Enhancing Medical Data Security via Combining Elliptic Curve Cryptography with 1-LSB and 2-LSB Image Steganography

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

University of Umm Al-Qura, University of Umm Al-Qura

Abstract

The paper proposed methods to protect secret information by encryption and hiding so as to conceal and protect medical data and records from being hacked . This is done through implementing two layers by using two method Elliptic curve cryptography and image steganography. First layer means first step encrypting the text through using ECC; then, the second layer is to hide the encrypted text inside the image by using 1-LSB and 2-LSB image steganography [25]. Selecting ECC, it constitutes an approach to cryptography of public key through relying on the algebraic structure of elliptic curves over finite fields, is considered as being a desired choice for being public key [13] [17]. Furthermore, it can be used in many type of media they use it in medical record system and in field such as X-Ray, CT scan, and MRI scan. Selecting Image Steganography, which is a technique to prevent the third person to have a look or detect easily the overlaying files, including the files that are encrypted [14]. Selecting the Least Significant Bit algorithm for steganography, it is commonly used straightforward steganographic algorithm and less complication. Testing two sorts of steganography (1-LSB and 2-LSB) to o find the difference between them and to clarify the positive negative aspects of each of them. 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:
information, ECC, 1-LSB, 2-LSB, Image Steganography, encryption, hiding, X-Ray, MRI, CT Scan.

1. Introduction

The security of medical data that exists is of utmost importance for the users [22]. The concern has increased in magnitude due to the constant improvement in technologies of hacking medical data such as Keylogger, Denial of Service, Waterhole Attacks, and Eavesdropping. This requires a reliable and high-performance security system to save these data from being hacked. The security techniques used can be classified into: Cryptography-based technique in which the plain text is converted into cipher text using Cryptography techniques such as ECC, DES, AES, and RSA. Selected ECC in this paper because of its pros as it needs less computational power, low level of memory and modest network connectivity, and low ability in communication bandwidth [18]. Steganography techniques in which, the confidential copy is covered under non-confidential cover. The stego-cover will be in shape of any multimedia type such as image and video [4]. In a more advance methods, new techniques that gather both encrypting and hiding the data have been used [11] [23].

This paper is focused on the improvement of the previous work by combining between ECC algorithm and image steganography. This is done by imposing the security enhancing benefits from steganography based ECC (Elliptic Curve Crypto) in image to achieve high level of reliability and security. This in-turn enhances the efficiency level [26].

The proposed scheme is based on generating share sets that can be distributed to the participants. The scientific journals are subjected to various applications that deal with the secret sharing techniques by ECC (Elliptic Curve Crypto) [19]. Most of the papers are addressed to share the problem related to the secret sharing techniques. [3] has proposed that new secret sharing processes involve the combination of Shamir's idea of detecting the cheating shares. By comparing the different schemes the resercher4 found that the rate of cheater detection problem is higher than the any other schemes.

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 would examine theoretical background. This includes exploring ECC in subsection 2.1. followed by a detailed examination of steganography in subsection 2.2. and highlights sorts of steganography and differences between Steganography in 1-LSB and 2-LSB Then, section 3 provides a detailed description the idea, procedure, algorithm, implementation tests and results analysis & comparison Section 4 suggests potential improvements to the literature based on the findings of this study. Finally, section 5 summarizes of the whole research.

Manuscript received December 5, 2020
Manuscript revised December 25, 2020
https://doi.org/10.22937/IJCSNS.2020.20.12.26

2. Theoretical Background

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

2.1 Elliptic Curve Cryptography

Elliptic curve cryptography constitutes an approach to cryptography of public key through relying on the algebraic structure. It protect the secret data through the use of keys. ECC is based on the theory of Elliptic curve [15]. The Elliptic curve theory is employed to form smaller and faster effective keys of cryptography [17]. It provides better security and protection the secret protected data. Elliptic curve cryptography uses the elliptic curves to design the elliptic keys [9]. 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.

