Al-Khwarizmi Engineering Journal, Vol. 18, No. 1, Marh, (2022)
P. P. 26- 37

Al-Khwarizmi Engineering Journal

Enhancement of System Security by Using LSB and RSA Algorithms

Muna M. Hummady* **Ameer Hussein Morad****

**, **Department of Information and Communication Engineering / Al-KhwarIzmi College of Engineering / University of Baghdad/ Iraq*

*Email: muna@kecbu.uobaghdad.edu.iq
**Email: ameer@kecbu.uobaghdad.edu.iq

(Received 17 October 2021; Accepted 9 March 2022)
https://doi.org/10.22153/kej.2022.03.001

Abstract

A steganography hides information within other information, such as file, message, picture, or video. A cryptography is the science of converting the information from a readable form to an unreadable form for unauthorized person. The main problem in the stenographic system is embedding in cover-data without providing information that would facilitate its removal. In this research, a method for embedding data into images is suggested which employs least significant bit Steganography (LSB) and ciphering (RSA algorithm) to protect the data. System security will be enhanced by this collaboration between steganography and cryptography.

Keywords: *Cryptography, LSB, RSA, Steganography.*

1. Introduction

Digital life witnessed an increase in information security. Security procedures, particularly data communication, are compelled by the emergence of new technologies. The amount of data are exchanged over the Internet has grown, so hqas the significance of network security. Information security relies heavily on cryptography and steganography. Figure (1) depicts the widest range of information security measures. One side of the coin is Steganography, which hides the communication's tracks, while the other side employs cryptography to render it unintelligible.

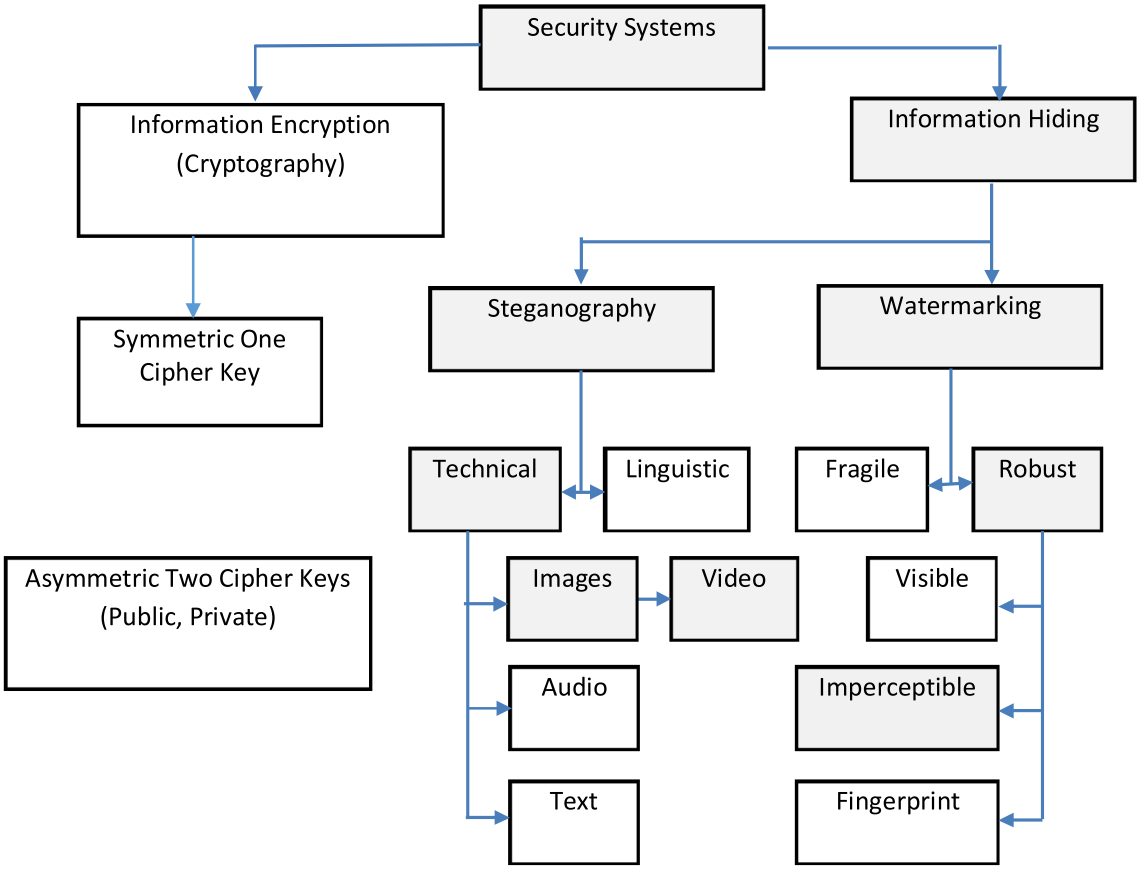


Fig. 1. Information security techniques.

Steganography is a method of disguising communication by enclosing the secret message within a false message. A cover carrier, a hidden message, a stego key, and a stego carrier are all required components of the steganography process. Text, audio, picture, and video are all function as cover carriers for the secret information they carry. The Stego carrier is created by combining a cover carrier with an embedded message. Additionally, the Stego key is utilized as supplemental secret information, such as a password that the recipient uses to extract the message [1].

