تم استلام الورقة بتاريخ:23/ 6 /2024م وتم نشرها على الموقع بتاريخ: 20/ 7/2024م

Use the secret key instead of LSB as a Pointer with MSB to hide the data for greater security than the LSB-MSB combination method

www.doi.org/10.62341/samu2367

Salem Sulaiman Husain[1], Ahmad Abd Alrhman Abosleala[1]
Mohamed Faraj Igbaisha[2]

1 - Higher Institute for Science and Technology Misurata – Libya
2 - Higher Institute for Science and Technology Alkhoms – Libya

salemsulaiman9999@gmail.com

Abstract

Steganography in images has become an important technique for protecting sensitive information by concealing data within images. While current techniques offer some levels of security, there is always a risk of detection or extraction by unauthorized parties. In this paper, we propose a novel approach to significantly enhance the security of image steganography by using a secret key as a pointer to guide the data hiding process. Our proposal introduces a unique blend of two established techniques: combine the Least Significant Bit (LSB) and Bit of secret key we designate the least significant bit of the image pixel according to the secret key bit, thus embedding the data. This modification adds an additional layer of complexity, making it difficult for attackers to detect any hidden data. We provide a detailed algorithm outlining the process of embedding and extracting data, emphasizing the role of the secret key. The key itself is encrypted using a secure algorithm, ensuring that even if hidden data is discovered, decrypting it remains exceedingly challenging. Experimental results. The result was excellent as the proposed method increased security without affecting image quality.

KEYWORDS: image, Data, LSB, Data hiding, steganography, Des secret key, MSE.

تم استلام الورقة بتاريخ:23/ 6 /2024م وتم نشرها على الموقع بتاريخ: 20/ 7/2024م

استخدام المفتاح السري بديلا عن LSB كمؤشر مع MSB لإخفاء البيانات لزيادة أمان بشكل أكبر من طريقة مزيج LSB – MSB

سالم سليمان حسين[1]، أحمد عبد الرحمن أبوسليلة[1]، محمد فرج غبيشة[2]

1 – المعهد العالي للعلوم والتقنية مصراته

2– المعهد العالي للعلوم والتقنية الخمس

salemsulaiman9999@gmail.com

الملخص:

لقد ظهر إخفاء المعلومات في الصور كطريقة مهمة لحماية المعلومات الحساسة من خلال إخفاء البيانات داخل الصور، وعلى الرغم من وجود بعض التدابير الأمنية في المنهجيات الحالية، فإن إمكانية قيام أطراف غير مصرح لها باكتشاف أو استخراج المعلومات المخفية تظل مصدر قلق، تقدم هذه الدراسة استراتيجية جديدة تهدف إلى تعزيز أمن إخفاء الصورة بشكل كبير من خلال استخدام مفتاح سري لتوجيه عملية إخفاء البيانات، وذلك من خلال دمج تقنية الجمع بين البت الأقل أهمية (LSB) والبت الاعلى اهمية MSB مع بتة المفتاح السري، وبالتالي تحديد البتة الأقل أهمية من بكسل الصورة استنادًا إلى بت المفتاح السري لتضمين البيانات، ودلك باستبدال البت الاقل اهمية بدلا منه ببت من المفتاح السري يقدم هذا التعديل طبقة إضافية من التعقيد، مما يجعل من الصعب على المتسللين المحتملين التعرف على أي معلومات مخفية. يتم تقديم خوارزمية شاملة تحدد إجراءات تضمين البيانات واستخراجها، مما يؤكد أهمية المفتاح السري، وقد أظهرت نتائج ممتازة مع زيادة قوة الخوارزمية.

