Journal of Telematics and Informatics (JTI)
Vol.8, No.1, December 2020, pp. 78~90 ■ 78
ISSN:2088-8708

A STEGANOGRAPHY LEAST SIGNIFICATION BITS (LSB) TECHNIQUE FOR HIDE TEXT DATA ENCRYPTION WITHIN IMAGE

Riyadh Alnajih Alsayih*. Muhammad Qomaruddin, Imam Much Ibnu Subroto**, Suryani Alifah****
*Higher Institute for Comprehensive Professions, Sorman, Libya
**Department of Electrical Engineering, Universitas Islam Sultan Agung, Indonesia

ABSTRACT

With the development of means of communication and the exchange of information over the Internet, and with the development of hacking operations, intruders became able to view, and change information, so the need to find means to preserve privacy and information exchange arose. Cryptography and steganography had a prominent role in this field Encryption distorts the message and steganography hides the message's presence. In this paper, the proposed system uses both steganography and cryptography to provide a double layer of security. In cryptography, we use both a substitution and RSA algorithm to encrypt the message. In steganography, we used LSB technology with a stego key to embed data in the image, all of this to improve data security. A scale of Mean Square Error (MSE) and a scale of peak signal-to-noise ratio (PSNR) assessed system performance. The results showed that the image quality is good, and it is difficult to notice any difference between it and the original image. The results of both MSE and PSNR were good, as the PSNR value was more than 56.

Keyword: Encription, Steganography, LSB

1. Introduction

Maintaining privacy in personal communications is something everyone wants, so information and data security is one of the most important factors in communication technology. The over whelming advances in digital data-sharing methods have brought tremendous potential to both security and protect confidential data from unauthorized acceptance. Accordingly, the development of security systems are critical to ensuring data security while moving through the Internet. There are many fields of security technology that deal with protecting confidential data. The most important of these techniques are encryption and information hiding [1].

Combining cryptography and steganography in one system aims to increase security, and that all the information (message) inserted into the media images could not be open easily by unauthorized persons. The cryptography converts messages and information confidential to a shape that cannot read unless by using a secret key. The information only retrieved with the same key. The form of encrypted message (untidily) raises doubts in revealing their content, which attract the hackers to tamper the message that they could not decrypt, while the steganography is about embedding the information into media files where it is neither observed nor detected, and its existence cannot be recognized, where the overall form of the carrier file is maintain. In steganography was used method the least signification BITS (LSB) technique because it is easy, simple, and uncomplicated method for embedding, in which pixel values are processed directly and produce a slight change in the coat data that cannot be perceived by the human senses [2].

1.1 Cryptography

In the past cryptography was a mysterious art practiced by only a handful of individuals working in government and military institutions [3]. Currently, cryptography is a well-established academic field that is taught in many universities and can be used widely by companies and individuals [4]. Many factors influenced this transformation. The emergence of the Internet as a means of communication is the main factor for this transformation. Companies now want to conduct business with their customers online. Where the cryptography today has a prominent place among the sciences, as its practical applications diversified to include multiple fields, such as diplomatic, military, security, commercial, economic, media and banking. The idea of any encryption system is to hide secret information in a way through which its meaning becomes incomprehensible to anyone who is not authorized to view it [5][6][7]. The two most common uses for encryption are to store data securely in a computer file or transfer it over an insecure channel such as the Internet. Either way, the fact that the document is encrypted does not prevent unauthorized people from accessing it, but it ensures that they cannot understand what they see [8][9][10].

Cryptography can be define as converting data from a readable form to an incomprehensible form that cannot be read or processed until after it is decoded. This method is the art of secret writing [11][12]. Cryptography is useful for achieving confidentiality transfer across the networks where the sender sends the cipher-text, and the receiver on the other side receives the cipher-text then decrypt it to plaintext. The Figure.1 show the Basic Model of Cryptography [13]. The main goal of cryptography is to make confidential information unreadable to all but the recipient person, and achieve privacy or confidentiality, data integrity, authentication and non-repudiation [4][5].

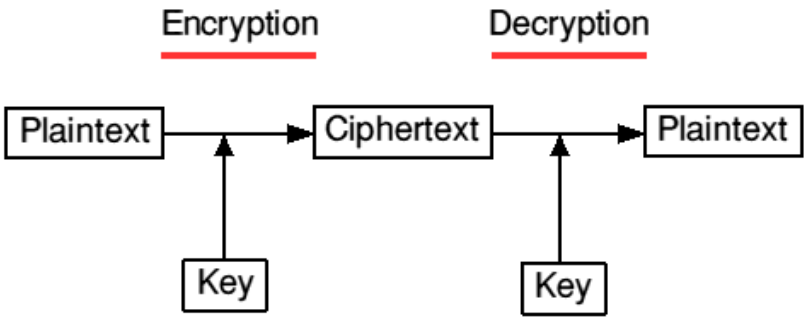

Figure.1 Basic Model of Cryptography.