Cryptography offers a variety of encoding strategies for ensuring security when communicating over a public network. A simple example of cryptography is when a sender delivers a message that is originally in plaintext. Prior to transmission across the network, the message is encrypted and transformed to cipher text. When the recipient receives this message, it is decrypted back into plaintext [1].

Many mechanisms and algorithms are appeared in researches for combining these techniques for high level information security on open communication channel.

M. Gajalakshmi and R. Vidya (2018) [1] and Mustafa S.T et al (2019) [2], are review different approaches on process of hiding information in multimedia (such as text, image, movies, or sound). These approaches are merging two security mechanisms (Cryptography and Steganography) to achieve two levels of information security.

Manoj K. R. and et al (2017) [3] proposed hybrid steganographic model based on both steganography and cryptography. The model is designed depending on the strength of conventional 3-Data Encryption Standard (DES) and discrete wavelet transform (DWT) to improve quality of image and security.

Dheyab S. Ibrahim (2019) [4], propose an algorithm to increase the security of data using two levels of encryption. The first level of security is done by using DES & RSA algorithms. While the second level is to enhance the security by using LSB algorithm in order to hide these encrypted data inside edges of color images.

Marwa E. Saleh and et al (2016) [5], propose a technique for both data security using Cryptography and Steganography techniques. This technique used to increase the information security. The first step is to encrypt the secret data using the Advanced Encryption Standard (AES_MPK) algorithm. After that, the encrypted data has been hidden in gray image by using PVD-MPK and MSLDIP-MPK methods.

Shambhavi U and et al (2015) [6], propose a combination of two types of steganography (audio and image). The aim of this work is to hide secret message (data) in an audio and image of a video file. The video has many frames inside both the image and audio. This proposes can select anyone of these frames for hiding secret data. Two algorithms can be used for this purpose. These algorithms are 4LSB for image steganography and phase coding algorithm for audio steganography.

Ameer H. Morad and Hatem Nahi Mohaisen (2016) [7,8], the article presents hiding system based on steganography using cover video and watermarking techniques to provide both of confident and authentication. The hiding process is done in random fashion use LSB method to embed and distribute the message and watermark on many video frames.

Finally, Mustafa Sabah Taha et al (2019) [9] review several ways of combining steganographic and cryptographic techniques to achieve a hybrid system and state some of the differences between cryptographic and steganographic techniques.

In this paper, the proposed system merges both the Cryptography and Steganography techniques to make the transmission of secret information (text or image) more secured. This is done, at sender side, by encrypted the secret information using RSA encipher before hiding it into cover image. The LSB method is used to hide the secret information into cover image to obtain stego image. At receiver side, firstly extract the encrypted secret information from stego image, then decrypt it by RSA decipher to retrieve the original secret information.

2. The RSA Algorithm (Rivest-Shamir-Adleman)

Asymmetric cryptography is RSA [10, 11]. It is frequently used to protect sensitive data, such as that transmitted over the internet. RSA encrypts messages use both public and private keys. The key that is used to encrypt and decrypt a communication is the inverse of the key used to encrypt it. This is a critical reason for RSA's popularity as the most extensively used asymmetric algorithm. The RSA algorithm ensures the secrecy, integrity, authenticity, and irreproducibility of electronic communications and data storage.

3. LSB (Least Significant Bit)

The transform domain and the spatial domain are too widely used to embed approaches in image steganography [12]. In the spatial domain, the secret data is directly incorporated in the cover image pixels' LSBs (Least Significant Bits).The LSB method is the most common method used to hide the secret messages into a covered image. The (LSB) is easy to understand and relatively fast in the process of inserting secret information into cover image. It is only modify the low weight bits in the insertion process, so the difference between the stego image and the original image will not be noticeable to any person who views the image. Many methods and procedures are proposed by researchers for applying LSB in applications such as insertion individually or combination in one or more of three least weight bits directly or in random fashion [13, 14].

4. Evaluation criteria (Measurements)

The evaluation of hiding process is done to measure the amount of differences between the stego image and the cover image. This requires measuring the quality of the stego image. Those measures are Mean Square Error, similarity test and Peak Signal-to-Noise Ratio.

Mean Square Error (MSE) is a statistical term that refers to the mean or average of the square of the difference between actual and estimated values. MSE is utilized in this study to identify the difference between the cover and Stego images [8, 9].

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}\left(S_{xy} - C_{xy}\right) \qquad ...(1)$$

Where x and y are the image coordinates. M and N are the number of rows and columns in the input images. S_{xy} and C_{xy} are pixel gray (or color) values at X Y coordinate in the generated stego-image and the covered image respectively.

The content of the image hidden information must be embedded using the image steganography system in order not change the quality of the image.

PSNR is the maximum signal to noise ratio in the stego image. PSNR is commonly used to quantify reconstruction quality for images and video subject to lossy compression. The PSNR value indicates the better quality of image; i.e. less distortion.

$$PSNR = 10\,Log_{10}\left(\frac{Maxmum\ Signal\ Power}{Noise\ Power}\right)$$

$$= 10\,Log_{10}\left(\frac{M*N*(L-1)^2}{\sum_{x=1}^{M}\sum_{y=1}^{N}\left(S_{xy}-C_{xy}\right)^2}\right) \quad \cdots(2)$$

Where:

M*N: Cover image size (Height and width) in pixels.