Introduction

People worldwide have shown interest in data hiding techniques due to the widespread proliferation of computer networks, leading to an increased focus on data protection. Digital copyright protection, information security[1], and confidentiality can be achieved through the use of digital hiding methods. Employing data hiding mechanisms presents a distinct and intriguing challenge for digital

تم استلام الورقة بتاريخ:23/ 6 /2024م وتم نشرها على الموقع بتاريخ: 20/ 7/2024م

forensics analysts. Information transfer heavily relies on data transmission in current times. The concept of "data hiding" has emerged to secure information and ensure its protection from unauthorized disclosure. Digital data transmission can be executed over computer networks with minimal errors and often without any interruptions [2]. The Internet provides a communication platform for disseminating information widely. Therefore, it is necessary to maintain the security and safety of data to prevent unauthorized access and misuse. Both concealment and encryption function as techniques to hide information by modifying messages to obscure their content from potential malicious interception. Concealment and encryption are among the various methods of hiding information. Concealment involves embedding messages within unexpected forms of multimedia and is often used for secret communication between parties already known to each other. Through this technique, irrelevant or unused components of the digital medium are replaced with confidential information. The concept revolves around hiding something by embedding it within another larger entity in a way that escapes detection by the unaided eye [3]. Any digital file format can be employed for steganography; however, formats with high redundancy levels are preferred. Redundant components of an object are those that can be altered without immediate detection by other parts of the object. Digital images serve as the most prevalent cover medium used in steganography procedures. Steganography capitalizes on the surplus redundant data often found in digital images to obfuscate the hidden message. Cryptography serves to obscure the content of data, rendering it unintelligible to anyone other than the intended recipient and creator. Steganography can be compared to encryption's enigmatic sibling. While encryption focuses on protecting the content within the message, steganography conceals the existence of the message itself. This distinction is crucial between the two. Therefore, if communication is encrypted, the secrecy of both parties may be apparent to the observer any digital file format can be employed for steganography; however, formats with high redundancy levels are preferred. Redundant components

تم استلام الورقة بتاريخ:23/ 6 /2024م وتم نشرها على الموقع بتاريخ: 20/ 7/2024م

of an object are those that can be altered without immediate detection by other parts of the object. Digital images serve as the most prevalent cover medium used in steganography procedures. Steganography capitalizes on the surplus redundant data often found in digital images to obfuscate the hidden message. Cryptography serves to obscure the content of data, rendering it unintelligible to anyone other than the intended recipient and creator. Steganography can be compared to encryption's enigmatic sibling. While encryption focuses on protecting the content within the message, steganography conceals the existence of the message itself. This distinction is crucial between the two. Therefore, if communication is encrypted, the secrecy of both parties may be apparent to the observer. Steganography works as a technique to hide the existence of a secret message in a way that prevents any external observer from discovering that secret communication is taking place. The principles of data embedding rely on three main principles: capacity, security, and robustness. The term "capacity" refers to the medium's ability to store data covertly without changing its complexity. Security, in the context of embedding algorithms, entails the impossibility of extracting embedded information without detecting it through deliberate attacks. Meanwhile, robustness refers to the cover image's ability to withstand manipulations without revealing any alterations. Steganography and encryption play a fundamental role in ensuring the achievement of these principles. Both work as techniques to conceal data and can be used together without compromising data integrity. Steganographic systems can effectively conceal encrypted data [4].Steganography works as a technique to hide the existence of a secret message in a way that prevents any external observer from discovering that secret communication is taking place. The principles of data embedding rely on three main principles: capacity, security, and robustness. The term "capacity" refers to the medium's ability to store data covertly without changing its complexity. Security, in the context of embedding algorithms, entails the impossibility of extracting embedded information without detecting it through deliberate attacks. Meanwhile, robustness refers to the cover image's ability to

تم استلام الورقة بتاريخ:23/ 6 /2024م وتم نشرها على الموقع بتاريخ: 20/ 7/2024م

withstand manipulations without revealing any alterations. Steganography and encryption play a fundamental role in ensuring the achievement of these principles. Both work as techniques to conceal data and can be used together without compromising data integrity. Steganographic systems can effectively conceal encrypted data [5].

Literature Review

Rajkumar (2023), proposed A NEW METHOD FOR IMAGE STEGANOGRAPHY USING THE COMBINATION OF LSB AND MSB. During this research, an original strategy for information hiding was proposed. The spatial domain concept was utilized by manipulating pixel values to conceal and retrieve information. In this study, the message was embedded using Least Significant Bits (LSB) of pixels and then extracted using Most Significant Bits (MSB). In this research, the key was chosen instead of the least significant bit, which increased security.