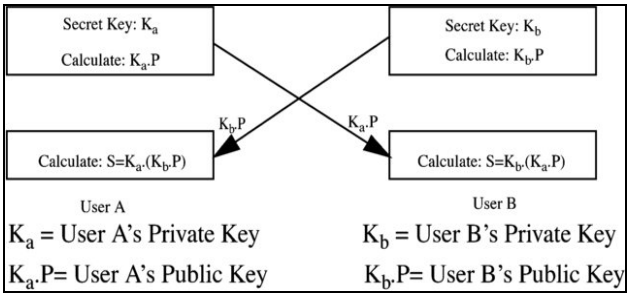

Fig. 1 Public key and Private key generated & exchanging

Fig. 1. shows the ECC secret-key-exchange algorithm block diagram and how public and private keys are generated.

2.2 Steganography

The method of Steganography can be used in the images or the videos or the recorded messages [8]. The common usage of this program is in images but the characteristic of the method is typically written in some figures including hash marking. Unauthorized view and the pirated copyrights are being protected from the sides of Steganography [18].

Steganography known as a technique during which the secret information or the secret data is hided in such how that its presence can't be detected. this is often the rationale why steganography is understood as covered writing [2]. the aim of steganography isn't just to guard the protection but also to cover it in such how that nobody can recognize or determine the presence of the hidden secret information. the most aim of this system or technology is to cover the presence of any of the hidden information [6]. The one that isn't authorized to urge the access of the knowledge shouldn't even know that if any hidden information is present or not [11]. Message, carrier and therefore the password are the three main components of the steganography. The message is that the secret text, image or the video or the audio that had to be protected through the technique of steganography[22]. The carrier is that the path or the medium through which the key and therefore the covered message is transferred. The password is that the stego-key through which secret data is protected and may be disclosed.

Basic steps of steganography as shown in Fig. 2.

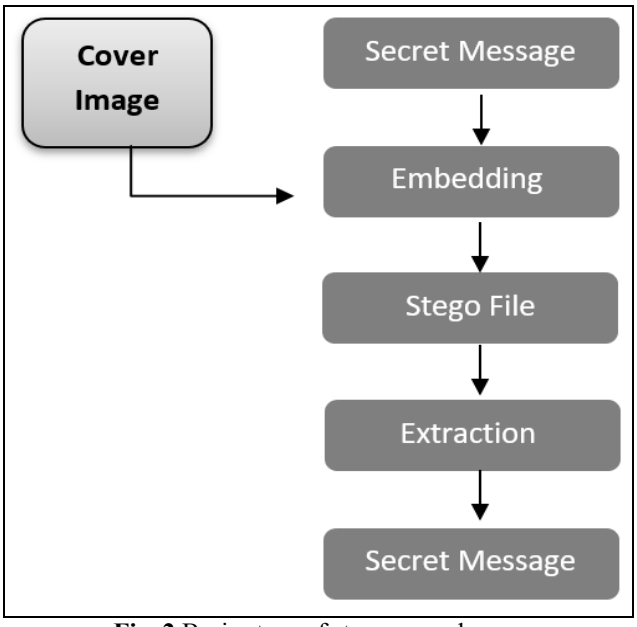

Fig. 2 Basic steps of steganography

2.2.1 Steganography is Categorized into Three types:

As the Fig. 3. Shows there are three sorts of steganography

(i) Text: this is the most commonly used type of steganography technique [14].
(ii) Audio/video: This type of steganography is the most difficult and complex type of steganography [23]. 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. [19].

(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 [22]. 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.[8, 19].

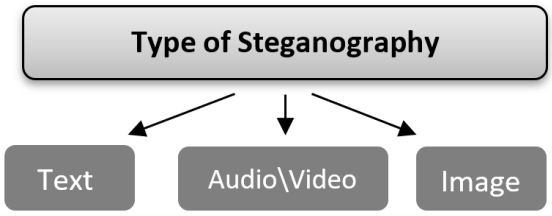

Fig. 3 Types of Steganogaphy

Among the three types of steganography the most common and popular steganography used it the Image steganography [9]. 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 [10]. It uses the technique of Least Significant Bit. This method is much easy than the other method of steganography [19]. 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 [10].