L: determine the number of gray scales in stego image (in this paper L=256).

x, y: are image pixel coordinates.

C_{xy}: is cover image gray (or color) value at coordinate x and y.

S_{xy}: is stego image gray (or color) value at coordinate x and y.

Calculate the correlation between the stego image and the cover image to determine the similarity test. When the stego-image is perceived to be identical to the original cover-image, the correlation is one. Correlations can be determined using the formula below. [15, 16].

$$Cor = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N}\left(C_{xy}-\bar{C}\right)\left(S_{xy}-\bar{S}\,\right)}{\sqrt{\sum_{x=1}^{M}\sum_{y=1}^{N}\left(C_{xy}-\bar{C}\right)^2\left(S_{xy}-\bar{S}\right)^2}} \cdots(3)$$

Where

$$\bar{C} = mean\ gray\ (or\ color) value\ for\ cover\ image = \frac{1}{M*N}\sum_{x=1}^{M}\sum_{y=1}^{N} C_{xy}$$

$$\bar{S} = mean\ gray\ (or\ color) value\ for\ stego\ image = \frac{1}{M*N}\sum_{x=1}^{M}\sum_{y=1}^{N} S_{xy}$$

5. Cryptography vs. Steganography

It is possible to combine the encrypting message techniques by using cryptography and hiding the encrypted message using steganography. The resulting stego-image is transmitted without revealing that secret information which has been exchanged. Even if an attacker defeats the steganographic technique and detects the message from the stego-object, the attacker still requires the cryptographic decoding key to decipher the encrypted message [19]. Table (١) shows that both technologies have advantages and disadvantages [20].

Table 1,
Advantages and disadvantages comparison

Steganography	Cryptography
Unknown message passing	Known message passing
Little Known Technology	Common Technology
Technology still being developed for certain formats	Most algorithms known to government departments
Once detected message is known	Strong algorithm are currently resistant to brute force attack large expensive computing power required for cracking technology increase reduces strength

6. The Proposed System

Individually, both steganography and cryptography techniques are insufficient for completing information security; therefore, the two techniques are being combined to achieve reliable and strong mechanism [1-9]. The proposed system based on combining these techniques. This can maintains the requirements used for security and robustness in order to transmit important information. The proposed system use cryptography technique based on RSA to encrypt the secret information then hidden it in the covering image using LSB steganography technique. The proposed system algorithm is illustrated in Figure (2):

Sender side

The secret information (message) is encrypted according to RSA to generate encrypted message using public key. Then both encrypted and public key are embedded into cover image. Many procedures for hiding process are used for system evaluation. These procedures are covered in result paragraph.

Receiver side

1. Both encrypted message and public key are extracted from stego image based on inverse LSB steganography. Then use public key to generate private key according to RSA algorithm.
2. The original secret information is recovered by decrypting the extracted message.

Table (2), lists the algorithm steps for encrypting and embedding secret message (like text or image) into a cover image.

Table (3), lists the algorithm steps for extract and decrypt of the secret message from the stego image.