There are two basic stages in cryptography namely, Encryption: It is the conversion of plain text from clear and readable form to incomprehensible and illegible symbols (cipher text) using algorithms of cryptography and encryption keys. Decryption: It is returning the cipher text to its previous position as understandable and readable text (plain text) using cryptographic algorithms and decryption keys [14][12].

1.2 Steganography

Steganography not considered a modern science. It was the first appearance of this science in the Greek era. Where one of the men at that time contacted one of his relatives in Greece by shaving the hair of servants, then tattoo the messages on their heads, waits for the growth of their head hair and then sends them to the person who wants to communicate with him [15]. The science of Steganography has developed a lot nowadays and uses digital information and computers as a means of transferring data[16]. The term Steganography comes from the Greek words Stenos, which means cover, and Graphia, which means writing, hence, steganography means covered writing [13].

Steganography is a branch of data security through mystery. It defined as the art of hiding and sending information through (carriers) in an attempt to hide the existence of certain data until it hidden that there is a connection or exchange of information done in secret, only the concerned persons are aware of this communication. It is also known as camouflaging the information to conceal its existence and make it invisible, and thus to completely hide the fact that confidential information exists, also known as invisible communication. Figure.2 shows the steganography system Scenario [17][18][19].

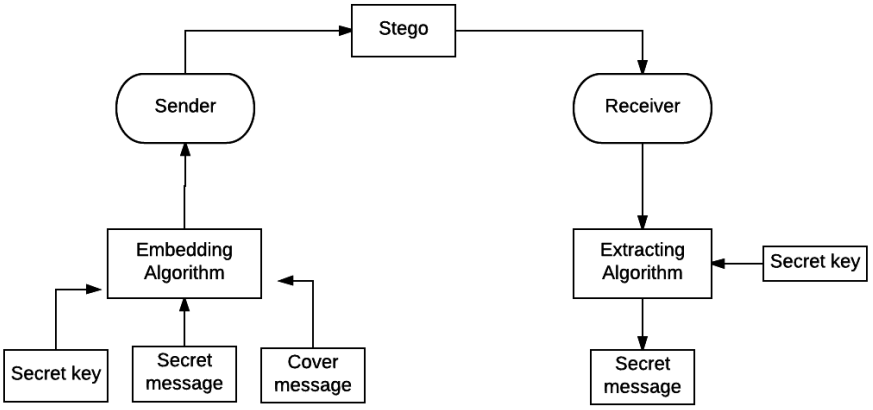

FIGURE.2 STEGANOGRAPHY SYSTEM SCENARIO

The main terminology used in steganography systems are [20]:

- Cover message (the carrier): is the host in which the secret message be hidden, such as an image, sound, video, etc.
- Secret message is the data to hidden in a suitable digital media cover.
- Secret key: An optional password for increased security. Used to control access to hidden data.
- Algorithm of Embedding: it is the method used to include confidential data in a cover message.
- Algorithm of Extraction: it is the method used to extract hidden data from a stego file.
- Stego: The cover file with a message containing confidential information inside it, it is the result obtained after the secret message hidden in the cover file.

The purpose of hiding information is not to prevent others from knowing hidden information, but to remove the doubt about the existence of hidden information. The distinguishing thing about information hiding techniques is that they keep pace with modern technologies, and can be used in all computer media such as images, texts, sound, video and network protocols .The information hiding applications are used in many areas such as online transactions, communications, military, and others [15][21].

There are many types of steganography, the data is hidden by embedded it inside the cover. Steganography systems use media files as a cover media, almost all digital file formats can be use, in the steganography process such as video, images, sound, and text. The figure.3 shows the main types of steganography[22].

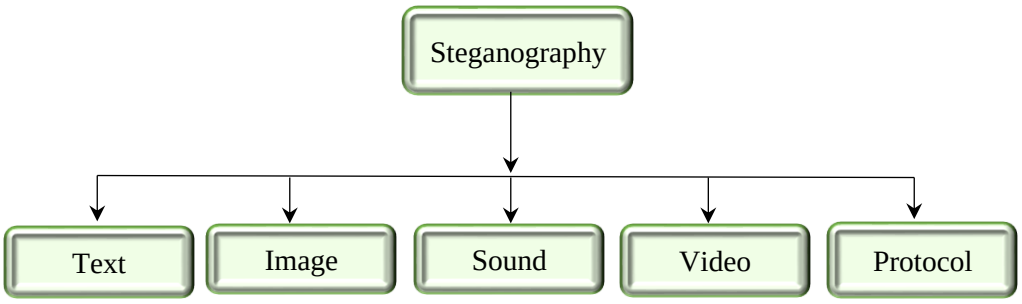

FIGURE.3 TYPES OF STEGANOGRAPHY.

