JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 1228 - 1235
https://publishoa.com
ISSN: 1309-345

Usage LSB Method in Hiding Text Information within Text in an Image

[1]Sahar Najah Hussein, [2]Khansaa Azeez Obayes Al-Husseini, [3]Ali Hamzah Obaid

asssdali44@gmail.com
inb.khanssa@atu.edu.iq, khansaaazeez@gmail.com, inb.ali210@atu.edu.iq, alimk.iq@gmail.com
[1,2,3]Al-Furat Al-Awsat Technical University, Babylon Technical Institute, 51015 Babylon, Iraq

ABSTRACT

At present, hiding messages and information sent via the Internet and social networking sites has become an urgent need with the development of hackers' methods in revealing hidden information. This paper presents a new hybrid approach to hiding information, including text steganography and image steganography techniques. First, this approach hides information that represents a text message in text using the inter-word spacing technique. Then, hiding the stego text in the image using the LSB method. The proposed method used a new approach to increasing the capacity of the stego text to be able to carry more letters of the message. Also, using that approach to reduce the pixels that are used to hide the stego text in the cover image. The results of the system are illustrated using the PSNR metric to measure the rate of error between the original image and the cover image.

Keywords: Information, PSNR, Message, Hidden, Cover, LSB.

Introduction

Historically, there have been many cases of data theft and digital information or unauthorized access to digital content to use it illegally, and with the development of information technology and modern means to reveal the confidentiality of data, it has become necessary to protect information and digital content from potential threats. Where the science of digital steganography refers to hiding or embedding information within the information to protect data from theft. Steganography is a centuries-old art form. It is used in open systems to provide security. Its primary objective is to disguise sensitive information within a cover. One of the important things that affect the characteristics of an element is the amount of evidence that can be contained within the cover media. There are numerous complicated methods for concealing, assessing, and recovering sensitive information [1].

Steganography techniques are an important part of the future of Internet security and privacy on open systems such as the internet. Messages have been embedded in a variety of methods using video, music, images. Despite the availability of numerous steganography techniques, they are vulnerable to visual, structural, and statistical attacks [2].

Capacity, security, and robustness are three elements of information hiding systems that compete with one another. When secret communication is kept private and untraceable by eavesdroppers, security is essential, whereas capacity refers to the amount of information that can be hidden in the medium. Finally, resilience might be defined as the amount of change that the stego medium can withstand before an attacker can delete hidden data [3].

One of the simplest ways to embed information in a multimedia file is to use the least significant bit (LSB) coding. The two ways of LSB steganography are LSB replacement and LSB matching. The first is the LSB replacement, which is the most basic of the LSB. The end parts of a cover image are replaced with each bit of the message that has to be hidden using LSB replacement steganography. The second method is LSB matching, which involves taking each pixel of the cover image in a pseudo-random order created by a secret key, If the cover pixels match with the confidential data part, no modifications are made to the confidential information, and on the contrary, one of the pixels values is subtracted from the random wrapper [4].

There are two basic ways for calculating image quality: The first is visual quality, which entails displaying images in the form of original, noisy, and treated images and allowing the user to compare them. The statistical method, which employs conventional quality indicators such as peak signal-to-noise ratio (PSNR), mean absolute error (MAE), mean square error (MSE), and structural similarity (SSIM), is the second way [5].

This study aims to introduce a new approach to hiding secret information that adopted two steganography techniques. This is done using two main steps: first hiding the secret text in the cover text, second hiding the stego text in the cover image to produce a more secret method to hide the information. This paper also aims to increase the number of letters of secret messages that hide in cover text and reduce the pixels used to hide the stego text with a high quality of the resulting stego image.

The rest of the paper is as follows: Steganography is explained in Section 1. Section 2 discusses the related work. Section 3 describes the proposed work. The results are shown in Section 4. Section 5 also concludes the paper.

