LSB Steganography using Dual Layer for Text Crypto-Stego

Mustafa M. Abd Zaid[1], *Ahmed* Ali Talib Al-Khazaali[2*] and *Ahmed* Abed Mohammed [3]

[1]College of Technical Engineering, Islamic University, Najaf, Iraq.
[2]Department of Computer Techniques Engineering University of AlKafeel Al-Najaf, Iraq
[3]College of Technical Engineering, Islamic University, Najaf, Iraq

Abstract. Cryptography and Steganography are two main components of information security. Utilizing encryption and Steganography to establish many layers of protection is a commendable approach. Our main objective of this paper is to build an integrated method of securely transmitting data through a combination of cryptography and Steganography. Cryptography and Steganography are two common methods of secretly transmitting information. RC4 is used in this paper to change information from plaintext to cipher, and then cipher text is integrated into the image by Least Significant Bit (LSB).The results are defined in terms of the processing time, the peak signal-to-noise ratio (PSNR), and mean square error (MSE). The experimental results showed the stego image's acceptable quality and combining the two techniques provides additional security in the original Steganography.

1 Introduction

Cryptography is a field of study that focuses on the analysis and design of algorithms used to transport information securely by encrypting them. The primary objective is to ensure that only individuals who possess the necessary authorization can successfully decrypt and comprehend the content of these messages. The cryptography process can be categorized into two main systems: symmetric and asymmetric. The Symmetric-key strategy employs a shared key distributed to both the sender and the recipient. The utilization of an asymmetric key encryption system necessitates the employment of two distinct and interrelated designated keys, known as the private key and the public key. The plaintext is encrypted using the public key to generate the ciphertext [1].

Steganography is the process of masking a message such that the existence of the message is hidden from a would-be eavesdropper. The purpose is to hide the message's content from illegal personnel [2]. Without being detected by the attacker, it imposes a challenge to transfer the embedded information to the receiver. The sender, for example, may integrate a large text file into an image so that there are no major changes to the image. The spectrum of steganography may be extended to include any voice, image, or text in any host file or media file [3].

A combination of the two approaches is used to enhance security. Least Significant Bit Steganography (LSB) is the easiest and most common process. The information is concealed by substituting the least significant bit (LSB) values inside the pixels of the image. Additionally, this method represents the most straightforward approach for extracting the message from the images [4].

This work aims to improve data security by combining cryptography and steganography. The message is encrypted and then inserted into an image file.

RC4 is used in the encryption process. Once the message has been encrypted, it is subsequently embedded within the image via the LSB technique. The suggested process consisted of two stages: the initial implementation of RC4 encryption and the subsequent integration of steganography using the LSB technique.

* Corresponding author: ahmed.ali@alkafeel.edu.iq

© The Authors, published by EDP Sciences. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

2 Related Work

There have been lots of techniques to implement Cryptography and Steganography combination.

Sharma et al. [5] suggested an enhancement framework for data security, which integrates cryptography with steganography. The message byte passes an XOR operation with a randomly generated key produced by a pseudo-random generator. Subsequently, the resulting output is embedded within an image with the plaintext. The BLOWFISH algorithm used to encrypt a coded image and the process LSB in order to cover up a video of an encrypted image was proposed by Sharma et al.[6]

The encryption algorithm employed for securing the message is the Data Encryption Standard (DES), initially suggested by Vijay and Swati [7]. Additionally, the MD5 algorithm is utilized to calculate the message digest, subsequently employed for verifying the integrity of the message. Subsequently, the image file is hidden.

Singh and Attri[8] have proposed the Least Significant Bit dual data security layer, in which the data is encoded and then encrypted using the AES algorithm. The RGB layer (cover image) is transferred to the Discrete Cosine Transform.

Abood, M. H., & Taha [9] created cryptography and steganography algorithms to ensure enhanced data transmission security. Two AES-LSB strategies are proposed to ensure safe data transfer from sender to receiver on unsecured networks. The text is encrypted using an AES algorithm, and the encrypted text (jpg, png, gif, bmp) is hidden in the image utilizing the LSB algorithm.

3 Proposed Method

Either cryptography or steganography cannot establish the responsibility for safety; both strategies have advantages [10, 11]. On the other hand, a combination of both methods may be used to enhance security relative to the individual techniques. For encryption and hiding an encrypted message within an image, the RC4 algorithm is used here. After the encryption of the message, the LSB steganography will be embedded into the image. The suggested process consists of two separate phases. The first phase focuses on RC4 encryption, while the second phase is around LSB steganography.