In the science of steganography, the less important bit (LSB) substitution is one of the most well know techniques for hiding data in images. The less important bit (LSB) is a simple way to embedding information into the digital cover so that an accidental observer cannot detect it. The technique works by replacing some data in a given pixel from the cover with the data to be hide. Where the replacing is perform on the less important bits. Applying LSB technique on byte of an 8-bit gray image, one bit can be encoded into each pixel as each pixel is represented by one byte and applying LSB technique to 3 bytes for color image 24-bit, 3 bits can be encoded into each pixel as each pixel is represented by 3 bytes [23][24].

2. Research Method

As shown in Figure.4, the data will be encrypted first using a Substitution algorithm, then using the RSA algorithm, in this algorithm we use the public key to encrypt and private key to decrypt. On the other hand, the encoded data will be hide in the image files using the LSB embedding method, and we will use the stego key for embedding and extract. Where the LSB algorithm ensures that there is no visually noticeable change, this ensures there are few chances to attack. The integration of these two methods can improve the security of the embedded data. This method also achieves requirements such as security, capacity and robustness, for secure data during transmission over an open channel (Internet). The resulting Stego image can be transfer without disclosing the exchange of secret information. Moreover, even if the attacker were able to defeat steganography, he would still need to decrypt the encrypted message.

The proposed model is divide into five stages, which are as follows:

1. Substitution cipher process.
2. Encrypt the secret message using RSA (Encryption process).
3. Hide encrypted data in image files (Embedding process).
4. Extract encoded data from image files (Extraction process).
5. Decrypt the secret message (Decryption process).

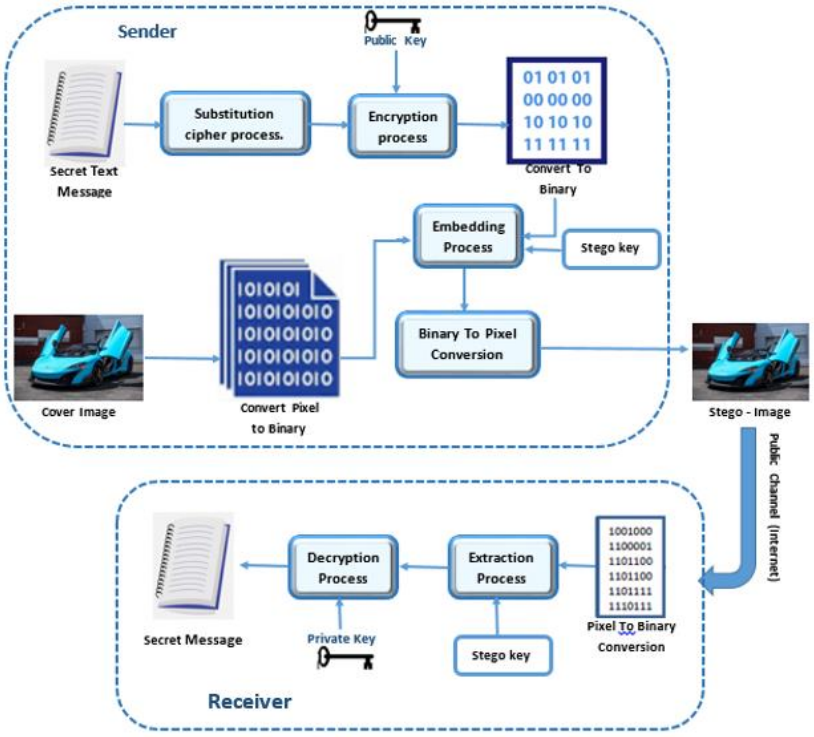

Figure.4 the proposed system model

2.1 Substitution cipher process.

Substitution cipher is a method of encoding in which alphabetic characters or symbols are randomly write under the letters of the alphabet just as they are arranging alphabetically. The rule of encryption is represented in substituting each letter with the letter or symbol underneath it, while the decryption rule is to perform the same action opposite[25][26].

Example:

	Input	**Output**
–	GET	AKN
–	BIG	M!A

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
S	M	J	@	K	#	A	W	!	P	Z	V	$	E	R	L	%	B	&	N	C	D	O	U	F	Q

2.2 Encryption process.

In the encryption process will be used an algorithm RSA. The RSA is an asymmetric master cipher system created in 1976 by Rivest, Shamir and Adleman, and it based on encrypting messages using modular exponentiation and public key sharing. The security of the RSA algorithm depends on the length of the key. Factors for large integers are difficult to find. In the RSA algorithm, there are two different keys, a public key and a private key, but they are relate to each other. The public key is use to encrypt the message, it can be posted to anyone, and the private key is used for decryption the message. The RSA algorithm includes three steps, which are key generation, message encryption, and message decryption[27][28].