Related work

The related work to paper who work in this field: The proposed the multiple approaches to steganography in an image It has been demonstrated that the space pixel has a greater capacity than the frequency domain [6]. The proposed system's purpose is to increase the complexity of cryptosystems while keeping the execution time similar to the original methods. It then hides the encrypted messages inside images in such a way that no attacker can determine that there is a secret message. As a result, the system under consideration is more efficient[7]. It is proposed to split the secret information by randomly distributing the bits for each row in the image, which generates a series of random steps, and then the information in the rows is masked in the reverse approach. This means that LSB technology makes pixel masking more difficult. The reported findings demonstrate the method's strength and security, as well as providing stronger protection for hidden information. In addition, the results show the quality of the stego picture in comparison to the original image using PSNR and SSIM quality measurements [8]. The proposed technique consists of three major components. That is due to a discovered supplementing of the secret text. The complemented text is then hidden in cover picture pixels using a pseudo-random number generator, and the bits of complemented text are eventually hidden in each pixel using the inverted bit LSB approach [9]. The proposed a new technique for hiding a text message with a grey image to ensure security while maintaining high-quality results the integers and key matrix were then subjected to an XOR operation. The last two bits of the grey level value were then ANDed with the first two bits of the matrix to produce randomized plain text, which was then embedded within the original image. The use of XOR and AND operations assures that the resulting image has the fewest defects possible, which boosts the image's quality [10]. There are many methods of steganography in data steganography systems, including the least important bits, Pseudorandom Permutation, and overlays. Parity bits, Cover-Regions usually, it is used to embed pieces of confidential information. [11,12].

Proposed Work

In this paper, we hide confidential information using the shortened bits for each character in the secret message. Then we use the spacing method to hide the secret text in the cover text. Next, apply the LSB method to hide Stego text in the cover photo. MATLAB 7.12.0 is the environment used with the appropriate Graphical User Interface (GUI). Using the GUI provides an active way to hide any secret message they want in the specified cover body from the path file. This method includes the following steps:

Step 1: Hiding Text in Text Using Spacing Method

The input of this step is the secret message and the cover text, and the output of this step is the stego text. In this step, we reduce the characters bits from 8 characters to just 5 bits. The useful number of bits in each secret character is fewer than six (with only five bits, we may represent (32) characters, of which (26) are English alphabetic characters and the remaining are significant characters such as (space, comma, bracket...etc). We arrange secret characters in the range (0.. 31) to increase the size of the embedding and complexity (to reduce the number of bits to represent its). Then, using the spacing method, hide it in the cover text.

Step 2: Hiding Stego Text in the cover image using the LSB method

Starting from the beginning of the image, for each pixel in the image convert the last bit in the pixel with one bit of the stego text. For example, if the value of the pixel is 00110101, and the current stego bit is 0 then the pixel's value will be 00110100 and stored in the stego image that is displayed**.**