2.2.2 Least significant bit (LSB) replace algorithm

The Least Significant Bit algorithm could be a commonly used straightforward steganographic algorithm, which is employed to embed secret information inside a cover Medea. during this method, the secret information is stored within the least significant bits of the original cover image and therefore the bits are flipped accordingly. during this process, the change only takes place at the smallest amount significant bits of the original image and never on the foremost significant bits due the resultant noise within the image [7].

2.2.3 Different between 1-LSB and 2-LSB in steganography

As Fig. 4, shows the deference between 1- LSB and 2-LSB that we change the last bit from the least significant bit through using 1-LSB, on the other hand we change the two last bits from the least significant bit while using 2-LSB [7].

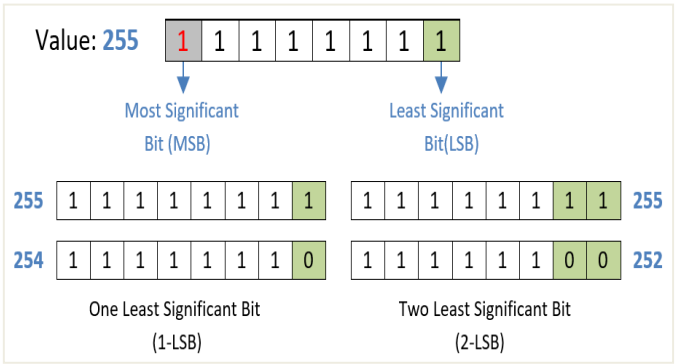

Fig. 4 Difference between 1 LSB and 2 LSB

2.2.4 Challenging in steganography

With the advancement of technology it has become important to protect the data that is hidden using the technique of steganography [20]. Also, the care has to be taken that while applying steganography the information or the secret message does not get destroyed completely [25]. Furthermore, the steganography technique should strongly face techniques of compression and cropping [1].

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

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

Encrypting and Hiding Data Process Fig. 5. this process starts through selecting sensitive data file 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.

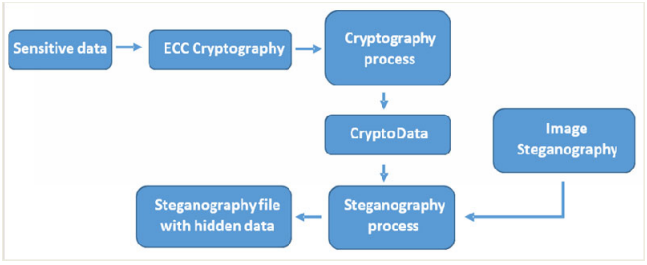

Fig. 5 Encrypting and hiding data

After that Retrieving Data Process Fig. 6.will take place through extracting cypher text and then ECC. decryption should take place in order to get the original sensitive text.

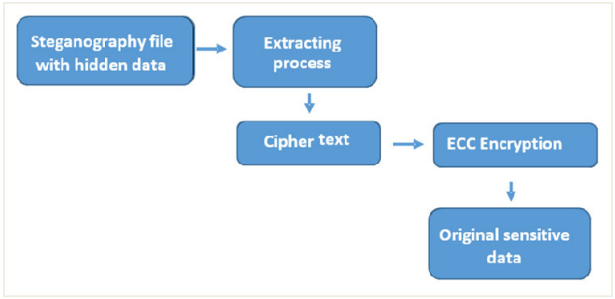

Fig. 6 Retrieving Data Process

3.2 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 [11, 18].

3.3 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 layer 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. 7. giving the user two choices enter data or extract the data.