. Kh. Abuzanouneh and M. Hadwan (2021) proposed the utilization of the feature selection methodology combined with a pixel selection technique for concealing covert messages. To enhance the complexity of steganalysis, the confidential data is dispersed and irregularly embedded within the stego-image. The confidential file's binary sequence encompasses encoded elements, with MPPST developing a sophisticated key for pinpointing their locations within the binary sequence. A comparison is conducted between the Least Significant Bit (LSB) method, an established algorithm in the domain, and the novel MPPST approach to assess their respective efficacies.

Sally A. Mahdi a*, Maisa’a A. Khodher (2020) proposed An Improved Method for Combine (LSB and MSB) Based on Color Image RGB, This paper presents two techniques that combine the most significant bit (MSB) as well as the least significant bit (LSB) based on a color image (24bit for RGB). The presented study proposes a novel method to combine (LSB and MSB) bits based on check MSB values and replace bits from LSB with a secret message. The result of this proposed method that made not affect quality stego

تم استلام الورقة بتاريخ:23/ 6 /2024م وتم نشرها على الموقع بتاريخ: 20/ 7/2024م

-image based on the resulting histogram that shows a match between the cover image and stego- image and more secure because not hidden in all image. The factors were used Mean Square Error (MSE), Compute Payload, in addition to Peak Signal to Noise Ratio (PSNR). The PSNR's rate is high and MSE is less. The result of this paper when applying on the different image gives high PSNR of 87.141 and less MSE of 0.00012 when inserting message 80 bits and reduction value PSNR of 72.023 and MSE of 0.0040 when inserting message 1200 bits and measure entropy is the same value for cover image and stego –image then this method is more security for the attacker.

Steganography in Image

Steganography in image consists of two fields: - Spatial domain technique and Transform domain technique, where the spatial domain (image domain) works with the bits in the cover image and embeds the secret message in this image where it does not affect the image and the noise is processed. The transform domain (frequency domain) works to transform the image and manipulate the algorithm [1].

Image Domain (Spatial Domain Technique)

Spatial domain contains different techniques. These techniques replace some bits in the image pixel value without changing or affecting the image to hide information such as less significant bits It is one of the uncomplicated techniques but gives a good result and does not affect the image and the modifications of the less significant bits in the value will be invisible to the human eye. This technique involves resisting uniform affine transformations including rotation, scaling and shearing [6].

In general, in LSB methods, hidden information is stored into a specific position of LSB of image. For this reason, knowing the retrieval methods, anyone can extract the hidden information. [7].

The Proposed Method

In this paper, a method was applied in which the least significant bit is one of the encryption key bits as an indicator that determines the

تم استلام الورقة بتاريخ:23/ 6 /2024م وتم نشرها على الموقع بتاريخ: 20/ 7/2024م

value that was hidden in the specified color of the pixel, and the change is to the least significant bit of the color in case the change is needed, The following steps show implementing the method:

1- Read e the text, image, and key as shown in figures 1.
2- Generating 16 bits as a key using the Des method image as shown in figures 2.
3- Distribute the key bits on the image as shown in figures 3.
4- The hiding process as shown in figures 4.

1- The process of reading the text, image, and key

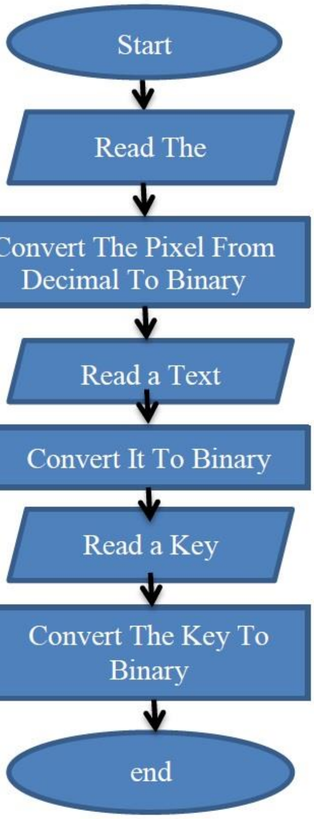

Start
Read The
Convert The Pixel From Decimal To Binary
Read a Text
Convert It To Binary
Read a Key
Convert The Key To Binary
end

