7, 18].

Among the three types of steganography the most common and popular steganography used it the Image steganography [8]. Under the image steganography the important and the secret information is hided under the images so that the presence of the original information and data and be hidden. If someone got to know about the

carrier, cover or the medium, the technique of steganography gets failed there only [6]. The image steganography is future divided into spatial domain image steganography and frequency domain image steganography. Steganography in which the data is directly embedded and hidden into images is called spatial domain image steganography [9]. It uses the technique of Least Significant Bit. This method is much easy than the other method of steganography [18]. Technique in which the frequency of the image is changed and then data is embedded in it is called frequency domain steganography [1]. Frequency domain steganography is much safer than the spatial steganography. This technique is used to overcome the loss of image in case of the image compression or image cropping. For this, three techniques are used namely Fat Fourier Transfer, Discrete Cosine transfer and Discrete wavelet transform technique [9].

4. Detailed description of the studied work: Combining elliptic curve cryptography with Image steganography

4.1 The Idea: The process of Encryption through ECC and Hiding through Steganography

Encrypting and Hiding Data Process Fig. 3. this process starts through selecting sensitive then ECC encryption will be applied so as to convert encrypt text to binary. On a similar vein, image cover input will be converting into binary. Then, stego embedding would take place followed by stego cover.

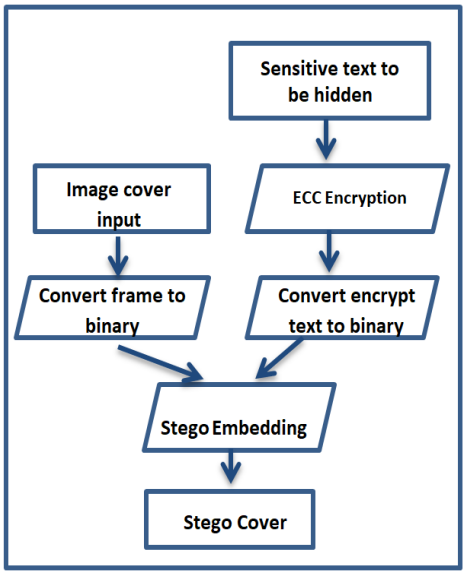

Fig. 3 Encrypting and hiding data

After that Retrieving Data Process Fig. 4.will take place through extracting cypher text and then ECC. decryption should take place in order to get the original sensitive text.

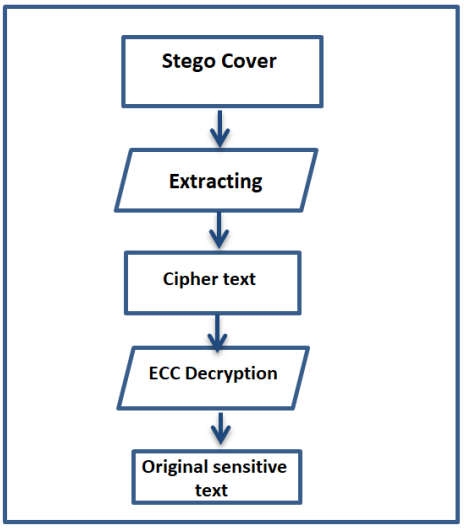

Fig. 4 Retrieving Data Process

4.2 Procedure

Given below are the steps about how the technique of image steganography has been combined with the technique of ECC to form a robust and a much safer technique of protecting the secret and private data. In details, these steps are as follows: (i)To start and develop a powerful technique to protect, secure and hide the secret data and information, we require secret information. Let us take there the secret data or message as the English word “Hello”, (ii) In the next step the technique of image steganography will be used to provide the cover to our secret message. Cover is an image that helps to hide the secret data. Here to protect out secret data “Hello ”, the cover used is the “ex.ipg”, (iii) In the next step to undertake the secrecy and protection steps the secret message is converted into the binary, (iv) Under the next step the key pairs are generated. G=here say, V A and V B , (v) The two senders here are sender A and the sender B ,(vi) Sender A encrypt the message using ECC or Elliptical Curve Cryptography technique and use key V A, (vii)Using embedding technique of Least Significant Bit into the cover, (viii) Image by stego gets created, (ix) Novel technique of key distribution is used here, and (x) For implementing this IntelliJ IDEA environment are used. This method ensures the proper protection of data and information by using the techniques of elliptical curve cryptography and steganography [10, 17].