There are five steps for generating the keys for the RSA algorithm, and they are as follows:

1. Choose two prime numbers (p, q), the larger the two numbers, the greater the level of complexity and the more difficult cipher analysis.
2. Calculate n = p x q. is the length of the key.
3. Calculate φ(n) = (p-1) * (q-1), where φ is the Euler function.
4. Find the value of **e** based on the following conditions:
   - $1 < e < \varphi(n)$
   - GCD (e, φ(n)) = 1

   Where **e** is the public key.
5. Find the value of **d** from the following equation:

$$ed = 1 + k * \varphi(n)$$

Where d = int, $d \neq e$ and d is the privet key.

After creating the public and private keys, the message encryption and decryption process carried out according to the following formulas:

Encryption: $c = m^e \pmod n$, where m is the message in plaintext.
Decryption: $m = c^d \pmod n$, where c is the cipher text.

2.3 Embedding process.

The embedding process takes place on the sender's side. After encrypting the secret message using the proposed algorithm, the data resulting from the encryption process is included in the cover image. The inputs are a text file, cover image, and stego key while the output is a stego image. The following steps shows the process for embedding a confidential message into a cover image.

1. Enter the cover image and the secret message to be hide.
2. Divide the pixel into RGB color components.
3. Convert the pixel of the image to a binary.
4. Convert a secret message to a binary, a string of 8 bits.
5. Divide the string into 1-bit substrings.
6. Replace this 1 bit from the secret message with the last 1 bit of the cover image.
7. Repeat the step 6 to include all the data for the secret message.
8. Save the stego image.

2.4 Extraction process.

The extraction process implemented in the receiver side. The extraction process reverses the embedding process, which is to retrieve the secret message from a Stego image. The inputs are a Stego image and a stego key while the output is the confidential message. The following steps explain the process for extracting the secret message from a Stego cover image.

1. Enter stego-image and key.
2. Divide the pixels into components of RGB color.
3. Convert image pixels to binary.
4. Extract bit from the color component to make the character.
5. Repeat step 4 until all secret bits are decoded.
6. Write the secret message.

2.5 Decryption process.

At this stage, the cipher text is decrypted to obtain the original message. One of the

most basic requirements in this process is the availability of the private key, as no one will be able to obtain the data except the person who owns this key.

3. Results And Analysis

All steganography algorithms aim to include the digital representation of the message within the image without leaving the embedding process any visual trace that could cause the detection of any modification to the image that may lead to the location of the secret message, meaning making the stego image as similar to the original image as possible. The effect of the concealment process should not reduce the quality of the host image carrying the message. Where spaces and punctuation marks calculate when encoding the secret message before embedding it into the image, and usually these characters are encoding using the ASCII encoding, which assigns each character a single byte that has a specific sequence as specified in the encoding table for the ASCII encoding. There are several measures for evaluate steganography algorithms. This is measure by histograms, mean square error (MSE) and Peak signal-to-noise ratio (PSNR).

3.1 Histogram.

Histogram it is a graphical display of the scheduled frequencies. This test based on the comparison between the original image and the stego image, whereby the deterioration of the quality of the images can be visually observe through it. We compared the histogram of three images (greencar1, Garden1, and Desert1) with a stego image hide 100 characters and 48000 characters, and the Figure.5, Figure.6 and Figure.7 illustrate the comparison results of histograms.