Figure 1. The process of reading the text, image, and key

تم استلام الورقة بتاريخ:23/ 6 /2024م وتم نشرها على الموقع بتاريخ: 20/ 7/2024م

2 - Generating 16 bits as a key using the Des method

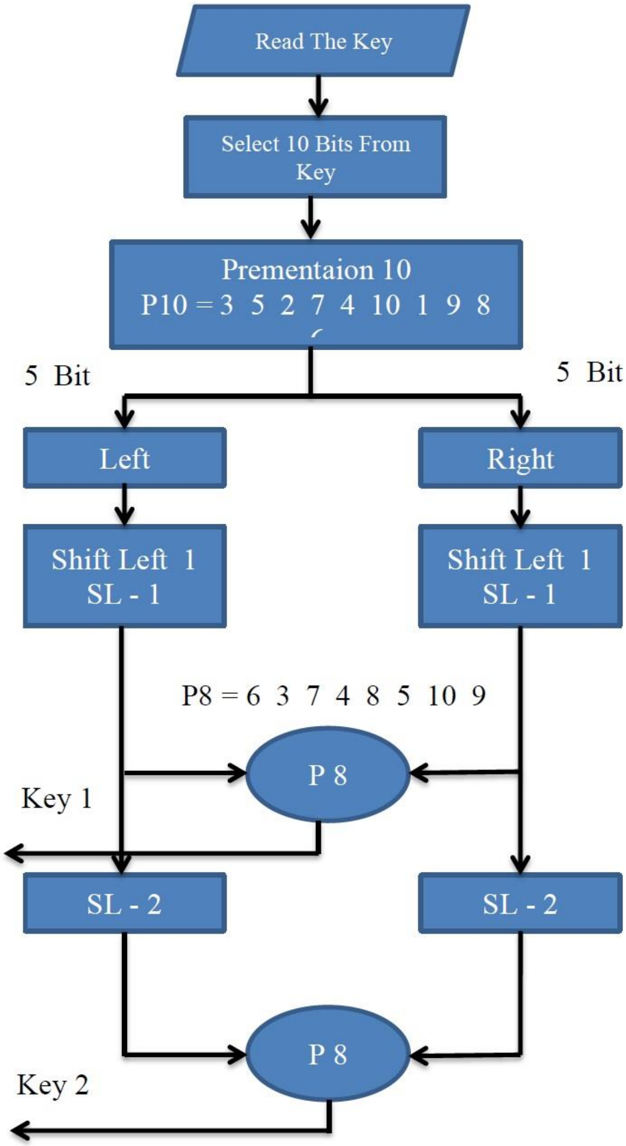


Figure 2. Generating 16 bits as a key

تم استلام الورقة بتاريخ:23/ 6 /2024م وتم نشرها على الموقع بتاريخ: 20/ 7/2024م

3- The process of distributing the key bits on the image

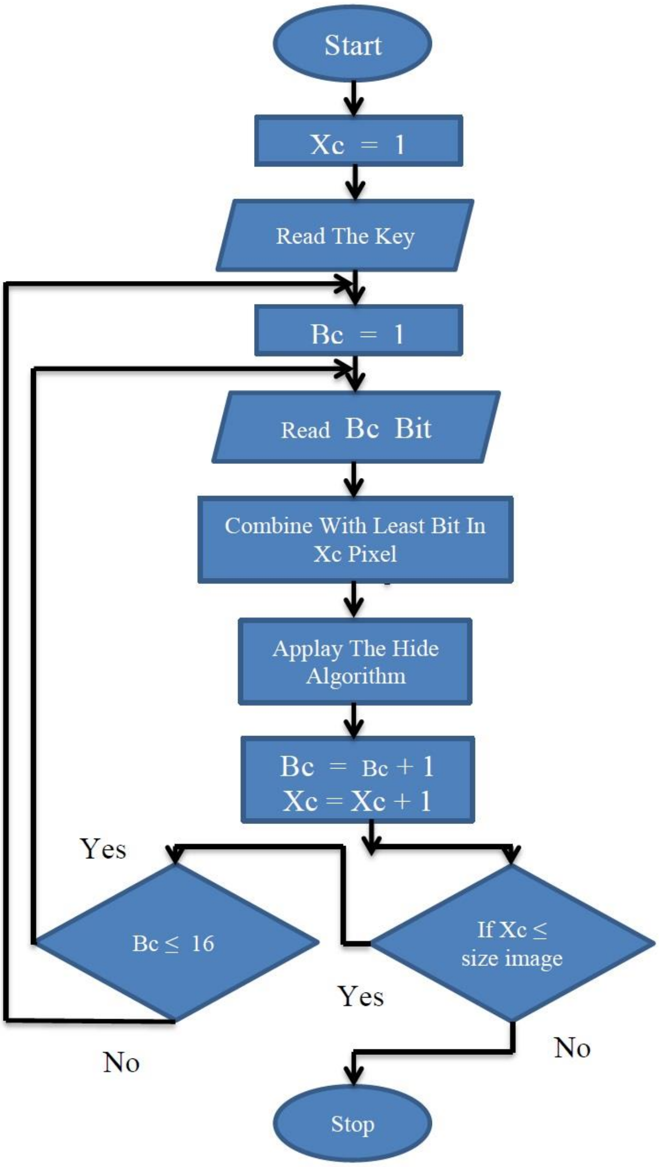