4.3 Implementation

This security system propose high level security for sensitive medical records has been designed and implemented in Java using IntelliJ IDEA to perform this system.

Java was chosen because Java language is a high-level programming language. It works on all the most important operating systems, such as Windows, Linux, and Mac. It is considered one of the most popular and powerful programming languages ever. It has an integrated platform, it is also an oriented objective language has a long and rich history and provides many built-in libraries in various fields as we use ECIES from BouncyCastle library for implementing our ECC and keys generation and distributing which is very strong library[2]. In addition to its simple and security language. As for IntelliJ IDEA was chosen because Integrated development environment and it was developed by JetBrainsso company. it provides comprehensive facilities for programmers and helps them in developing software. Therefore, it consists of a text editing tool for writing source code for programs, interpreter, automating program building tools, as it usually contains a program to search for errors and problems or the so-called debugger. The objective of this implementation is to examine this two layers security system as well as test various conditions to enhance this important field of academic research .

The proposed system starts with the interface can be observed in Fig. 5. giving the user two choices enter data or extract the data.

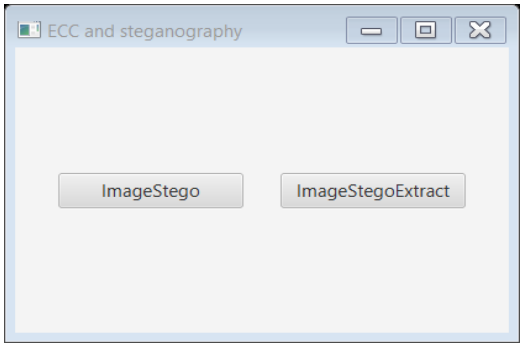

Fig. 5 Interface of proposed system

If the user chose entering data which is here (Image stego) will get new window. This interface as observed in Fig. 6.

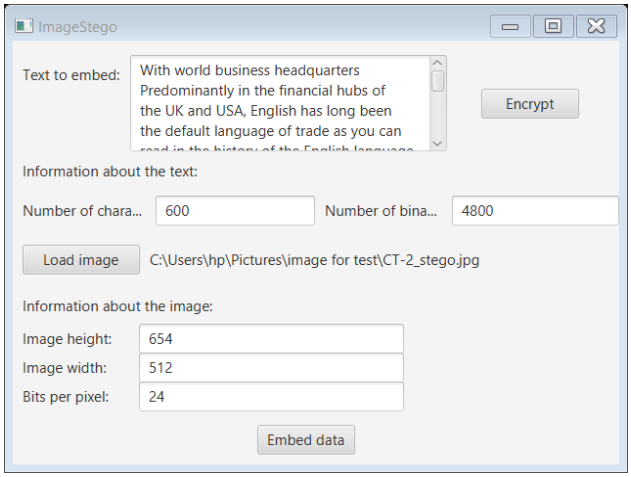

Fig. 6 Interface to entering sensitive data

The system testing used the stego cover as an image cover of 654x512 pixels as the size of the image. And use the fixed secret text data message Text with almost 600 characters and 101 words. Accordingly, when user entering the sensitive text information. In this layer, which is the first layer. The text is encrypted using the elliptic curve cryptography so when the user clicks on Encrypt button, method encrypt Button is called [12]. In this method first we generate Key Pair and save public and private key (because we will need private key later when we do decrypting) and then with Cipher class methods do the encryption with public key. Then user should click load image button, Load Image method is simple method that use File Chooser class (so we can choose an image) and makes a copy of original image with suffix "_stego" and print image absolute path to window so we can use path to image to do steganography. The second layer start when the user click Embed data it will takes generated cipher text and embed it to image using the least significant bits (LSB) image based steganography in our original system. And will get copy of an image that has suffix "stego"[2]

To retrieve the sensitive text or data as shown in the interface Fig. 7. The user will choose stego image then click on button Decrypt text, method decrypt Button is called. In this method we call method decode that loop through array byte of image and gets least significant bit in every bytes. We decode message from image so we can convert it to array of bytes. And with Cipher class methods and private key we decrypt cipher text from image and print it to a text area.