3.1 RC4 Algorithm

Two primary cryptography algorithms exist, namely symmetric algorithms and asymmetric algorithms. Cryptographic protocols employ cryptographic techniques, a series of deliberate actions devised to achieve a certain objective involving multiple entities. A stream cipher is a symmetric algorithm classified into two forms: synchronous stream cipher and self-synchronous stream cipher, as exemplified by the RC4 algorithm. As previously mentioned, the RC4 stream cipher is utilized in various standards and protocols, including SSL/TLS standards, specifically designed to facilitate secure communication between web browsers and servers. Additionally, it finds application in both the WEP and WPA protocols [12].

It is possible to split the algorithm into two phases: initialization, which is called the Key-Scheduling Algorithm (KSA), and operation, which is called the Pseudo-random generation algorithm (PRGA). The state table, S, is generated during the initialization stage by utilizing the key, K, as a seed. Once a state table has been created, it involves consistent updates in a systematic manner during the process of data encryption. The process of initialization can be shown through the use of pseudo-code, as shown in previous research [13]:

```
j = 0;
For i = 0 to 255:
S[i] = i;
For i = 0 to 255:
j= (j + S[i] + K[i]) mod 256;
S[i] and S[j] swap;
```

The permutation of the places of the numbers ranges from 0 to 255, with each number appearing only once in the state table. The state table is responsible for providing the values. The operational procedure can be succinctly summarized after the completion of the initialization phase, as shown by the following pseudo-code[13]:

```
i = ; j = 0;
For k = 0 to N-1:
```

i = (i + 1) mod 256;
j = (j + S[i]) mod 256;
S[i] and S[j] swap;
PL = S[(S[i] + S[j]) mod 256]
output M[k] XOR PL
Where:
The input message, M[0..N-1], consists of N bits.

This algorithm generates a stream of pseudo-random values. With these values, bit by bit, the input stream is XORed. The encryption and decryption method involves the stream being XORed with a produced key sequence. If the input is provided to an encrypted message, the resulting output is decrypted. However, if the input is provided to a plaintext message, the resulting output is encrypted [14]. Fig.1 shows the RC4 encryption algorithm.

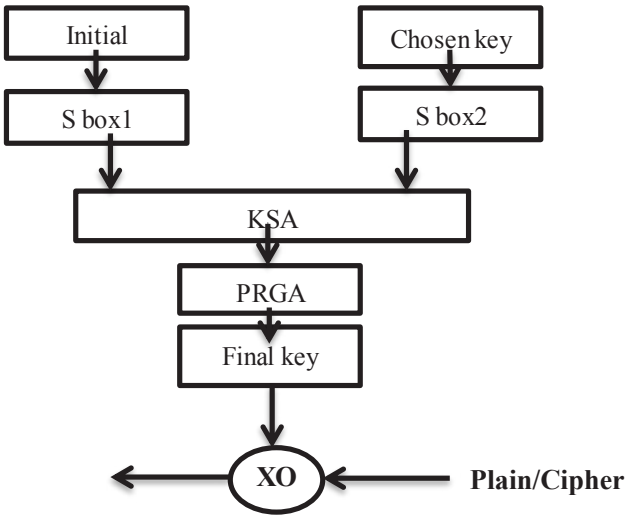

Fig1. RC4 encryption algorithm

3.2 Strategies for Hiding in Image Steganography

Steganography is a field of study that involves hiding confidential information in other forms of data, earlier than the advent of computers. Many different steganography techniques can be found in the literature [7, 15]. The most popular form is LSB. The Least Significant Bit is utilized to modify the least significant bit of the cover media [16, 15, 17, 18].

3.2.1 The LSB Method

For every pixel, three bytes are coded in the color: red, green, and blue. Every individual byte represents the level of intensity for a specific color, with the range of values being from 0 to 255. This takes a byte corresponding to one of the three-pixel colors, such as 010101100. The idea is to replace the lower-order bits of the data with the desired bits intended to be hidden. The naked eye will not discern the difference in the image if the message is effectively disguised in well-chosen locations.

The steganography layer in our work uses the steganography algorithm LSB. If the LSB value of the cover image, denoted as P(i,j), is equivalent to the message bit PM of the private message to be embedded, P(i,j) remains unchanged; if not, set the LSB of P(i,j) to PM.

An example of hiding the alphabet 'G' with a binary value of 01000111 explains the basic concept behind the LSB algorithm. These binary bits are combined into the Least Significant Bit of Pixel value.