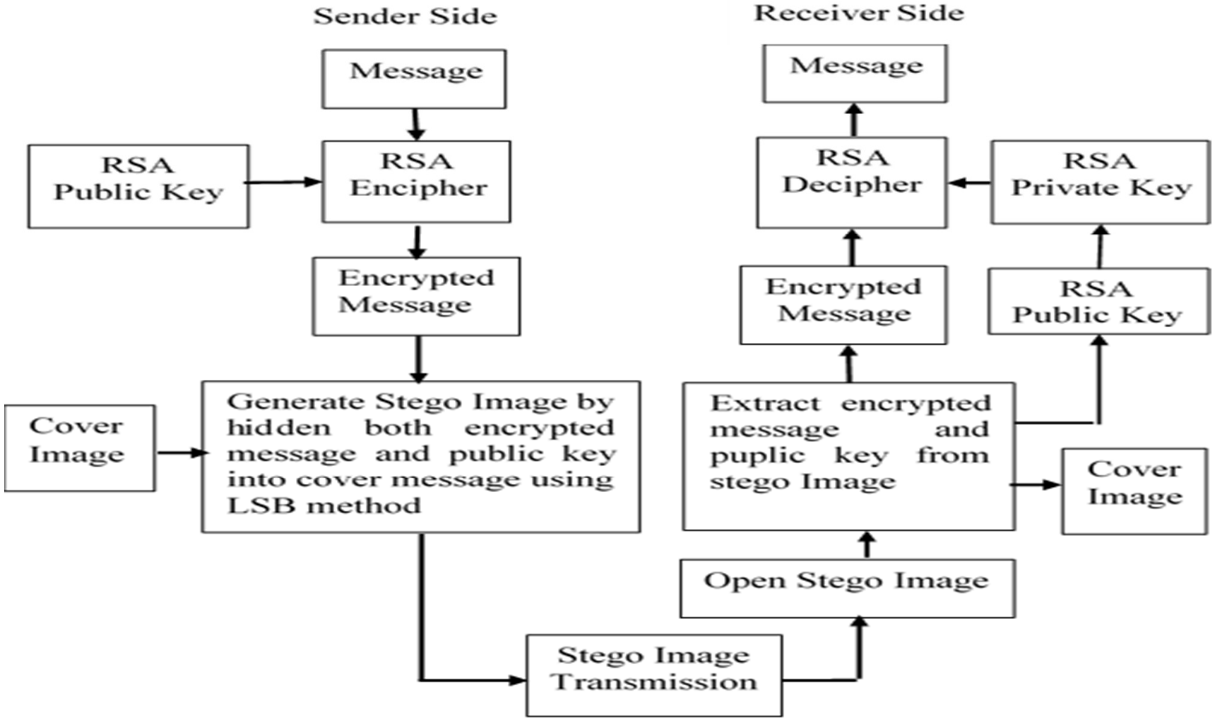


Fig. 2. Proposed system structure.

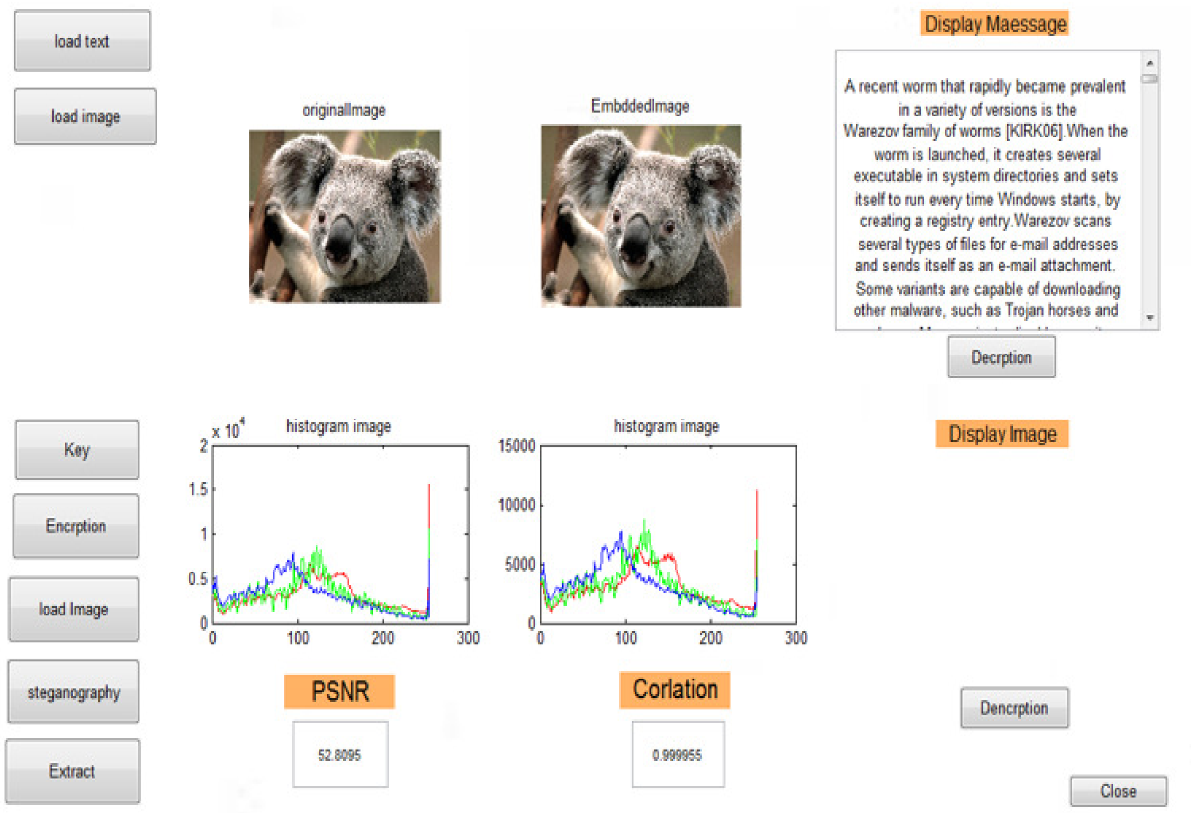
Table 2,
Embed Algorithm steps

Step	Process
1	Read the cover image (gray or RGB color) and secret message (text or image)
2	Convert the secret message (like text or image) to binary. The alphabets of text are convert into binary by encode them according to ASCII code. The image pixel values are encoded according Uint8 format.
3	Generate public key using RSA criteria.
4	Encrypt secret message using RSA encipher
5	Replace one by one each LSB pixel of cover image (gray or RGB color) with secret message bits.
6	Embedding public key into specific LSB pixel of cover image. After completing steps (5, 6), the result is stego image.
7	Transmit stego image on web.

Table 3,
Retrieve Algorithm steps

Step	Process
1	Read the stego image.
2	Extract both encrypted secret message and public key from stego image.
3	Use public key to generate private key according to RSA criteria.
4	Decrypt the secret message using private key and decipher RSA.
5	Convert each 8 bits into a character or an image pixel value to retrieve the original secret message like text or image.
6	Display the secret message on screen.

The proposed system is implemented using MATLAB. Develop interactive screen shown in Figure (3) to make the system easier to use. The interactive screen enable the user to read and display both the cover image and secret message (may be text or image). All embedded and extracted processes (such as generation of public key, encryption and decryption of secret message, and stego image generation, are all done directly by on clicking on specific bottoms. Also, all the evaluation measurements, such as histograms, PSNR and correlation, are calculated and displayed.