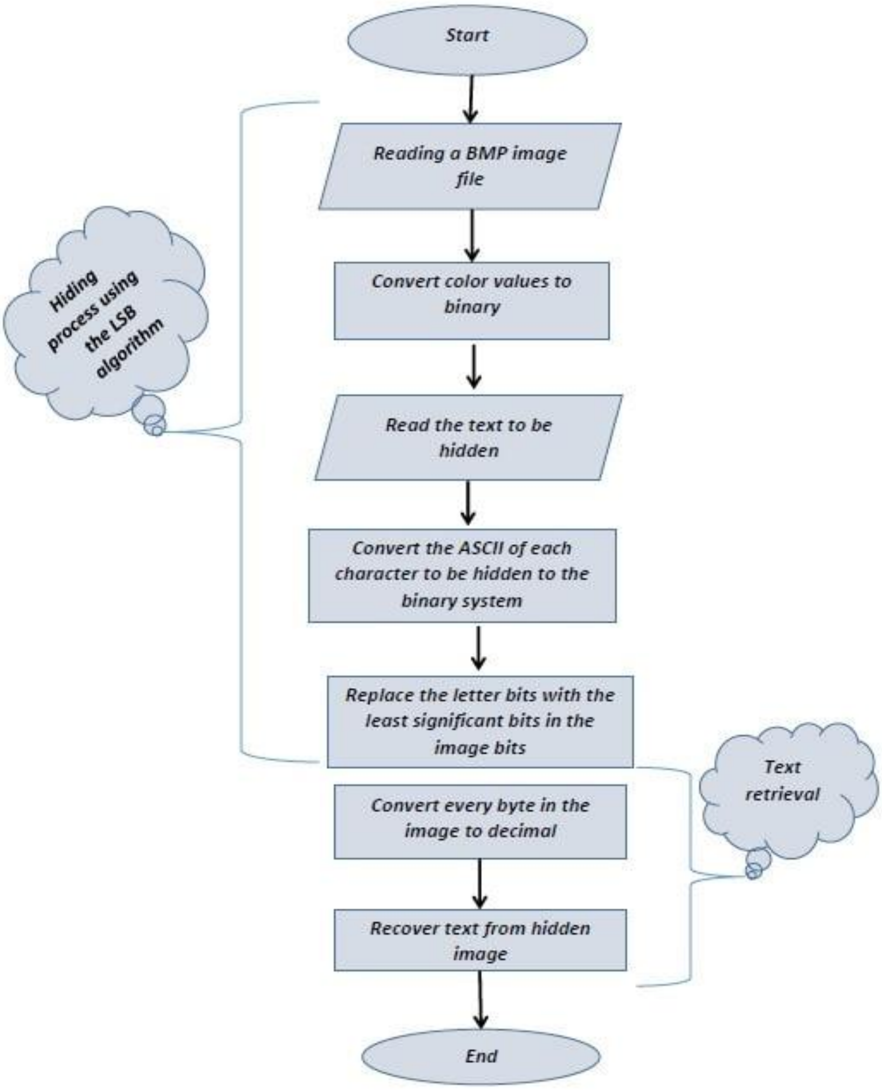