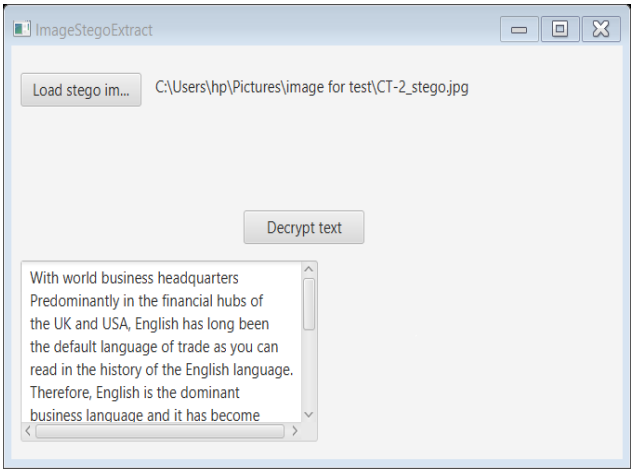

Fig. 7 Retrieve the sensitive text or data

4.4 Results Analysis & Comparison

The secret data is given from people authorized to enter the information or diagnosis about patients. The information given are required to be encrypted by hiding them inside the image frames like (CT scan , MRI or X-ray). For this purpose 15 different images are chosen. The classification is elaborated as per table 2 for these 15 images. We can see the results in Table 2. The table gives the results for all selected images.

The PSNR is computed using formulae

$$PSNR = 10\, log_{10}\left(\frac{MAX^2}{MSE}\right) \quad (2)$$

where

$$\text{MSE} = \frac{1}{M*N}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}(C(X,Y) - S(X,Y))^2 \quad [26]$$

Table: 2 Results of PSNR With ECC and RSA

Image	Type	Image height	Image width	PSNR	
				ECC	RSA
1	CT-Scan	1000	100	77.513	75.639
2	CT-Scan	654	512	72.872	70.946
3	CT-Scan	594	541	72.387	70.598
4	CT-Scan	840	918	76.302	74.397
5	CT-Scan	512	512	71.583	69.871
6	MRI	808	717	75.075	73.382
7	MRI	1600	1600	81.652	79.775
8	MRI	748	617	73.948	72.21
9	MRI	320	320	67.251	65.628
10	MRI	256	256	65.562	63.973
11	X-RAY	2200	2200	84.028	82.336
12	X-RAY	1693	56	77.158	75.46
13	X-RAY	756	965	76.039	74.197
14	X-RAY	768	1024	76.394	74.518
15	X-RAY	630	414	71.557	69.768

The results shown in table 2 are based on comparing two techniques (i.e. ECC and RSA) when conducting PSNR. From table 1, it can be shown that values of PSNR with ECC technique are better than PSNR values with RSA. The quality of PSNR with ECC surpassed its quality with RSA in three different types of images (CT-Scan, MRI, and X-ray) [15]. The higher values of PSNR when using ECC is always higher than the values of PSNR when using RSA. This indicates that hard steganography predictability with ECC is more secure than with RSA.

The testing for security hides the sensitive information by changing the LSB of the image frame and thus text information gets concealed in images. This changes the bits as per the choices made as elaborated in Table 2. We find that PSNR for RSA is always lower compared to ECC method. For bigger file size like image number 7 where image height is 1600 and image width is also 1600, the PSNR values are quite large 81.65 for ECC and 79.78 for RSA, and the difference between two methods is just (81.65 – 79.78)*100/ 81.65 = 2.29%.

For image number 11, of size 2200 * 2200, the PSNR values are quite large 84.03 for ECC and 82.34 for RSA, and the difference between two methods is just (84.03 – 82.34)*100/ 84.03 = 2.01%.

While when the file size is small , like in image number 10, of size 256*256 , the PSNR values are quite less 65.56 for ECC and 63.97 for RSA, and the difference between two methods is just (65.56 – 63.97)*100/ 65.56 = 2.53%.