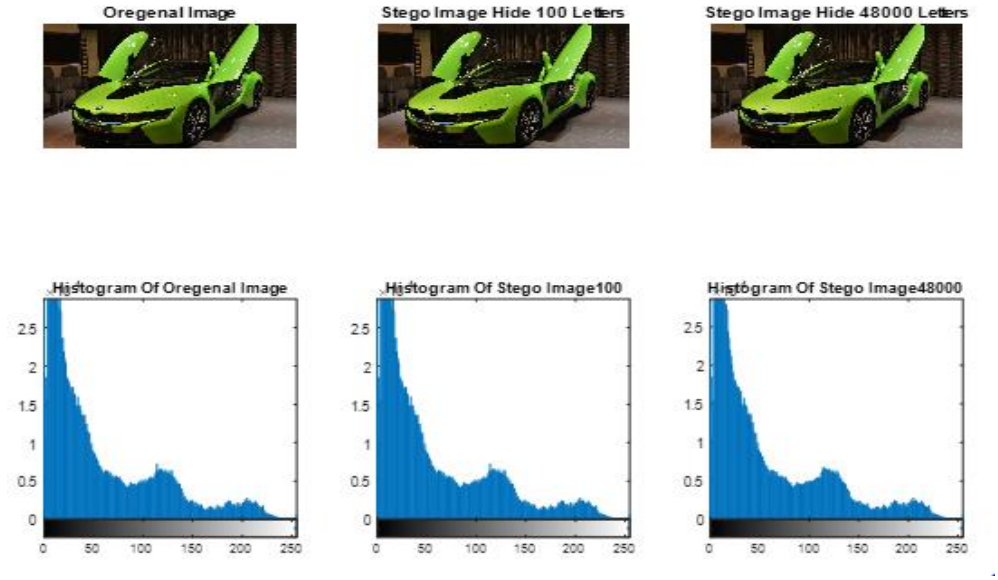

Figure.5 Histogram of Original and stego image (greencar1).

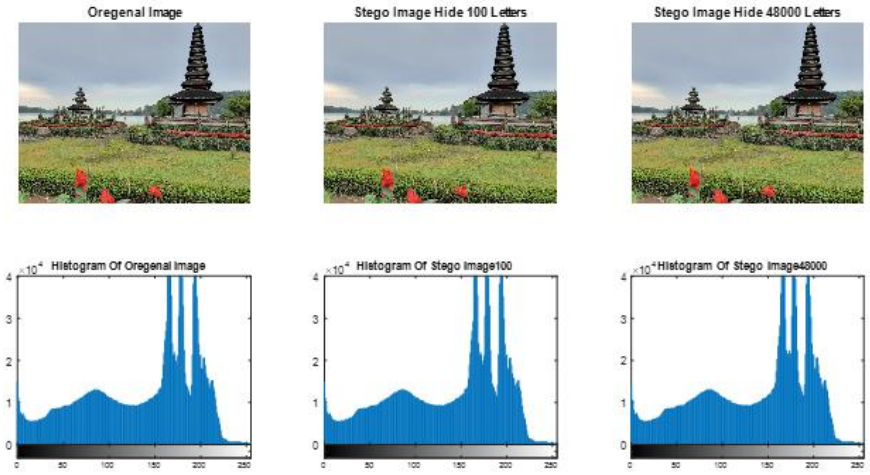

Figure.6 Histogram of Original and stego image (Garden1).

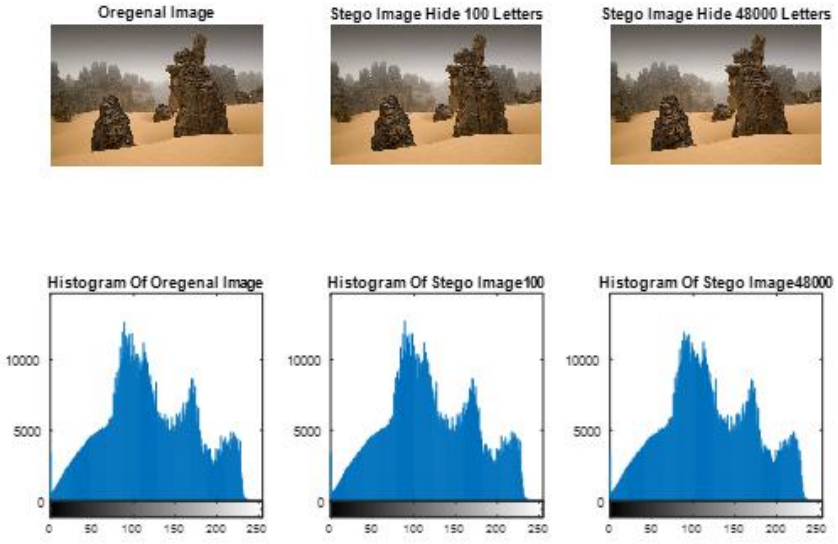

Figure.7 Histogram of Original and stego image (Desert1).

From the results of the histogram, we can conclude that the difference between the original image and the Stego images is small, as few pixel values have been change. Thus, it will not visually deduce the presence of any hidden data in the Stego image.

3.2 Testing Results Using MSE & PSNR

The most common metrics used to measure image quality is the mean square error (MSE) value between the stego and the cover image and the peak signal-to-noise ratio (PSNR). Indeed, this test used to determine if the hidden message is not visible as well as the imperceptibility and visual quality of the stego image as compared to the cover image.

The lower the MSE values, the less error. The more values PSNR higher, the better the stego image quality, taking into mind the typical value is start from 40.

Different sizes of the secret message were hide in the cover images, where the message size starts from 100 Letters and increases to 48000 Letters. The equation of MSE were applying to find mean square error and the equation of PSNR to find the peak signal-to-noise ratio. Where Table.1 shows the MSE and PSNR values for the greencar1 image, Garden1 image and Desert1 image.