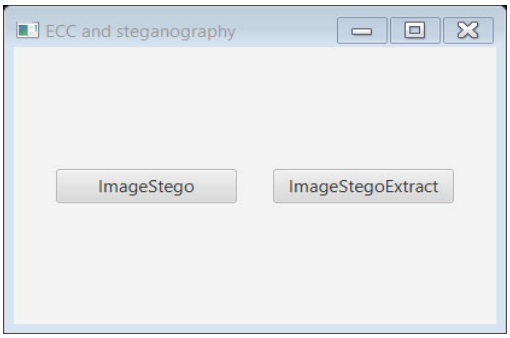

Fig. 7 Interface of proposed system

If the user chose entering data which is here (Image stego) will get new window. This interface as observed in Fig. 8.

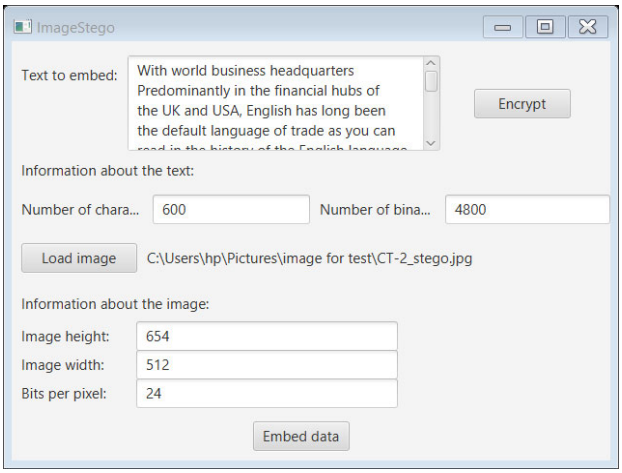

Fig. 8 Interface to entering sensitive data

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 [13]. 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. 9. 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.

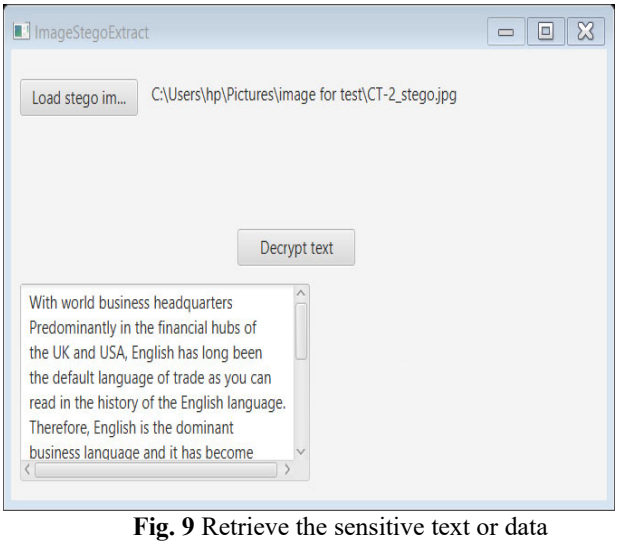

Fig. 9 Retrieve the sensitive text or data

3.4 Results Analysis & Comparison

The secret information is taken from a file that authorized person use it . The information given from the authorizes person in the system are required to be encrypted by hiding them inside the image frames.[3] For this purpose 15 different images are chosen. The classification is elaborated as per table 1 for these 15 images. We can see the results in Table 1. The table gives the results of PSNR and capacity for all selected images.

The PSNR is computed using formulae

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

where

$$MSE = \frac{1}{M*N}\sum_{X=0}^{M-1}\sum_{y=0}^{N-1}(C(X,Y) - S(X,Y))^2 \text{ [27] (3)}$$

The capacity per image, i.e. stego cover-media, is estimated as the amount of data which will be hidden within the image file without significantly changing it. it's measured consistent with the cover that's used [3]. the subsequent formula illustrates the metric

$$\text{Capacity} = \frac{(number\ of\ charcters)\times 8}{number\ of\ bit\ in\ image} \times 100 \text{ [Ref 3] (4)}$$

