Available online at www.qu.edu.iq/journalcm
JOURNAL OF AL-QADISIYAH FOR COMPUTER SCIENCE AND MATHEMATICS
ISSN:2521-3504(online) ISSN:2074-0204(print)

New Steganography Technique by Integrating Genetic Algorithm and Data Hiding

***Shahbaa Mohammed Abdulmaged* [a]*, *Nadia Mohammed Abdulmaged* [b], *Saba Abdulbaqi Salman* [c]**

[a] *Al-Iraqia University, Baghdad, Iraq . Shahbaa.abdulmaged@aliraqia.edu.iq:*

[b] *University of Baghdad, Baghdad, Iraq . Nadya.m.a@ihcoedu.uobaghdad.edu.iq:*

[c] *Al-Iraqia University, Baghdad, Iraq .sabasalman2019@gmail.com:*

ARTICLE INFO

Article history:
Received: 13 /04/2024
Rrevised form: 12 /06/2024
Accepted : 23 /06/2024
Available online: 30 /06/2024

Keywords:

Cryptography,
genetic algorithm,
steganography,
data protection,
security

ABSTRACT

There is a great need of internet applications that involves data to be sent in an extra safe way. Steganography and cryptography help in providing data safety. Steganography hides the existence of message by inserting data in some other digital media and Cryptography transforms data in to cipher object that can be in unreadable form to normal user. To resume the defense of data defeating and communication over internet, this paper suggests a hybrid heuristic, integrating a genetic algorithm and steganography technique to efficiently solve this problem.

Computational results show that the suggested technique can significant improvement the performance of a genetic algorithm for this problem, this was proven by the results of the comparison between the suggested technique and several other proposed systems. Genetic Algorithm is used for pixel variety of image where secret data is to be hidden so that detection of secret data become multifarious.

MSC..

https://doi.org/10.29304/jqcsm.2024.16.21547

1. Introduction

Many efforts have already been made in the modern era to protect data. Passwords and data cryptography are the most popular and straightforward methods for securing data [1]. While many other forms of protection can be employed, these methods are somewhat secure in preventing an intruder from obtaining crucial information. However, they typically have a significant drawback: the mere evidence of concealment may be enough to prompt the invaders to begin their pursuit of the information. This drawback is not present with the picture hiding procedure. A significant portion of the population sends images with their messages. Crackers might not even realize there is pertinent information inside the message if crucial information can be concealed inside a picture without affecting its quality to the point where it can be perceived. Steganography then prevents hackers from intercepting the message

*Corresponding author

Email addresses: Shahbaa.abdulmaged@aliraqia.edu.iq

Communicated by 'sub etitor'

and attempting to bypass the security measures [2], in addition to safeguarding the data by encoding it inside the picture.

The paper is organized as follows. In section 2 & 3, we discuss a basic concept of genetic algorithm and how can we use it in the suggested technique and RSA algorithm respectively. The suggested technique is presented in section 4. In section 5, we present the main concepts of MSE and PSNR. The experimental results are represented in section 6. Finally, in Section 7, the conclusion to the suggested technique is commented.

2. Genetic Algorithm

Steganography's capacity or imperceptibility can be increased by using Genetic Algorithms (GA) [3]. A GA evolutionary approach was proposed to create safe steganography encoding on JPEG images.

In this technique, the GA is used to determine the segment scanning mode in the image and starting segment in the scanning, in a manner to get an image with the highest quality of the stego-image. For each image, 9 scanning mode can be take into account. For example, the scanning for an image of 3×3 size is shown in Fig. 1.

1	2	3	3	2	1	1	2	3
4	5	6	6	5	4	6	5	4
7	8	9	9	8	7	7	8	9
3	2	1	1	4	7	1	6	7
4	5	6	2	5	8	2	5	8
9	8	7	3	6	9	3	4	9
3	6	9	3	4	7	7	8	9
2	5	8	2	5	8	4	5	6
1	4	7	1	6	9	1	2	3

Fig. 1- 9 scanning mode for an image of 3×3 size

3. RSA

MIT's Rivest, Shamir, and Adelman provided the algorithm. Using the RSA algorithm (RSA algorithm is an asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. Public Key and Private Key. As the name describes that the Public Key is given to everyone and the Private key is kept private [4]), a message encryption cryptosystem, two prime numbers are first calculated, and the product of these values yields a public and a private key that can be used for both encryption and decryption. Advanced LSB and the RSA method could be combined to incorporate the original text—in the form of encrypted text—into the cover image.