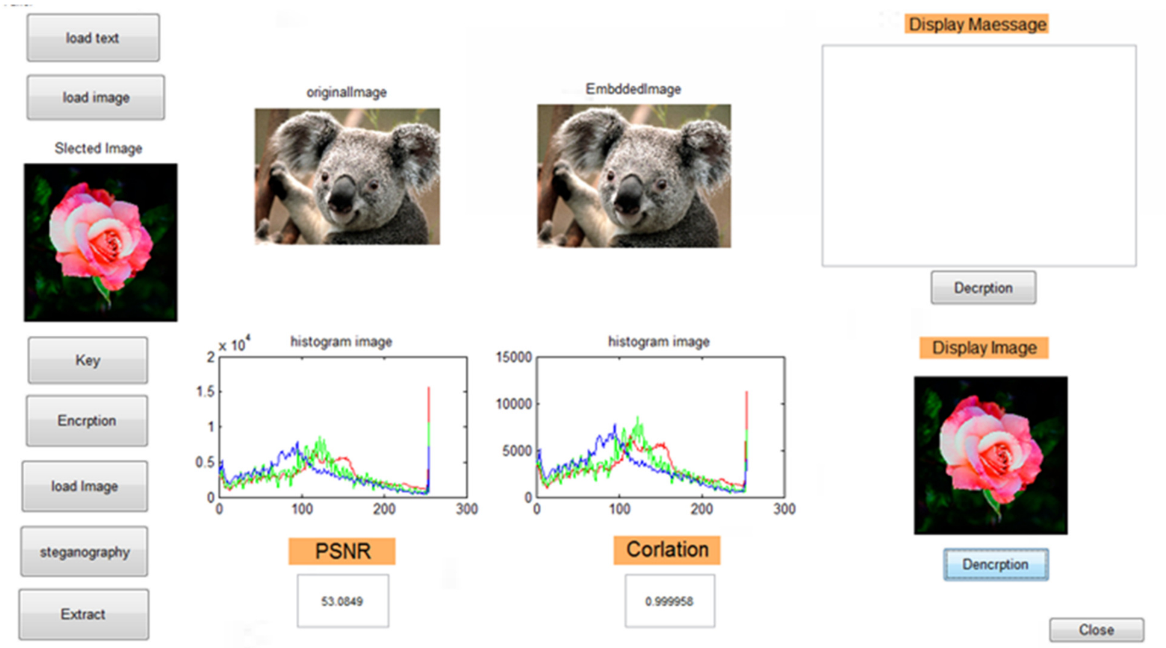


A recent worm that rapidly became prevalent in a variety of versions is the Warezov family of worms [KIRK06].When the worm is launched, it creates several executable in system directories and sets itself to run every time Windows starts, by creating a registry entry.Warezov scans several types of files for e-mail addresses and sends itself as an e-mail attachment. Some variants are capable of downloading other malware, such as Trojan horses and

PSNR 52.8095

Corlation 0.999955

A) Embed text into image.



PSNR 53.0849

Corlation 0.999958

B) Embed image into image.
Fig. 3. Interactive display screen for the proposed system.

7. Results

To evaluate the system, select a cover image: RGB color of size 1024x768 or 768 KB which is sufficient as a hidden media. The system is tested to hidden both text and images. The hiding process is done in different ways as shown:

1. Firstly, hiding secret message bits one by one into a one bit of pixels of cover image like in 1st LSB, 2nd LSB, 3rd LSB or 8th LSB.
2. Secondly, hiding randomly in one of 3 first LSB (1st, 2nd, 3rd bit LSB).