Figure 3. Distributing the key bits on the image

تم استلام الورقة بتاريخ:23/ 6 /2024م وتم نشرها على الموقع بتاريخ: 20/ 7/2024م

4- The hiding process

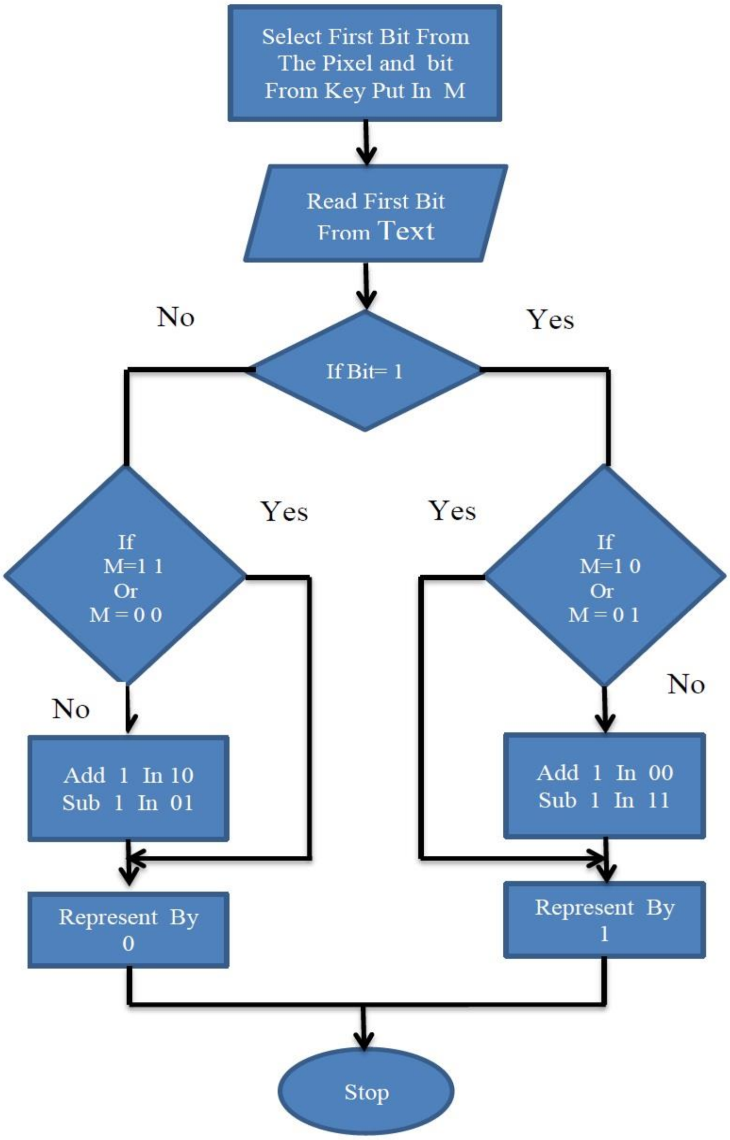


Figure 4. The hiding process

Effective Reduction Methods Factor

Measuring image quality requires comparing the results of the cover image and the stealth image and the commonly used metrics (maximum signal-to-noise ratio, mean square error, and payload).