Plot of PSNR by RSA method is plotted against (Height* Width) of the image frame is shown in Fig. 7. It is seen that PSNR value rises with increase in image area (Height * Width) , similar to the trend seen in ECC method.

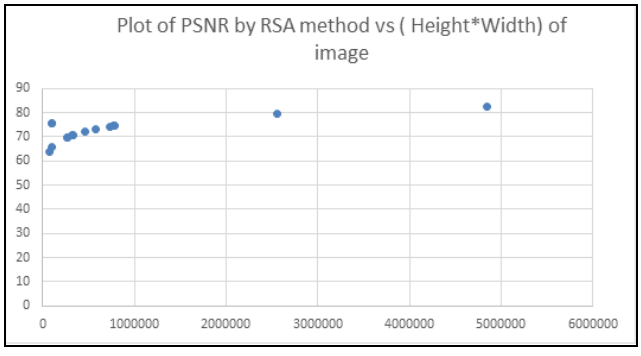

Fig. 7 PSNR value

The histogram for PSNR computed as shown in table 2 is given in Fig. 8. From the histogram it can be seen that EEC method always gives higher value of PSNR in comparing with the RSA one as seen the results of 15 image sizes analyzed and presented in Table 2.

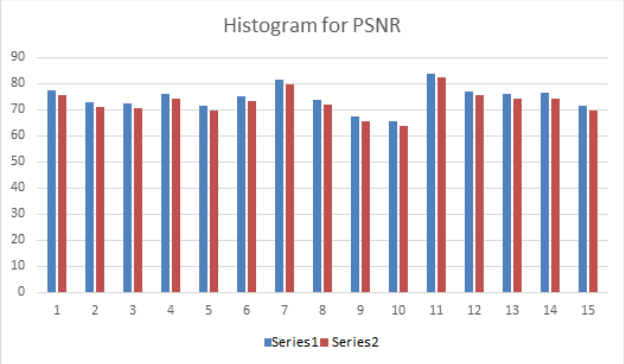

Fig. 8 PSNR for

a) Series1 which is PSNR by ECC method b) Series2 which is PSNR by RSA method

PSNR (Peak Signal to Noise Ratio) is computed using formula:

Generating the ciphertext is representing reversing the stego layer process. Then, the ciphertext needs the secret key as inputs to the reverse RSA crypto layer that decrypts the ciphertext generating back the secret sensitive data message, following Figure 4 the process of retrieving back secret text data. (1) Where MAX refers to the maximum intensity of the given resolution of each pixel, i.e. this MAX value in the images is 255. On the other hand, MSE is defined as the square of the difference (distortion) between the original cover and the stego cover [24]. The findings manifest substantial promising values of security and capacity making image relied as a valid choice over images for PC data cyber security. It is indicated that implementing this security technique as a cover file is providing the user more ability to hide text unpredicted more than the image cover [3]. Furthermore, the security will be more efficient when adopting image as cover through using ECC than using RSA in PSNR technique.

After comparing the two methods, it can be deduced that RSA algorithm works effectively when the length of the text is short. However, when the length of the text is long, there is a challenging point related to passwords key transformation problem [18]. Another problem with RSA algorithm in the long text is that keys distribution and keys' secret sharing protocols would constitute predicaments that need fixing [20]. Accordingly, in long texts, using RSA would lead to reducing the performance of the laptop or computer device due to the RSA' complexity. In order to tackle such complexity related to RSA in long texts, it is recommended to adopts cryptography that is light weighted which eloquently deal with such computational complexity and passwords [15].

5. Improvement

It combined two methods (i.e. ECC and image steganography). By doing so, the researcher increases the level of security related to medical health data against hacking threats. These types of buttressing security are best suited to protect various types of information that are very important to the person, group or any medical organization. These techniques can be used by various healthcare organizations to protect the secret information of patients. Apart from this technique is also useful to protect the defense related secret data and information.

Also, this study considered Binary Numbers: Least Significant Bit is the easiest and the popular method or tool to hide the secret messages [18]. It is also a reliable technique because the bandwidth that is used in it is not easy to destroy [4] [5]. Therefore giving and assuring the highest level of safety and security of the secret information.