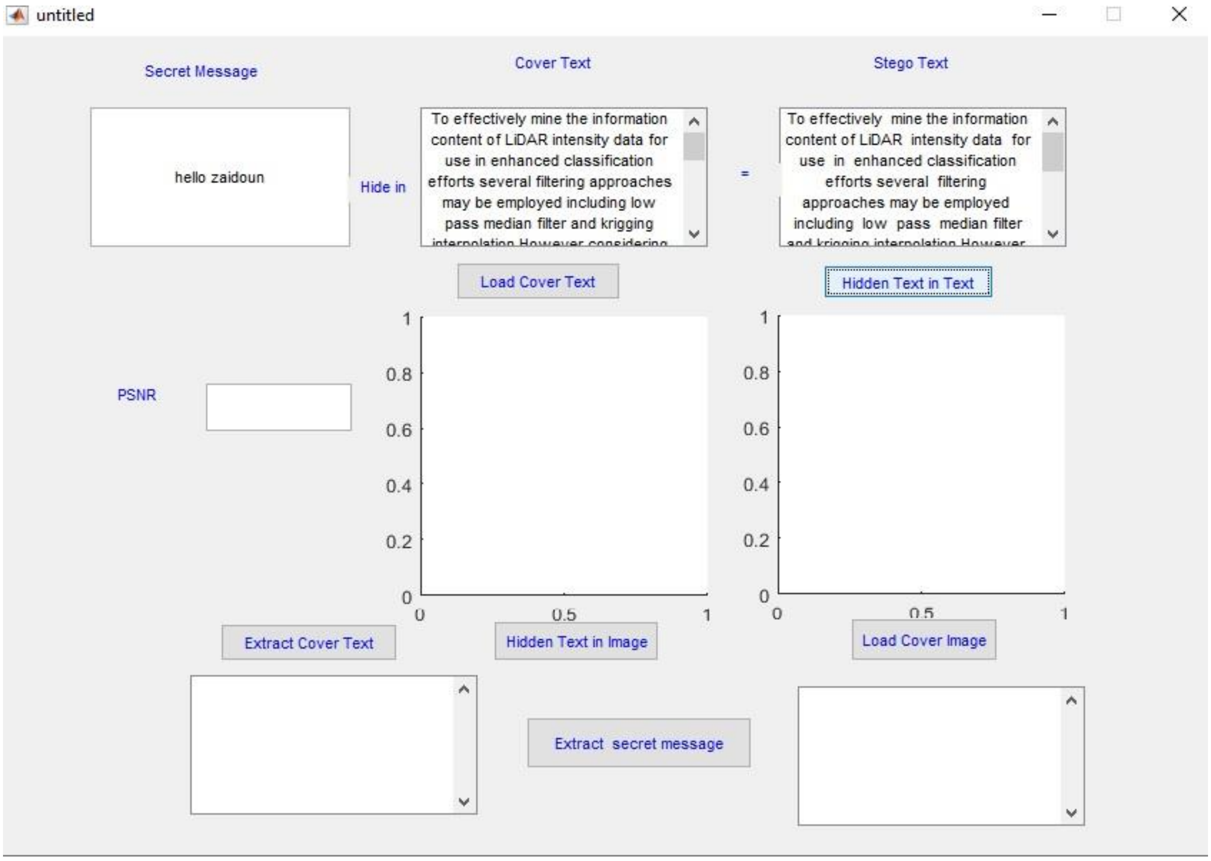