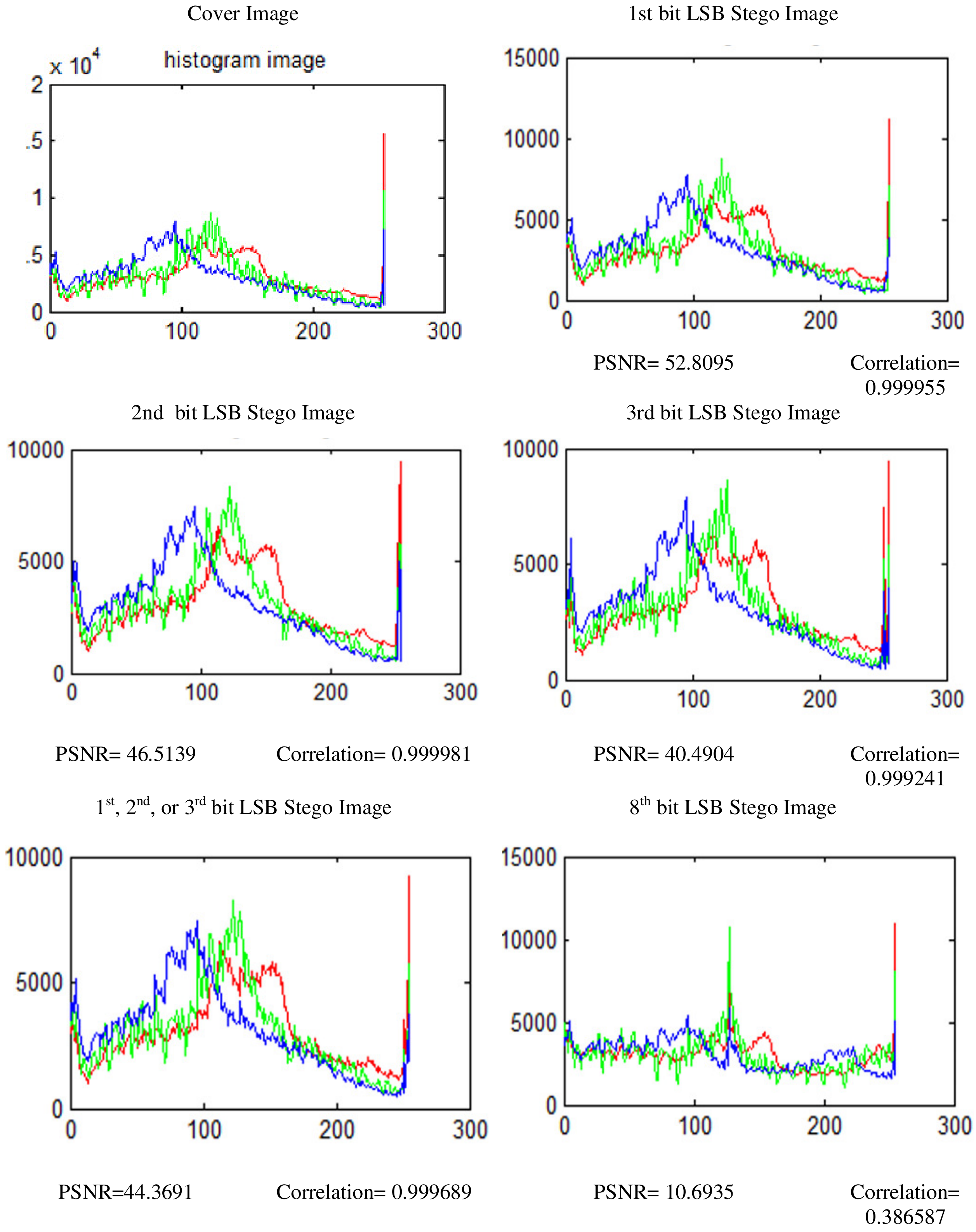
For each hiding process, PSNR and correlation are calculated as shown in Table (٤) and Table (٥). Also the three histograms of R, G, and B colors for both cover image and stego image are drawn. The evaluation results for hidden secret text of 104 KB are shown in Figure (4). While the evaluation results for hidden secret color image of (98.3 KB) are shown in Figure (5).

Table 4,
PSNR and correlation results for hidden secret text of (104 KB)

Image	Cover Image Size	Hidden image Size		PSNR	Correlation
1	1024*768	1024*104	**1st bit LSB**	52.8095	0.999955
2	1024*768	1024*104	**2nd bit LSB**	46.5139	0.999981
3	1024*768	1024*104	**3rd bit LSB**	40.4909	0.999241
4	1024*768	1024*104	**1st, 2nd, 3rd bit LSB**	44.3691	0.999689
5	1024*768	1024*104	**8th bit LSB**	10.6935	0.386587

Table 4,
PSNR and correlation results for hidden secret color image of (98.3 KB)

Image	Cover Image Size	Hidden image Size		PSNR	Correlation
1	1024*768	1024*98.3	**1st bit LSB**	53.0849	0.999958
2	1024*768	1024*98.3	**2nd bit LSB**	46.7707	0.999822
3	1024*768	1024*98.3	**3rd bit LSB**	40.7585	0.999288
4	1024*768	1024*98.3	**1st, 2nd, 3rd bit LSB**	44.0844	0.999668
5	1024*768	1024*98.3	**8th bit LSB**	10.7022	0.383604