There are some advantages of RSA Algorithm:

1. Public key cryptography's main benefit is its greater security and persuasiveness.
2. It also offers digital signatures that are unrepudiable.
3. Public key authentication prevents the type of rejection and each user has its own responsibility for protecting his private key.
4. To increase the security of our keys, we can choose big prime integers.

4. Related work

Through fewer efforts at assault, the suggested solution in the paper [5] seeks to improve the security of sensitive data. Using a genetic approach, random hiding sites are generated, and the Huffman method is used to compress the data. Important information is taken out of the final rows by the recipient side and converted back into the original text. Genetic and Huffman algorithms reduce data size and enhance cover capacity, hence improving system efficiency and robustness. PSNR, a range of text sizes, and cover photos were used to gauge the system's efficacy.

Steganography is a technique used to secure data in communication, particularly in image steganography, which uses least significant bit (LSB) techniques. This paper [6] proposes a steganography-based RGB image using genetic algorithm (GA) to generate random keys for secret blocks. Experimental results show the proposed system is more efficient than other steganography techniques in terms of fidelity criteria and degradation quality.

5. The suggested technique

The aims of the suggested technique is to increase the speed of the algorithm performance, enhance the quality of the stego-image, and strengthen security level by using RSA algorithm and GA.

5.1. Embedding Algorithm

The embedding algorithm of the secret text in the cover-image is shown below. The flowchart of embedding algorithm is shown in Fig. 2, as well.

1. Read the cover-image and the secret text.
2. Dividing the cover-image into segments, each segment with size (3×3).
3. Encrypt the secret text by using the RSA algorithm to produce the encrypted text.
4. Specifying the scanning mode and the starting point for embedding the secret text through GA (the best permutation).
5. Inserting the encrypted text in the least significant bit of the cover-image.
6. Inserting the scanning mode and the starting point in the least significant bit of the cover-image.
7. Output the stego-image.

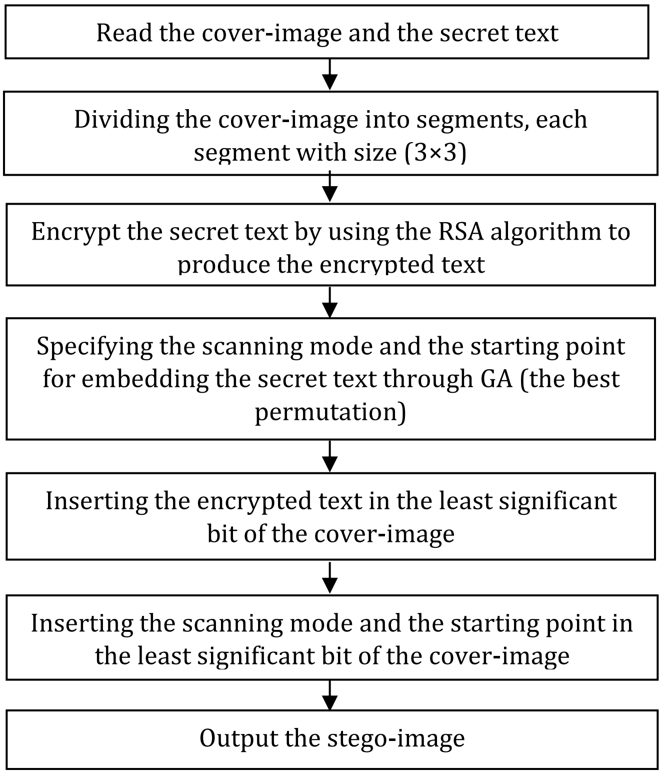

Read the cover-image and the secret text
Dividing the cover-image into segments, each segment with size (3×3)
Encrypt the secret text by using the RSA algorithm to produce the encrypted text
Specifying the scanning mode and the starting point for embedding the secret text through GA (the best permutation)
Inserting the encrypted text in the least significant bit of the cover-image
Inserting the scanning mode and the starting point in the least significant bit of the cover-image
Output the stego-image

Fig. 2- Flowchart of embedding algorithm

5.2. Extracting Algorithm

The extracting algorithm of the secret text from the stego-image is shown below. The flowchart of extracting algorithm is shown in Fig. 3, as well.