Image	Type	Image high	Image width	PSNR		Capacity	
				1-LSB	2-LSB	1-LSB	2-LSB
1	CT-Scan	1000	1000	77.513	72.794	3000000	6000000
2	CT-Scan	654	512	72.872	68.511	1004544	2009088
3	CT-Scan	594	541	72.387	68.511	964062	1928124
4	CT-Scan	840	918	76.302	72.063	2313360	4626720
5	CT-Scan	512	512	71.583	66.976	786432	1572864
6	MRI	808	717	75.075	70.43	1738008	3476016
7	MRI	1600	1600	81.652	77.678	7680000	15360000
8	MRI	748	617	73.948	70.135	1384548	2769096
9	MRI	320	320	67.251	63.438	307200	614400
10	MRI	256	256	65.562	60.864	196608	393216
11	X-RAY	2200	2200	84.028	81.132	14520000	29040000
12	X-RAY	1693	56	77.158	72.498	2832192	5664384
13	X-RAY	756	965	76.039	71.961	2188620	4377240
14	X-RAY	768	1024	76.394	72.674	2359296	4718592
15	X-RAY	630	414	71.557	67.538	782460	1564920

Table: 1 Results of PSNR and Capacity

The results shown in table 1 are based on comparing two algorithms in steganography (i.e. 1LSB and 2 LSB) when conducting PSNR and Capacity. From table 1, it can be shown that values of PSNR with 1 LSB algorithm are better than PSNR values with 2 LSB. The quality of PSNR with 1 LSB surpassed its quality with 2 LSB in three different types of images (CT-Scan, MRI, and X-ray) [3]. The higher values of PSNR when using 1 LSB is always higher than the values of PSNR when using 2 LSB. This indicates that hard steganography predictability with 1 LSB is more secure than with 2 LSB.

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 (1 LSB or 2 LSB)as elaborated in Table 1. We find that PSNR for 2 LSB is always lower compared to 1 LSB algorithm. 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 1 LSB and 77.678 for 2 LSB, and the difference between two algorithms is just (81.65 – 77.678)*100/ 81.65 = 4.86%.

For image number 11, of size 2200 * 2200, the PSNR values are quite large 84.03 for 1 LSB and 81.13 for 2 LSB, and the difference between two methods is just (84.03 – 81.13)*100/ 84.03 = 3.45%.

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 1 LSB and 60.86 for 2 LSB, and the difference between two methods is just (65.56 – 60.9)*100/ 65.56 = 7.1%.

The histogram for PSNR computed as shown in table 1 is given in Fig. 10. From the histogram it can be seen that 1-LSB algorithm always gives higher value of PSNR in comparing with the 2 LSB one as seen the results of 15 image sizes analyzed and presented in Table1.

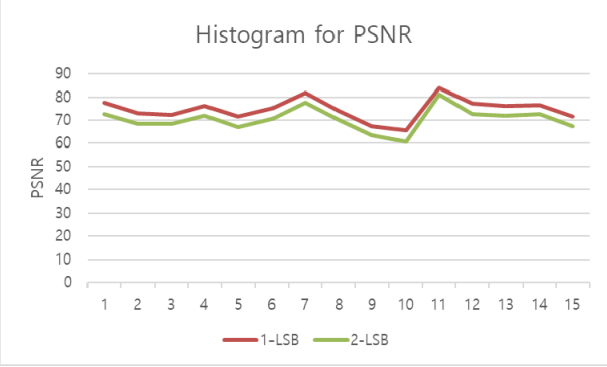

Fig. 10 Histogram of PSNR

In the other hand the results of capacity Inverse the result of PSNR as the table 1 shown.