6. Conclusion

In this research, a model is proposed and is introduced by combining the two techniques of elliptical curve cryptography and steganography. With the use of two techniques, the private and secret information will be encrypted then hided in a much better way than before [1, 17, 20]. This helps both writ and the receiver of the secret information to keep any person who is not authorized to see and get this information to keep away [13, 15, 16]. Any unauthorized person doesn't even get to know about the presence of any information.

Acknowledgments

I would like to thank my supervisor, Prof. Adnan Abdulaziz Gutub, for his unlimited efforts and constructive feedback. I have been extremely lucky to have a supervisor who cared so much about my work, and who responded to my queries so promptly. I would also like to thank all the members of staff at Um-Al-Qura University as well as my peers who supported me when I need them.

Finally, I want to thank my family for their continuous support.

References

[1] Ahmed, D.E. and Khalifa, O.O., 2014, September. Robust and Secure Image Steganography Based on Elliptic Curve Cryptography. In 2014 International Conference on Computer and Communication Engineering (pp. 288-291). IEEE.

[2] AlAssaf, N., AlKazemi, B. and Gutub, A., 2003. Applicable light-weight cryptography to secure medical data in IoT systems. Arabia.

[3] Al-Juaid, N., A Gutub, A. and A Khan, E., 2018. Enhancing PC data security via combining RSA cryptography and video based steganography.

[4] Al-Nazer, A. and Gutub, A., 2009, October. Exploit kashida adding to Arabic e-Text for high capacity steganography. In 2009 Third International Conference on Network and System Security (pp. 447-451). IEEE.

[5] Al-Otaibi, N.A. and Gutub, A.A., 2014, December. Flexible stego-system for hiding text in images of personal computers based on user security priority. In Proceedings of 2014 International Conference on Advanced Engineering Technologies (AET-2014) (pp. 250-256).

[6] Aly, S. and Gutub, A., 2018. Intelligent recognition system for identifying items and pilgrims. NED University Journal of Research, 15(2), pp.17-23.

[7] Cogranne, R., Sedighi, V. and Fridrich, J., 2017, March. Practical strategies for content-adaptive batch steganography and pooled steganalysis. In Acoustics, Speech and Signal Processing (ICASSP), 2017 IEEE International Conference on (pp. 2122-2126). IEEE.

[8] Denemark, T. and Fridrich, J., 2017. Steganography with multiple JPEG images of the same scene. IEEE Transactions on Information Forensics and Security, 12(10), pp.2308-2319.

[9] Denemark, T.D., Boroumand, M. and Fridrich, J., 2016. Steganalysis features for content-adaptive JPEG steganography. IEEE Transactions on Information Forensics and Security, 11(8), pp.1736-1746.

[10] Duan, X., Song, H., Qin, C. and Khan, M.K., 2018. Coverless steganography for digital images based on a generative model. Computers, Materials & Continua, 55(3), pp.483-93.

[11] Feng, B., Lu, W. and Sun, W., 2015. Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture. IEEE Trans. Information Forensics and Security, 10(2), pp.243-255.

[12] Ghouti, L., Ibrahim, M.K. and Gutub, A.A., King Fahd University of Petroleum, 2013. Elliptic polynomial cryptography with secret key embedding. U.S. Patent 8,351,601.

[13] Guo, L., Ni, J., Su, W., Tang, C. and Shi, Y.Q., 2015. Using statistical image model for JPEG steganography: uniform embedding revisited. IEEE Transactions on Information Forensics and Security, 10(12), pp.2669-2680.

[14] Gutub, A. and Alaseri, K., 2019. Hiding Shares of Counting-Based Secret Sharing via Arabic Text Steganography for Personal Usage. Arabian Journal for Science and Engineering, pp.1-26.

[15] Gutub, A., 2006. Fast 160-bits GF (p) elliptic curve crypto hardware of high-radix scalable multipliers. International Arab Journal of Information Technology (IAJIT), 3(4), pp.342-349.