Equation of MSE & PSNR [29][30].

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{\Xi^2}{\mathrm{MSE}}\right)$$

Where

$$\mathrm{MSE} = (mn\rho)^{-1}\sum_{\gamma\in\Gamma}\|\mathcal{C}(\gamma)-\mathcal{S}(\gamma)\|^2$$

And C and S are the cover image and the stego image respectively, of size m × n × ρ, with C, S ∈ {0, 1, . . . ,_}, and _ = max(max(C),max(S)). The index set γ = (ℓ1, ℓ2, ℓ3) sums over the set

$$\Gamma = \{1,\ldots,m\}\times\{1,\ldots,n\}\times\{1,\ldots,\rho\},$$

Where ρ = 1 for gray scale images and ρ = 3 for 24-bit color images.

Table.1: the test of image quality (MSE) and (PSNR) for greencar1, Garden1and Desert1 images.

Name of image	Image size	Size of hidden	MSE	PSNR
greencar1	1024 * 576	100 letters	0.00024	84.3151
		250 letters	0.00059	80.4098
		500 letters	0.0012	77.4600
		1000 letters	0.0023	74.5778
		2000 letters	0.0045	71.5621
		4000 letters	0.0090	68.5661
		8000 letters	0.0181	65.5594
		16000 letters	0.0361	62.5511
		24000 letters	0.0544	60.7787
		48000 letters	0.1087	57.7687
Garden1	1150 * 900	100 letters	0.00012	87.1186
		250 letters	0.00032	83.0732
		500 letters	0.00064	80.0476
		1000 letters	0.0013	77.0211
		2000 letters	0.0026	74.0135
		4000 letters	0.0051	71.0385
		8000 letters	0.0103	68.0221
		16000 letters	0.0206	65.0000

		24000 letters	0.0309	63.2340
		48000 letters	0.0618	60.2238
Desert1	**800 * 534**	100 letters	0.00028	83.5381
		250 letters	0.00075	79.3586
		500 letters	0.0015	76.3058
		1000 letters	0.0031	73.2721
		2000 letters	0.0062	70.1763
		4000 letters	0.0123	67.2157
		8000 letters	0.0248	64.1824
		16000 letters	0.0498	61.1617
		24000 letters	0.0748	59.3918
		48000 letters	0.1498	56.3746

Figure.8 shows the (MSE) and (PSNR) performance of the image greencar1 using the linear equation.

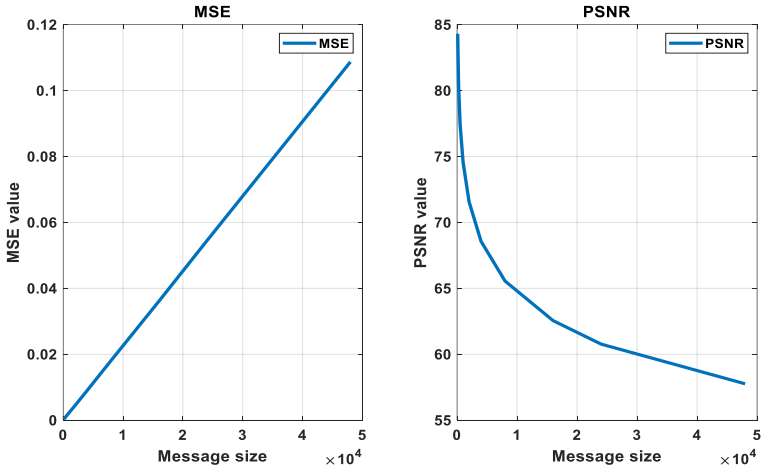

Figure.8 The value of MSE & PSNR for greencar1 image

Figure .9 shows the (MSE) and (PSNR) performance of the image Garden1 using the linear equation.

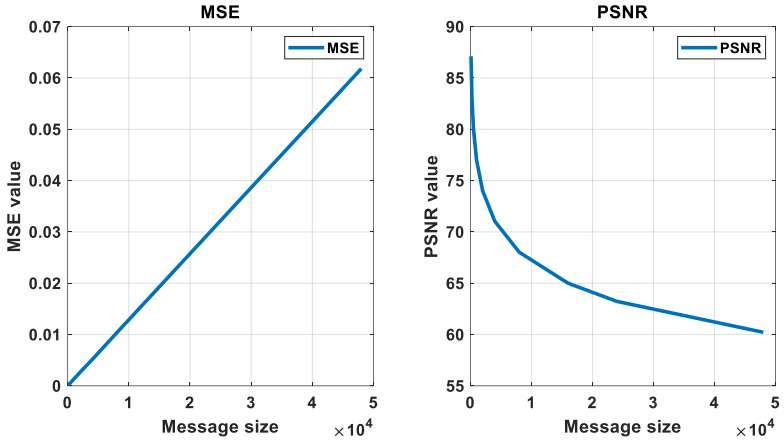

Figure.9 The value of MSE & PSNR for Garden1 image

Figure.10 shows the (MSE) and (PSNR) performance of the image Desert1 using the linear equation.