Start
Reading a BMP image file
Convert color values to binary
Read the text to be hidden
Convert the ASCII of each character to be hidden to the binary system
Replace the letter bits with the least significant bits in the image bits
Convert every byte in the image to decimal
Recover text from hidden image
End
Hiding process using the LSB algorithm
Text retrieval

Figure 1: Flowchart of the proposed hiding system

Result

The resulting GUI that obtained when applying the hiding information system. Figure 3 depicted the generated stego text after implementing the system's initial phase of hiding the secret message in the cover text file. Figure 4 explains the resulting image from stage 4 in fig 5 of the system that includes hiding the stego text in the cover image, with the PSNR between it and the original image. Figure 5 explains step 4 of the system that including the extraction process for the stego text and then for the secret message.

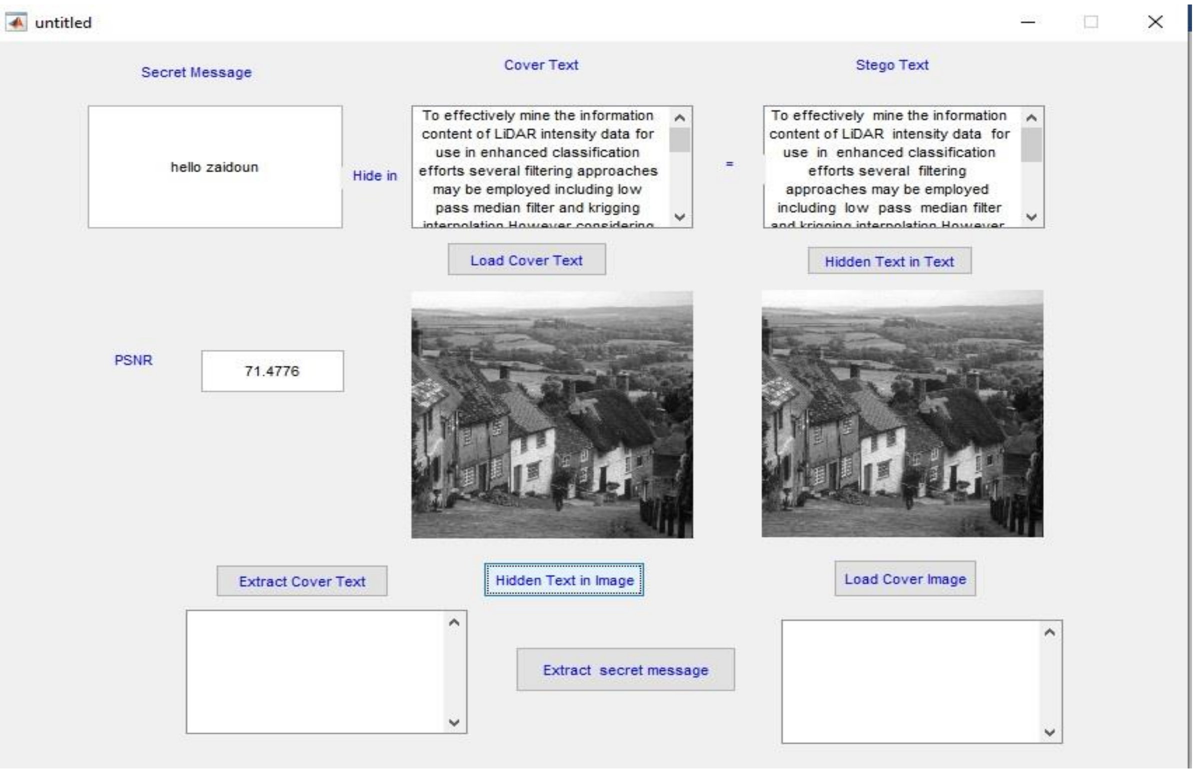


hello zaidoun

To effectively mine the information content of LiDAR intensity data for use in enhanced classification efforts several filtering approaches may be employed including low pass median filter and krigging interpolation However considering

To effectively mine the information content of LiDAR intensity data for use in enhanced classification efforts several filtering approaches may be employed including low pass median filter and krigging interpolation However