1. Read the stego-image.
2. Dividing the stego-image into segments, each segment with size (3×3).
3. Extracting the scanning mode and the starting point from the least significant bit of the stego-image.
4. Extracting the encrypted text from the least significant bit of the stego-image.
5. decrypt the encrypted text by using the reverse RSA algorithm to retrieval the secret text.

6. Output the secret text.

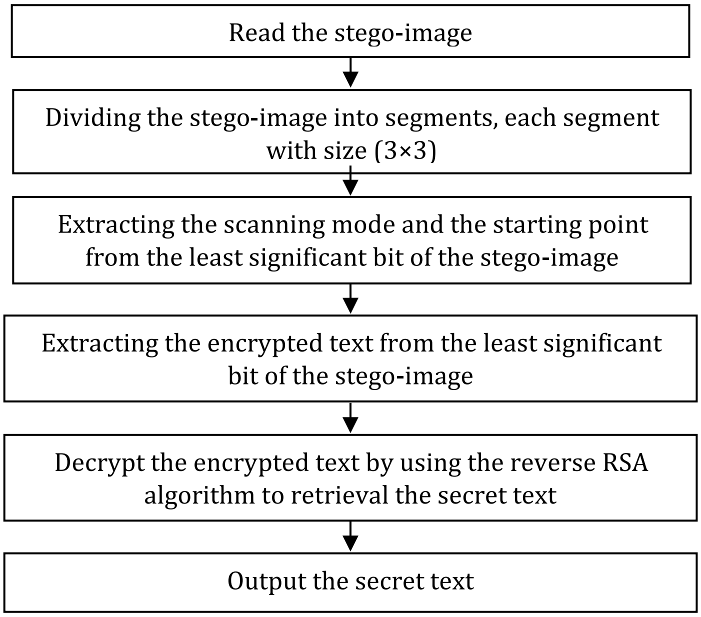

Read the stego-image
Dividing the stego-image into segments, each segment with size (3×3)
Extracting the scanning mode and the starting point from the least significant bit of the stego-image
Extracting the encrypted text from the least significant bit of the stego-image
Decrypt the encrypted text by using the reverse RSA algorithm to retrieval the secret text
Output the secret text

Fig. 3- Flowchart of extracting algorithm

6. Evaluation Of Image Quality

Measures of image quality, such as Mean-Squared Error and Peak Signal-to-Noise Ratio, are frequently used when comparing stego-image findings with cover results [7].

A. Mean-Squared Error

The mean-squared error (MSE) between two images $I_1(m,n)$ and $I_2(m,n)$ is:

$$MSE = \frac{\sum_{M,N}[I_1(m,n) - I_2(m,n)]^2}{M * N} \qquad (1)$$

The input images' rows and columns are denoted by M and N, respectively. Mean-squared error is highly dependent on the scaling of image intensity. An 8-bit image with pixel values in the range of 0-255 appears to have a mean-squared error of 100.0; whereas, a 10-bit image with pixel values in the range of 0,1023 barely shows an MSE of 100.0.

B. Peak Signal-to-Noise Ratio

This issue is avoided by Peak Signal-to-Noise Ratio (PSNR), which scales the MSE based on the image range.

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

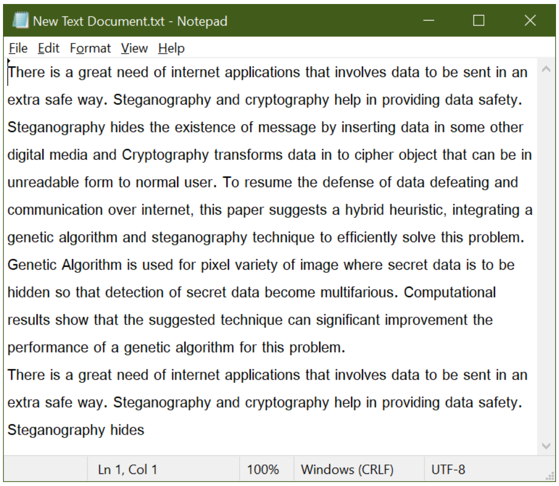
Decibels (dB) are used to measure PSNR. While PSNR is a useful metric for evaluating restoration outcomes within the same image, it has no significance when compared between images.

7. Experimental Results

The suggested technique is performed on the 24-bit true color images and JPG formats (Lina and Pepper) with size of (512×512), as shown in the table (1). The secret text to be embedded in these images is shown in Fig. (4) as well. The execution is done with Windows 10 operating system in Matlab (R2022b) Software.

Table 1- Results of the suggested technique.