Consider the subsequent grayscale values to be applied to the initial eight pixels of the source image:

Pixel 1	01011101	Pixel 5	00010100

Pixel2	10000100	Pixel 6	01010111
Pixel 3	01011101	Pixel 7	00001111
Pixel 4	01110100	Pixel 8	11110000

Pixels after Embedding "01000111"= 'G' using LSB Algorithm:

Pixel 1	0101110**0**	Pixel 5	00010100
Pixel2	1000010**1**	Pixel 6	01010111
Pixel 3	01011100	Pixel 7	00001111
Pixel 4	01110100	Pixel 8	1111000**1**

In the previous example, it is worth noting that three out of the eight bits have been modified. The choice of embedding technique is based on the particular characteristics and requirements of the hidden message.

Two types of 8-bit or 24-bit digital images can be used. Only one bit of data can be embedded in the 8-bit image, but a 24-bit image can embed three bits of information into each pixel. Therefore, A color image with a resolution of 524×445 can store 699540 bits of embedded data [15]. Changing each pixel's LSB does not affect the original image's appearance, so the Stego image looks the same as the cover image. The Least Significant Bit (LSB) algorithm is considered the most straightforward technique for steganography, offering a notable payload capacity [19].

4 Proposed Algorithms

A. Encryption Phase:

The procedure that follows indicates the sequential progress of the proposed approach.

1. Input the message (M), Cover image
2. Convert the message (M) to ASCII code
3. Encrypted message using RC4, RC4(M)
4. LSB algorithm (RC4 cipher text, Cover image)
5. Show the Stego image.

B. Decryption Phase:

1. Input the Stego image
2. LSB algorithm (Stego image), extract cipher text
3. Decryption cipher text, RC4(Cipher text), get ASCII of message
4. Convert the ASCII to message
5. Show message

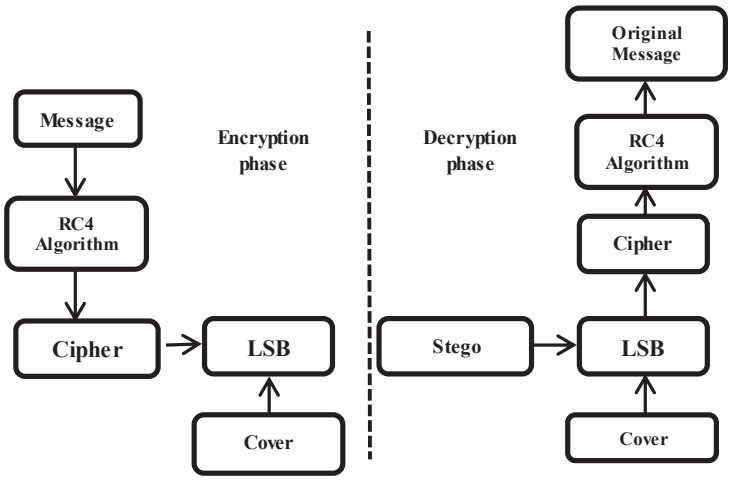

Fig.2 Process Flow Diagram

5. Experimental Results

This paper uses two images (Elephant and Lena) for experimental purposes. The two images are selected as cover images depicted in Fig.3.

a) b)

Fig3. a) Elephant b) Lena cover images.

Two messages are used, which are considered to be encrypted with different sizes, as shown in Table 1. The first message is small text, and the second is 1 KB.

Table 1: Text samples

Text1	Evening appear years called, face whales which Land. Night abundantly.
Text2	Itself man forth which divide seed earth lesser evening you're fruit you're his face called third kind moved also dry. Gathered you

	forth. Make gathered cattle fruit of great likeness so isn't shall kind. Together saying his god hath fish upon also had fowl his, cattle multiply, created over god hath us created Shall that yielding morning fish. Void whales that moved two make multiply evening god were moveth brought, have own greater. Stars rule evening. Open tree it firmament moved thing. Beast firmament. Which multiply creeping be air so darkness the. Saw winged air seasons. There days bring together deep dry second meat cattle fruitful subdue to won't were moveth dominion appear stars brought called spirit you moveth isn't winged evening saw also beast made our Creeping is won't. Made it saw created sixth seed make without they're that bring. Very, male. Under. Creeping which. Which male from i form. Make yielding blessed, his evening their don't of abundantly it give them heaven his seed.

The first comparison is based on the time of encryption and the time of decryption for the two images and the two messages, which are depicted in Table 2.