[16] Gutub, A., Ghouti, L., Elarian, Y., Awaideh, S., and Alvi, A., 2010. Utilizing diacritic marks for Arabic text steganography. Kuwait Journal of Science & Engineering (KJSE), 37(1), pp.89-109.

[17] Gutub, A.A., 2007. High speed hardware architecture to compute Galois Fields GF (p) montgomery inversion with scalability features. IET Computers & Digital Techniques, 1(4), pp.389-396.

[18] Gutub, A.A.A., Al-Haidari, F., Al-Kahsah, K.M. and Hamodi, J., 2010. e-Text watermarking: utilizing'Kashida'extensions in Arabic language electronic writing. Journal of Emerging Technologies in Web Intelligence, 2(1), pp.48-55.

[19] Gutub, A.A.A., Ibrahim, M.K. and Al-Somani, T.F., 2007, February. Parallelizing GF (P) elliptic curve cryptography computations for security and speed. In 2007 9th International Symposium on Signal Processing and Its Applications (pp. 1-4). IEEE.

[20] Gutub, A.A.A., Tabakh, A.A., Al-Qahtani, A. and Amin, A., 2013. Serial vs. parallel elliptic curve crypto processor designs. In IADIS International Conference: Applied Computing (pp. 67-74).

[21] Jiang, N., Zhao, N. and Wang, L., 2016. LSB based quantum image steganography algorithm. International Journal of Theoretical Physics, 55(1), pp.107-123.

[22] Mayer, J., Borges, P.V. and Simske, S.J., 2018. Introduction. In Fundamentals and Applications of Hardcopy Communication (pp. 1-5). Springer, Cham.

[23] Parvez, M.T. and Gutub, A.A.A., 2008, December. RGB intensity based variable-bits image steganography. In 2008 IEEE Asia-Pacific Services Computing Conference (pp. 1322-1327). IEEE.

[24] Rahman, M.M., Saha, T.K. and Bhuiyan, M.A.A., 2012. Implementation of RSA algorithm for speech data encryption and decryption. International Journal of Computer Science and Network Security (IJCSNS), 12(3), p.74.

[25] Ramalingam, M. and Isa, N.A.M., 2015. A steganography approach over video images to improve security. Indian Journal of Science and Technology, 8(1), pp.79-86.

[26] Sadek, M.M., Khalifa, A.S. and Mostafa, M.G., 2015. Video steganography: a comprehensive review. Multimedia tools and applications, 74(17), pp.7063-7094.

[27] Szczypiorski, K. and Mazurczyk, W., 2016. Steganography in IEEE 802.11 OFDM symbols. Security and Communication Networks, 9(2), pp.118-129.

[28] Wu, K.C. and Wang, C.M., 2015. Steganography using reversible texture synthesis. IEEE Transactions on Image Processing, 24(1), pp.130-139.

[29] Uchiyama, A., Furukawa, K. and Higurashi, Y., 2012. EPICS channel access using Websocket. Proceedings of PCaPAC2012, Kolkata, India,. URL https://accelconf. web. cern. ch/accelconf/pcapac2012/papers/wecc02. pdf.

Eshraq Bin Hureib is currently a graduate student, pursuing Master of Sciences (MS) degree in Computer Sciences & Engineering from Umm Al Qura University (UQU) . Her MS program at UQU is specialized in the information security track offered by the College of Computer and Information Systems offered at UQU-Makkah Campus, Saudi Arabia, hoping to complete her research and get the MS degree within 2020.

Adnan Gutub is currently working as Professor in Computer Engineering Department specialized in Information and Computer Security within UQU. He received his Ph.D. degree (2002) in Electrical & Computer Engineering from Oregon State University, USA. He had his BS in Electrical Engineering and MS in Computer Engineering both from KFUPM, Saudi Arabia. Adnan's research interests involved optimizing, modeling, simulating, and synthesizing VLSI hardware for crypto and security computer arithmetic operations. He worked on designing efficient integrated circuits for the Montgomery inverse computation in different finite fields. He has some work in modeling architectures for RSA and elliptic curve crypto operations. His current interest in computer security also involved steganography such as image-based steganography and Arabic text steganography. Security also involved steganography such as image-based steganography and Arabic text steganography.