Figure 2: Results of the hiding information system



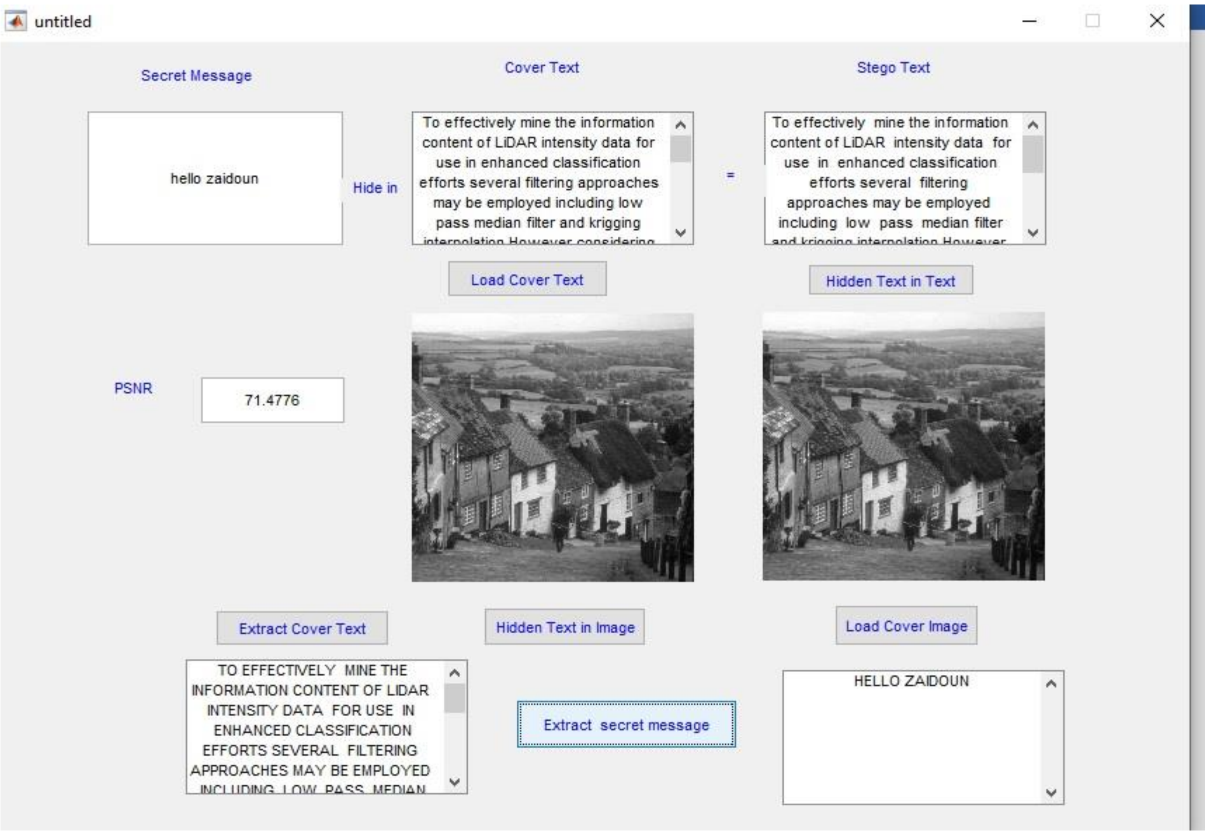
hello zaidoun

To effectively mine the information content of LiDAR intensity data for use in enhanced classification efforts several filtering approaches may be employed including low pass median filter and krigging interpolation However considering

To effectively mine the information content of LiDAR intensity data for use in enhanced classification efforts several filtering approaches may be employed including low pass median filter and krigging interpolation However

71.4776

Figure 3: Results of the hiding information system



hello zaidoun

To effectively mine the information content of LiDAR intensity data for use in enhanced classification efforts several filtering approaches may be employed including low pass median filter and krigging interpolation However considering

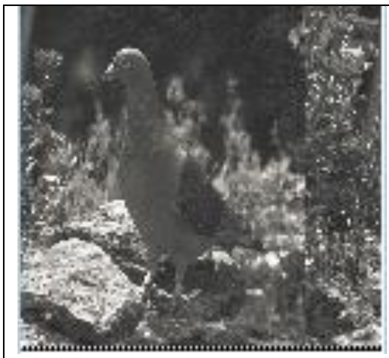
To effectively mine the information content of LiDAR intensity data for use in enhanced classification efforts several filtering approaches may be employed including low pass median filter and krigging interpolation However