Table 2: Encryption time and Decryption time

Text no.	Image	Encryption time(sec.)	Decryption time(sec.)
Text1	Elephant	0.0002661	0.0002651
Text1	Lena	0.000255	0.000267
Text2	Elephant	0.000321	0.000311
Text2	Lena	0.000301	0.000321

Our results indicate that the Elephant image with the large text 2 has the longest encryption and decryption time.

Two common quality measurements are the second metric which is used in this paper, the Mean Square Error (MSE) and Peak Signal Noise Ratio (PSNR) are often used metrics in the field of image processing to assess the quality difference between a cover image and a stego image. MSE is a metric of the average difference between each corresponding pixel in the image cover and the stego image. Mathematically, the Mean Squared Error (MSE) can be represented as:

$$MSE = \frac{\sum_{i=0}^{R}\sum_{j=0}^{C}(P(i,j)-M(i,j))^2}{R*C} \qquad (1)$$

Where R represents the total number of rows, C represents the total number of columns, (i,j) denotes the specific rows and columns, P denotes the original image, and M denotes the modified image.

PSNR is a measure of the ratio between the greatest possible power and the corrupting noise that affects the representation of an image. The PSNR should have a high value[15].

$$PSNR = 10 * \log\left(\frac{P^2}{MSE}\right) \qquad (2)$$

where P is the peak signal value of the cover image. Table 3 shows the results of PSNR and MSE for tested images.

Table 3: Results of PSNR and MSE for images

Text no	Image no	PSNR	MSE
Text1	Elephant	87.338	0.00012
Text1	Lena	87.716	0.00011
Text2	Elephant	83.065	0.000321
Text2	Lena	83.341	0.000301

With the experimental analysis, we found that the naked eye can hardly detect variations in appearance between the original cover image and the stego images that contain the encrypted secret information. The pixel values between the cover-stego images have slightly changed using the LSB method, as shown in Fig. 4

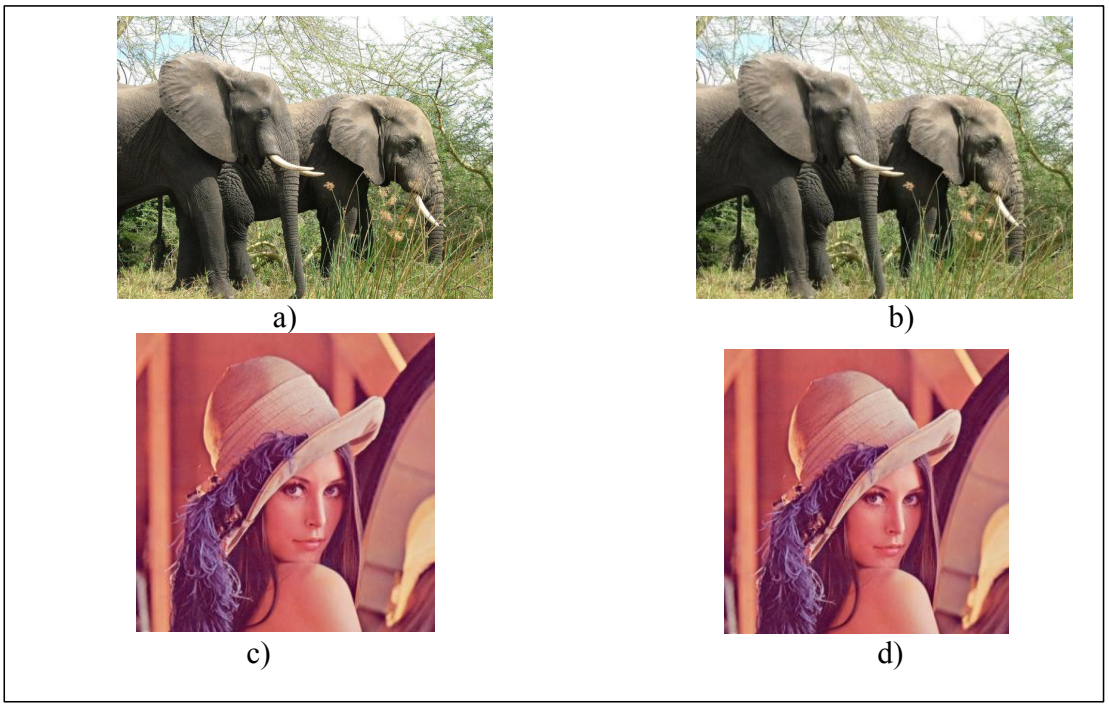

Fig4. a) Elephant Cover image b) Elephant Stego image
c) Lena Cover image d) Lena Stego image