Cover Image

1st bit LSB Stego Image

PSNR= 52.8095 Correlation= 0.999955

2nd bit LSB Stego Image

PSNR= 46.5139 Correlation= 0.999981

3rd bit LSB Stego Image

PSNR= 40.4904 Correlation= 0.999241

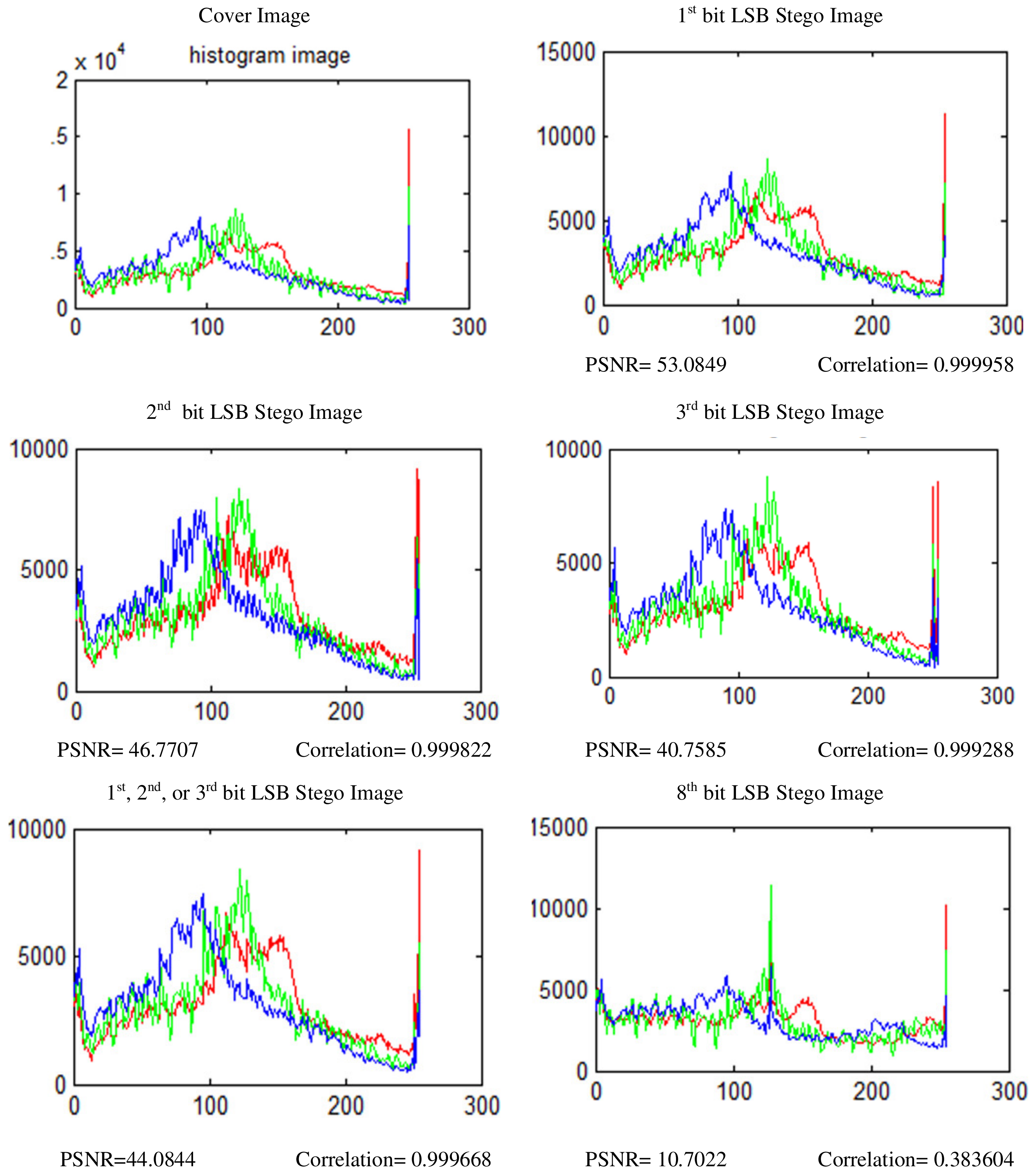
1st, 2nd, or 3rd bit LSB Stego Image

PSNR=44.3691 Correlation= 0.999689

8th bit LSB Stego Image

PSNR= 10.6935 Correlation= 0.386587

Fig. 4. Evaluation results for hidden secret text of (104 KB).



Cover Image

1st bit LSB Stego Image

PSNR= 53.0849 Correlation= 0.999958

2nd bit LSB Stego Image

3rd bit LSB Stego Image

PSNR= 46.7707 Correlation= 0.999822

PSNR= 40.7585 Correlation= 0.999288

1st, 2nd, or 3rd bit LSB Stego Image

8th bit LSB Stego Image

PSNR=44.0844 Correlation= 0.999668

PSNR= 10.7022 Correlation= 0.383604

Fig. 5. Evaluation results for hidden secret color image of (98.3 KB).

8. Conclusion

After studying the proposed stego-system, steganography message can be embedded into digital images in ways that are imperceptible to the human eye. In other words, a stego-image that is generated by the present algorithm has to be normal for human vision and cannot be detected to avoid visual attack.

The results indicate that the suggested steganography system is more secure as a result of the use of the RSA encryption. However, the time required to embed/extract the secret message is increased as a result of the encryption/decryption computation. Clearly, the results indicate that there do not notice any change in quality between cover image and stego image when embed the secret message in low LSB: 1st LSB, 2nd LSB, or 3rd LSB of cover image. Whenever increasing the amount of data stored is increased, the level of LSB increased. Also the value of PSNR and Correlation decreased gradually and this means that the cover image quality is decreased (small increasing in distortion).

After comparing histogram of the cover image with the stego image, it is quite clear that histogram of stego image is almost similar to cover image with a change of only last bit of pixels. So this method is capable of producing a secret embedded image that is totally indistinguishable from the original image by the human eye and can't be detected by histogram analysis method.

9. References

[1] M. Gajalakshmi and R. Vidya, "A Review on-Data Hiding using Cryptography and Steganography," International Journal of Computing Algorithm, vol. 07, Issue: 01, pp. 24-28, June 2018.

[2] Mustafa S. T., Mohd S.M.R., Sameer L., Mohammed M.H., Hassanain M. A., "Combination of Steganography and Cryptography: A short Survey," 2nd International Conference on Sustainable Engineering Techniques (ICSET), doi:10.1088/1757-899X/518/5/052003, 2019.