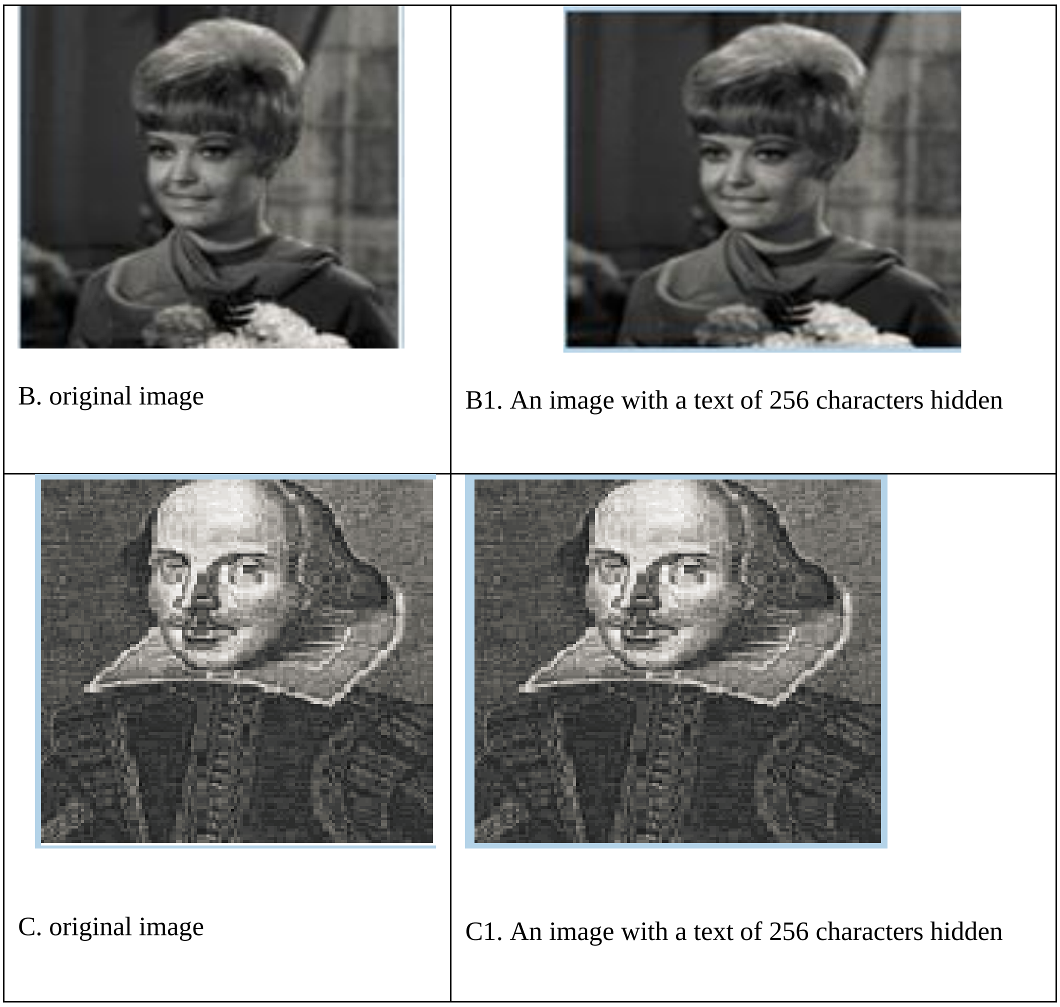
71.4776

TO EFFECTIVELY MINE THE INFORMATION CONTENT OF LIDAR INTENSITY DATA FOR USE IN ENHANCED CLASSIFICATION EFFORTS SEVERAL FILTERING APPROACHES MAY BE EMPLOYED INCLUDING LOW PASS MEDIAN

HELLO ZAIDOUN

Figure 4: Results of the hiding information system

 A. original image	 A1. An image with a text of 256 characters hidden



B. original image

B1. An image with a text of 256 characters hidden

C. original image

C1. An image with a text of 256 characters hidden

Figure 5: Models of the images which the hidden system

Computing of PSNR

After applying the hiding approach, there is, need to find the accuracy of this method by computing the quality measurement that is PSNR between the original image and the cover image. Table 1. Illustrated the results of PSNR when applying different cover images.

Table 1. PSNR for different image

Name image	**PSNR**
Cat	**70.0466**
Artist	**70.1975**
Bird	**70.1805**
Woman	**71.9627**
Lena	**74.1297**
Man	**74.9305**

Conclusion

The results proved the efficiency of the algorithm by retrieval the secret message without error and the stego image does not have distortion. This system increases the capacity of the cover text by reducing the character's bits of the secret message from 8 to 5 bits. This system can be considered as a new method to hide information using a hybrid method between text and image steganography. In future works will be suggested to develop the current system using another method of hiding text in the text to get more efficiency that represents by increasing the capacity of the cover text and being more secret. Developing the LSB algorithm to be more secret. Using another type of quality metrics to compute the quality of a resulting image.