Size of the secret text	Cover image (512 × 512)	Stego image (512 × 512)
1024 bytes		
1024 bytes		



There is a great need of internet applications that involves data to be sent in an extra safe way. Steganography and cryptography help in providing data safety. Steganography hides the existence of message by inserting data in some other digital media and Cryptography transforms data in to cipher object that can be in unreadable form to normal user. To resume the defense of data defeating and communication over internet, this paper suggests a hybrid heuristic, integrating a genetic algorithm and steganography technique to efficiently solve this problem. Genetic Algorithm is used for pixel variety of image where secret data is to be hidden so that detection of secret data become multifarious. Computational results show that the suggested technique can significant improvement the performance of a genetic algorithm for this problem.

There is a great need of internet applications that involves data to be sent in an extra safe way. Steganography and cryptography help in providing data safety. Steganography hides

Fig. 4- Secret text.

The quality of the stego-image is firstly tested by using PSNR. The MSE between the cover-image and the stego-image should be obtained as shown in equation (1). It is needed to get the PSNR as shown in equation (2).

As it is shown in table (2), the suggested technique enhances appearance quality of stego-image. So, the message with the same size improves the image quality and can be consummated in the same quality. The suggested technique has more capacity for embedding message.

Table 2- PSNR values of our results

Cover-Image name	Cover-Image size and type	Secret text size in byte	MSE	PSNR (dB)
Lina	512×512 JPG	1024	0.089	89.91
pepper	512×512 JPG	1024	0.079	88.63

A thorough comparison of related work and the suggested technique is provided in Table 3, and it is evident from the data that the suggested approach has outperformed the others.

Table 3- Comparison between related work & the suggested technique.

Approaches	Image size & type	Text size	PSNR
[5]	512 × 512 JPG	1032	83.073
[6]	348 × 348 JPG	1024	64.32
Proposed	512 × 512 JPG	1024	88.63

8. Conclusion

This research submits a technique for steganography in the color images. There are two levels of protection, one is the cryptography and the other is steganography. The genetic algorithm is used to detect the best spot for embedding data. In addition, the evolutionary algorithm can be used to minimize the difference between the cover-image and stego-image in order to obtain a decent PSNR. Then, the parallel genetic algorithm by calculating fitness is used to minimize the rather long executing time of this technique. Furthermore, the suggested technique is a blind algorithm which improves the security.

References

[1] M. Kanela, H. Dhingra, M. Singhal, G. Dhand, "Secure and Manage Passwords with Encryption and Cloud Storage", (April 24, 2021). Proceedings of the International Conference on Innovative Computing & Communication (ICICC) 2021, http://dx.doi.org/10.2139/ssrn.3833469.

[2] S. M. Abdulmaged, N. M. Abdulmaged, "A new steganography technique based on genetic algorithm", Global Journal of Engineering and Technology Advances, Vol. 16, Issue 2, pp. 135–139, 2023. DOI: https://doi.org/10.30574/gjeta.2023.16.2.0146.

[3] R. Wazirali, W. Alasmary, M. M. E. A. Mahmoud and A. Alhindi, "An Optimized Steganography Hiding Capacity and Imperceptibly Using Genetic Algorithms," in IEEE Access, vol. 7, pp. 133496-133508, 2019. DOI: 10.1109/ACCESS.2019.2941440.

[4] "RSA Algorithm in Cryptography", Last Updated: 09 Nov, 2023, visited on 8-6-2024, https://www.geeksforgeeks.org/rsa-algorithm-cryptography/.

[5] A.A. Hussein, R.M. Al Baity, S.A. Hadi, "Randomized information hiding in RGB images using genetic algorithm and Huffman coding", Revue d'Intelligence Artificielle, Vol. 37, 6, pp. 1435-1440, 2023. https://doi.org/10.18280/ria.370607

[6] R. D. AL-Dabbagh, N. A. Z. Abdullah, R. J. Essa, "Steganography Technique using Genetic Algorithm", Iraqi Journal of Science, Vol. 59, 3A, pp. 1312-1325, 2018. https://ijs.uobaghdad.edu.iq/index.php/eijs/article/view/284.

[7] S. A. Mahdi and M. A. Khodher "An improved method for combine (LSB and MSB) Based on color image RGB", Engineering and Technology Journal, Vol. 39, Part B, No. 01, pp. 231-242, 2021. DOI: https://doi.org/10.30684/etj.v39i1B.1574.