[3] Manoj K. R., Dinesh G. and Naveen H., "Data Hiding In Image Using Cryptography And Steganography: An Investigation," International Journal of Advanced Research in Computer Science, vol. 8, no. 7, pp. 953-956, July – August 2017.

[4] Dheyab Salman Ibrahim, "Enhancing Cloud Computing Security using Cryptography & Steganography," Iraqi Journal of Information Technology, vol. 9, no. 3, 2019.

[5] Marwa E. Saleh, Abdelmgeid A. Aly, Fatma A. Omara, "Data Security Using Cryptography and Steganography Techniques," (IJACSA) International Journal of Advanced Computer Science and Applications, vol. 7, no. 6, pp. 390-397, 2016.

[6] Shambhavi U. Burge, Nitin A. Sawant, Swapnil D. Choudhari, Priyanka A. Sonkusare, "Secure Data Hiding using Cryptography and LSB Techniques," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), vol. 4, Issue 10, pp. 3863-3870, Oct. 2015.

[7] Ameer H. Morad, Hatem Nahi Mohaisen, "Secret Message Hiding Randomly In Video," International Journal of Advancements in Computing Technology (IJACT), vol. 8, no. 3, June 2016.

[8] Hatem Nahi Mohaisen, Ameer H. Morad, "Secure Information Using Steganography and Watermarking," Iraqi Journal of Science, vol. Special Issue Part-A, pp. 112-128, 2016.

[9] Mustafa S. Taha, et al, "Combination of Steganography and Cryptography: A short Survey," 2nd International Conference on Sustainable Engineering Techniques (ICSET), appear in IOP Conf. Series: Materials Science and Engineering 518, 2019.

[10] Shireen Nisha, Mohammed Farik, "RSA Public Key Cryptography Algorithm – A Review," International Journal of Scientific & Technology Research, vol. 6, issue 07, pp. 187-191, July 2017.

[11] Dindayal Mahto, Dilip Kumar Yadav, "Performance Analysis of RSA and Elliptic Curve Cryptography," International Journal of Network Security, vol. 20, no. 4, pp. 625-635, July 2018.

[12] Divya.A1, S.Thenmozhi, "Steganography: Various Techniques In Spatial and Transform Domain," International Journal of Advanced Scientific Research and Management, vol. 1, issue 3, March 2016.

[13] Ammar Awad, "A Survey of Spatial Domain Techniques in Image Steganography," Journal of Education College Wasit University, vol. 26, Jan. 2018.

[14] Marwa M. Emam, Abdelmgeid A. Aly, andFatma A. Omara, "An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection,"

(IJACSA) International Journal of Advanced Computer Science and Applications, vol. 7, no. 3, pp. 361-366, 2016

[15] Harpreet Kaur and Jyoti Rani, “A Survey on different techniques of steganography,” MATEC Web of Conferences, doi: 10.1051/ 57, 02003, 2016.

[16] S. Udhayavene∗, Aathira T. Dev and K. Chandrasekaran, “New Data Hiding Technique in Encrypted Image: DKL Algorithm (Differing Key Length),” Procedia Computer Science 54, pp. 790 – 798, 2015.

[17] Yifeng Sun, Fenlin Liu, “Selecting Cover for Image Steganography by Correlation Coefficient,” 2010 Second International Workshop on Education Technology and Computer Science, 2010.

[18] Anita Pradhan, et al., “Performance evaluation parameters of image steganography techniques,” International Conference Research Advances in Integrated Navigation Systems (RAINS), 2016.

[19] S. Tanako, K. Tanaka and T. Sugimura, “Data Hiding via Steganographic Image Transformation,” IEICE Trans. Fundamentals, vol. E83-A, pp. 311-319, Feb. 2000.

[20] Haripriya Rout, Brojo Kishore Mishra, “Pros and Cons of Cryptography, Steganography and Perturbation techniques,” IOSR Journal of Electronics and Communication Engineering (IOSR-JECE), e-ISSN: 2278-2834, p.p. 76-81.

تحسين وتعزيز امن النظام باستخدام خوارزميات (LSA & RSA)

منى مصطفى حمادي* أمير حسين مراد**

*،**قسم هندسة المعلومات والاتصالات/ كلية الهندسة الخوارزمي/ جامعة بغداد

*البريد الالكتروني:muna@kecbu.uobaghdad.edu.iq

**البريد الالكتروني: ameer@kecbu.uobaghdad.edu.iq

الخلا□ة

علم إخفاء المعلومات يقو□ بإخفاء المعلومات التي قد تكون ملفًا أو رسالة أو صورة أو فيديو ضمن معلومات أخرى. علم التشفير هو علم تحويل المعلومات من نموذج قابل للقراءة إلى نموذج غير قابل للقراءة لشخص غير مصرح له. تكمن المشكلة الرئيسية في النظ□ الاختزالي في التضمين في بيانات الغلاف دون تقديم معلومات من شأنها تسهيل إزالتها. في هذا البحث، تم اقتراح طريقة لتضمين البيانات في الصور تستخد□ أسلوب إخفاء البايت الأقل أهمية (LSB) والتشفير (خوارزمية RSA) لحماية البيانات. سيتم تعزيز أمان النظ□ نتيجة لهذا التعاون بين علم إخفاء المعلومات والتشفير.