References

1. Christine K., "Genetic Algorithm Based Model in Text Steganography", The African Journal of Information Systems, 2013.
2. Hebah H. and Murad S., "PROPOSED DATA HIDING TECHNIQUE TEXT IMAGE INSIDE IMAGE (TIII)", IJRRAS 4 (2), 2010.
3. M.Grace V. and et al., "Hiding the Text Information using steganography", International Journal of Engineering Research and Applications (IJERA), 2012.
4. Deepesh R. and Vijaya B., "Steganography Technique for Hiding Text Information in Color Image using Improved LSB Method", International Journal of Computer Applications (0975 – 8887) Volume 67– No.1, April 2013.
5. V.R.Vijaykumar et al., "Robust Statistics Based Algorithm to Remove Salt and Pepper Noise in Images", International Journal of Information and Communication Engineering, 2009.
6. Tavoli, R., et al. (2016). "A new method for text hiding in the image by using LSB." International Journal of Advanced Computer Science and Applications 7(4): 126-132.
7. Ahmed, J. M. and Z. M. Ali (2011). "Information Hiding using LSB technique." International journal of computer science and network security 11(4): 18-25.
8. Abbood, E. A., et al. (2018). "Text in Image Hiding using Developed LSB and Random Method." International Journal of Electrical & Computer Engineering (2088-8708) 8(4).
9. Rupali Bhardwaj and Vaishali Sharma," Image Steganography Based on Complemented Message and Inverted bit LSB Substitution", 6th International Conference on Advances In Computing & Communications, 2016.
10. ElyaTawfiq, N. (2013). Hiding Text within Image Using LSB Replacement. IOSR Journal of Computer Engineering (IOSR-JCE): 13-16.
11. Obaid, A.H. 2015. Information hiding techniques for steganography and digital watermarking. UDC 681.518 (04) INTERACTIVE SYSTEMS: Problems of human-computer interaction. Collection of scientific papers, 306 p, 63. Ulyanovsk: USTU.
12. Khansaa Azeez Obayes, Information security in the field of technical development and information. UDC 681.518 (04) INTERACTIVE SYSTEMS: Problems of Human-Computer Interaction.–Collection of scientific papers.-Ulyanovsk: USTU, 2015.- 306 p. 2015, pp. 71.
13. Al-Husseini, K.A.O., & Obaid, A.H. (2020). Interaction between project tasks and risk management tasks in software development. Periodicals of Engineering and Natural Sciences (PEN), 8(4), 2300-2308.
14. Al-Husseini, K.A., & Obaid, A.H. (2019). Analysis and risk management in software development using the logical-algebraic model. In CEUR Workshop Proceedings, 2475, 241–248.
15. KEKRE, H. B., et al. Information hiding in audio signals. International Journal of Computer Applications, 2010, 7.9: 14-19.
16. RAJKAMAL, M.; ZORAIDA, B. S. E. Image and Text Hiding using RSA & Blowfish Algorithms with Hash-Lsb Technique. Int. J. Innov. Sci. Eng. Technol, 2014, 1.6.
17. SETHI, Pratiksha; KAPOOR, V. A proposed novel architecture for information hiding in image steganography by using genetic algorithm and cryptography. Procedia Computer Science, 2016, 87: 61-66.
18. BHOLE, Ashish T.; PATEL, Rachna. Steganography over video file using Random Byte Hiding and LSB technique. In: 2012 IEEE International Conference on Computational Intelligence and Computing Research. IEEE, 2012. p. 1-6.
19. MUHAMMAD, Khan, et al. A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image. Multimedia Tools and Applications, 2016, 75.22: 14867-14893.
20. SHEKHAWAT, Vaibhav Singh; TIWARI, Manish; PATEL, Mayank. A secured steganography algorithm for hiding an image and data in an image using LSB technique. In: Computational Methods and Data Engineering. Springer, Singapore, 2021. p. 455-468.

21. HALDER, Rituparna, et al. A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique. IOSR Journal of Computer Engineering (IOSR-JCE), 2016, 18.1: 39-43.

22. MARVEL, Lisa M.; BONCELET, Charles G.; RETTER, Charles T. Spread spectrum image steganography. IEEE Transactions on image processing, 1999, 8.8: 1075-1083.

23. HUREIB, E. S.; GUTUB, Adnan A. Enhancing medical data security via combining elliptic curve cryptography and image steganography. Int. J. Comput. Sci. Netw. Secur.(IJCSNS), 2020, 20.8: 1-8.

24. MAHDI, Mohammed Hashim, et al. Improvement of Image Steganography Scheme Based on LSB Value with Two Control Random Parameters and Multi-level Encryption. In: IOP Conference Series: Materials Science and Engineering. IOP Publishing, 2019. p. 052002.