Where we have noticed that Capacity for 2 LSB is always higher compared to 1 LSB algorithm. For bigger file size like image number 7 where image height is 1600 and image width is also 1600, the capacity are quite large 15360000 for 2 LSB and 7680000 for 1 LSB, and the difference between two algorithms is (15360000 – 7680000) = 7680000

For image number 11, of size 2200 * 2200, the Capacity are quite large 29040000 for 2 LSB and 14520000 for 1 LSB, and the difference between two methods is (29040000 – 14520000) = 14520000

While when the file size is small , like in image number 10, of size 256*256 , the Capacity are quite less than image before 393216 for 2 LSB and 196608 for 1 LSB, and the difference between two methods is (393216 – 196608) = 196608.

Based on the studies and results in the Table 1 we can hide double amount of data by using 2 LSB.

The histogram of capacity computed as shown in Table 1 is given in Fig. 11. From the histogram it can be seen that 2 LSB algorithm always gives higher value of Capacity in comparing with the 1 LSB one as seen the results of 15 image sizes analyzed and presented in Table1.

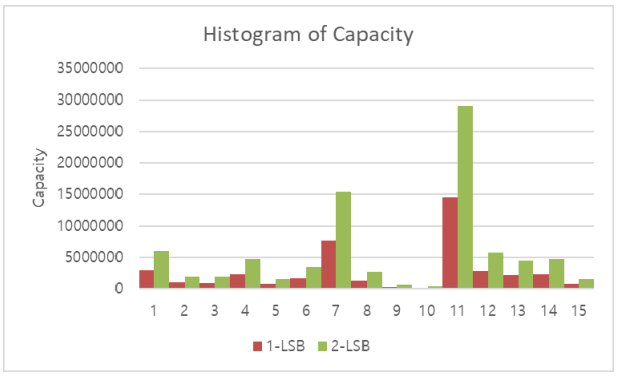

Fig. 11 Histogram of Capacity

After comparing the two methods, it can be deduced that LSB algorithm works effectively whenever use 1 LSB or 2 LSB . However, we have inverse relationship between PSNR and Capacity whenever the PSNR is higher the Capacity is low, vice versa whenever the capacity higher the PSNR will be lower. there is a challenging point related to pick acceptable LSB as we need to pick a reasonable number of LSB that balances capacity and security, as the PSNR indicates the level of security, That's where the relationship between the PSNR and level of

security is centrifugal. When the PSNR in the image is high means the stego image is near to the original image, so will be hard for the intruders recognize that there are secret data inside the image [3] [7].

3.4.1 Capacity vs. Security

To increase capacity in the proposed security system, need to increase number of LSB Steganography used. Whenever the LSBs increase the security in the system will be degrade in general [3]. But in the proposed system we selecting 1 LSB and 2 LSB to balance between the capacity and security, while 2 LSB provide large capacity with acceptable security.

4. Improvement

It combined two methods (i.e. ECC and 1 LSB and 2 LSB 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 defines related secret data and information.

In addition to increases the capacity of the cover media (i.e. image) to can be hide a large amount of secret information by using 2 LSB steganography at the same time keeping in the acceptable level of security system.

Also, this study considered Least Significant Bit is the easiest and the popular method or tool to hide the secret data [19]. 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.

5. Conclusion

In this research, a model is proposed and is introduced by combining the two techniques of elliptical curve cryptography and two sorts of steganography (i.e.1 LSB and 2 LSB). With the use of two techniques, the private and secret information will be encrypted then hided in a much better way than before [1, 18, 21]. It Also, there was a noticeable change in the vacant bits in the image capacity when using or applying 2 LSB with acceptable level of security. This helps both recorder and the receiver of the secret information to transfer more information and keep any person who is not authorized to see and get this information to keep away [14, 16, 17]. 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] Al-Anizy, N., Al-Anizy, A., Baghoza, N., Al-Ghamdi M and Gutub, A., 2018, October. 3-Layer PC Text Security via Combining Compression, AES Cryptography 2LSB Image Steganography. Journal of Research in Engineering and Applied Sciences (JREAS) 3(4):118-124 (2018).

[8]

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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).

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

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

[25] 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.

[26] 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.

[27] 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.

[28] 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.

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

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

[31] 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.