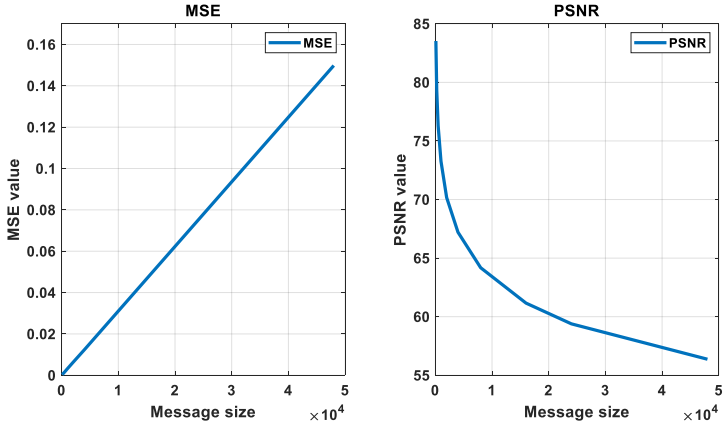

Figure.10 The value of MSE & PSNR for Desert1 image

Through the results presented in figures (8, 9, 10) we note that the greater the size of the secret message, the greater the mean square error (MSE) value and the Peak signal-to-noise ratio (PSNR) value has decreased. Higher PSNR values indicate better Stego image quality.

4. Conclusions.

Using encryption for secret messages before hiding them provides an additional level of protection against attackers. In this paper, we used both cryptography and steganography together, where we used both substitution and RSA to encrypt the message and use LSB technology to hide the message in the image to obtain a secure stego image. The system was apply to many images of different dimensions and messages of different lengths. When including 500 characters, the average value for mean square error (MSE) was 0.0011 and the average value for the Peak signal-to-noise ratio (PSNR) was 77.93. Through the experiments, some conclusions were drawn: The combination of steganography techniques and the encryption process enhances the security of the message, especially when using the secret key when the encryption and embedding process. We cannot find a difference by the eye when comparing the cover image before

and after the hiding process. We noticed that the increase in length of the text increases MSE value and PSNR value decreases.

References

[1] V. Sharma and Madhusudan, “Two new approaches for image steganography using cryptography,” *Proc. 2015 3rd Int. Conf. Image Inf. Process. ICIIP 2015*, pp. 202–207, 2016.

[2] R. S. Phadte, “Enhanced Blend of Image Steganography and Cryptography,” *Proc. IEEE 2017 Int. Conf. Comput. Methodol. Commun.*, no. Iccmc, pp. 230–235, 2017.

[3] H. F. Integrity, “public-key cryptography To cite this version : Integrity , Authentication and Confidentiality in Public-Key Cryptography,” *public-key Cryptogr. To cite this version Integr. , Authentication Confidentiality Public-Key Cryptogr.*, vol. 12, no. 5, p. 59, 2018.

[4] O. Reyad, “Cryptography and Data Security: An Introduction,” *10.13140/RG.2.2.30280.16646*, no. 9, 2018.

[5] A. Zaru and M. Khan, “General summary of cryptography,” *Int. J. Eng. Res. Appl.*, vol. 08, no. 02, pp. 68–71, 2018.

[6] E. W. Abood, “Combining a Hill Encryption Algorithm and LSB Technique With Dispersed Way for Securing Arabic and English Text Messages Hidden in Cover Image,” *مجلة ابن الهيثم للعلوم الصرفة والتطبيقية*, vol. 03, no. 2, pp. 214–223, 2017.

[7] D. Boneh and V. Shoup, “A Graduate Course in Applied Cryptography,” *Crypto.Stanford.Edu*, no. 1, pp. 1–400, 2015.

[8] M. S. Taha, M. S. Mohd Rahim, S. A. Lafta, M. M. Hashim, and H. M. Alzuabidi, “Combination of Steganography and Cryptography: A short Survey,” *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 518, no. 5, 2019.

[9] S. A. Shawkat, “Enhancing Steganography Techniques in Digital Images,” *Comput. Sci. Dep. Fac. Comput. Inf. Mansoura Univ.*, p. 201, 2016.

[10] K. Nassif Jassim *et al.*, “Hybrid cryptography and steganography method to embed encrypted text message within image,” *J. Phys. Conf. Ser.*, vol. 1339, no. 1, 2019.