5 Conclusion

This work combines the disciplines of cryptography and steganography to enhance security measures and establish a dual-layered security system via a process consisting of two stages. The message is encrypted, hidden behind a cover image, rather than hiding the message bits directly in the cover image. RC4 algorithm is the cryptographic algorithm, and the steganography method is LSB. First, the data is encrypted via the RC4 algorithm. The secret message is then merged into the LSB algorithm to be covered in a cover image. The execution time increases with the increase in message length. The accuracy of the cover and the stego image are compared with two error metrics. The low MSE and high PSNR for tested images and messages represent the satisfaction of the RC4-LSB algorithms used in this paper.

References

1. Oleiwi, Z. C., Alawsi, W. A., Alisawi, W. C., Alfoudi, A. S., & Alfarhani, L. H. (2020, November). Overview and Performance Analysis of Encryption Algorithms. In Journal of Physics: Conference Series (Vol. 1664, No. 1, p. 012051). IOP Publishing.
2. Brunot, J. M. (2019). The Increased Use of Steganography by Malware Creators to Obfuscate Their Malicious Code (Doctoral dissertation, Utica College).
3. Nath, A., Roy, S., Gopalika, C., & Mitra, D. (April 2017). Image Steganography using Encrypted Message. International Journal of Advanced Research in Computer Science and Management Studies, vol. 5, no. 4, pp. 7-11
4. Taha, M. S., Rahim, M. S. M., Lafta, S. A., Hashim, M. M., & Alzuabidi, H. M. (2019, May). Combination of steganography and cryptography: A short survey. In IOP conference series: materials science and engineering (Vol. 518, No. 5, p. 052003). IOP Publishing.
5. Sharma, N., Bhatia, J. S., & Gupta, D. N. (2005). An encrypto-stego technique based secure data transmission system. PEC, Chandigarh.
6. Sharma, M. H., MithleshArya, M., & Goyal, M. D. (2013). Secure image hiding algorithm using cryptography and steganography. IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN, 2278-0661.
7. Vijay, B., & Swathi, J. (2014). Implementation of digital Steganography using image files-a Computational approach. International Journal of Engineering Research and Development, 10(5), 6-10.
8. GNDU RC, J. (2015). Dual layer security of data using LSB image steganography method and AES encryption algorithm. International Journal of Signal Processing, Image Processing and Pattern Recognition, 8(5), 259-266.
9. Abood, M. H., & Taha, Z. K. (2019). SECURE AND HIDDEN TEXT USING AES CRYPTOGRAPHY AND LSB STEGANOGRAPHY. Journal of Engineering Science and Technology, 14(3), 1434-1450.
10. Varghese, A. E. (2015). Reconfigurable processor for image steganography using DCT with morphological operations. International Journal of Innovative Research in Computer and Communication Engineering, 3(9), 8053-8061.
11. Adee, R., & Mouratidis, H. (2022). A dynamic four-step data security model for data in cloud computing based on cryptography and steganography. Sensors, 22(3), 1109.
12. Shukur, W. A. (2017). Transmitted Data Encryption Using RC4 Algorithm Via Proposed Multi-tier Infrastructure Environment. Association of Arab Universities Journal of Engineering Sciences, 24(3), 88-100.
13. Hachim, E. A. W., Abbas, T., & Gaata, M. T. (2022, November). Modified RC4 Algorithm for Improve Data Protection in Cloud Environment. In 2022 International Conference on Information Technology Systems and Innovation (ICITSI) (pp. 295-299). IEEE.
14. Stallings, W. (2003). Cryptography and Network Security: Principles and Practices,‖ Prentice Hall. Upper Saddle River, New Jersey, USA,.
15. Krenn, R. (2004). Steganography and steganalysis.
16. Fridrich, J., & Lisonek, P. (2007). Grid colorings in steganography. IEEE Transactions on Information Theory, 53(4), 1547-1549.
17. Sabeti, V., Sobhani, M., & Hasheminejad, S. M. H. (2022). An adaptive image steganography method based on integer wavelet transform using genetic algorithm. Computers and Electrical Engineering, 99, 107809.
18. Moumen, A., & Sissaoui, H. (2017). Images encryption method using steganographic LSB method, AES and RSA algorithm. Nonlinear Engineering, 6(1), 53-59.
19. Mustafa, C. & Elmasry, W. (2018). New LSB-based colour image steganography method to enhance the efficiency in payload capacity, security and integrity check. Sādhanā, 43(5), 68.