[11] S. Almuhammadi and A. Al-Shaaby, “A Survey on Recent Approaches Combining Cryptography and Steganography,” pp. 63–74, 2017.

[12] S. Sharma and Y. Gupta, “Study on Cryptography and Techniques,” *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol. © 2017 IJSRCSEIT*, vol. 2, no. 1, pp. 249–252, 2017.

[13] A. Mehndiratta, “Data Hiding System Using Cryptography & Steganography : A Comprehensive Modern Investigation,” pp. 397–403, 2015.

[14] N. Sharma and U. Batra, “A review on spatial domain technique based on image steganography,” *2017 Int. Conf. Comput. Commun. Technol. Smart Nation, IC3TSN 2017*, vol. 2017-Octob, pp. 24–27, 2018.

[15] M. S. Abuali, C. B. M. Rashidi, M. H. Salih, R. A. A. Raof, and S. S. Hussein, “Digital image steganography in spatial domain a comprehensive review,” *J. Theor. Appl. Inf. Technol.*, vol. 97, no. 19, pp. 5081–5102, 2019.

[16] O. I. I. Al-Farraji, “New Technique of Steganography Based on Locations of LSB,” *Int. J. Inf. Res. Rev.*, vol. 04, no. 1, pp. 3549–3553, 2017.

[17] M. P. Rodrigues and S. Prabhu, “Pixel and Block Permutation on Combinations of Bit Planes with LSB Steganography,” *Proc. 2018 3rd Int. Conf. Comput. Syst. Inf. Technol. Sustain. Solut. CSITSS 2018*, pp. 145–150, 2018.

[18] F. Nabi and M. M. Afzal, “Image Steganography: Critical Findings through Some Novel Techniques,” *Int. J. Innov. Technol. Explor. Eng.*, vol. 9, no. 5, pp. 878–890, 2020.

[19] Z. T. R. AL-Windawi, “Security Enhancement of Image Steganography Using Embedded Integrity Features. Middle East University, Amman - jordan,” *MIDDLE EASR Univ.*, 2017.
[20] N. Singh, “Survey Paper on Steganography,” *Int. Ref. J. Eng. Sci.*, vol. 6, no. 1, pp. 68–71, 2017.
[21] M. Kaur and V. K. Sharma, “Encryption based LSB Steganography Technique for Digital Images and Text Data,” *IJCSNS Int. J. Comput. Sci. Netw. Secur.*, vol. 16, no. 9, pp. 90–97, 2016.
[22] I. Science, “在数字 图 像中 隐 藏文本的新方法,” *J. SOUTHWEST JIAOTONG Univ.*, vol. 55, no. 2, 2020.
[23] B. Chitradevi, N. Thinaharan, and M. Vasanthi, “Chapter 17 Data Hiding Using Least Significant Bit Steganography in Digital Images,” *Dep. Comput. Sci. Thanthai Hans Roever Coll. (Autonomous), Perambalur, Tamilnadu, India.*, vol. I, pp. 144–150, 2017.
[24] Naveen Verma | Preeti Sondhi | Gargi Kalia, “LSB Based Stegnography to Enhance the Security of an Image,” *Int. J. Trend Sci. Res. Dev.*, vol. 3, no. 4, pp. 1480–1484, 2019.
[25] R. Hudec, “AXRO introduction and historical background,” *Contrib. Astron. Obs. Skaln. Pleso*, vol. 48, no. 3, pp. 396–404, 2018.
[26] T. J. Shimeall and J. M. Spring, *introduction to Information Security*., pp. 155-186, 2014.
[27] S. Goyal, M. Ramaiya, and D. Dubey, “Improved Detection of 1-2-4 LSB Steganography and RSA Cryptography in Color and Grayscale Images,” *Proc. - 2015 Int. Conf. Comput. Intell. Commun. Networks, CICN 2015*, pp. 1120–1124, 2016.
[28] F. Meneses *et al.*, “RSA Encryption Algorithm Optimization to Improve Performance and Security Level of Network Messages,” *Int. J. Comput. Sci. Netw. Secur.*, vol. 16, no. 8, p. 55, 2016.
[29] A. Rehman, T. Saba, T. Mahmood, Z. Mehmood, M. Shah, and A. Anjum, “Data hiding technique in steganography for information security using number theory,” *J. Inf. Sci. 1–12*, vol. 45, no. 6, pp. 767–778, 2019.
[30] R. Kumar, G. Sharma, and V. Sanduja, “A Real Time Approach to Compare PSNR and MSE Value of Different Original Images and Noise (Salt and Pepper, Speckle, Gaussian) Added Images,” *Int. J. Latest Technol. Eng. Manag. Appl. Sci.*, vol. 7, no. 1, pp. 43–46, 2018.