Mean Square Error (MSE):- It is a measure between the cover image and the stealth image. C(x, y) and S(x, y) are calculated using the following equation:

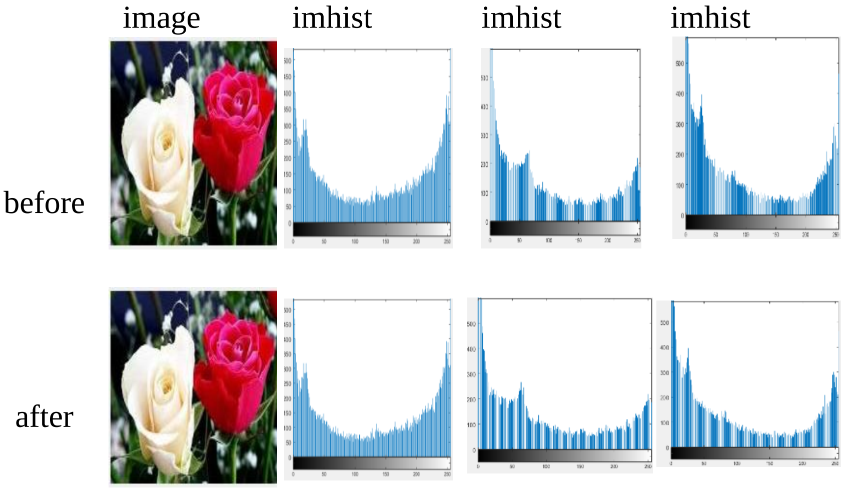
$MSE = \Sigma\ [C(x, y) - S(x, y)]2/x*y$

Where x is the number of rows and y is the number of columns within the cover image.

Evaluation and Result

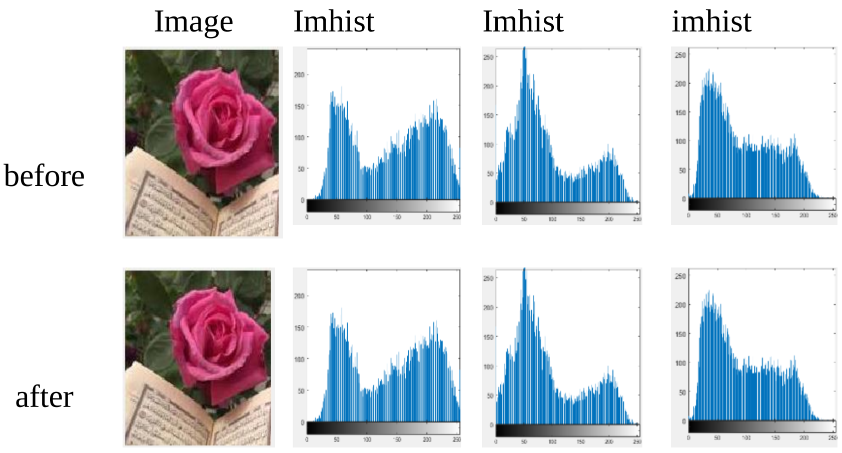
The proposed method has been used MSE factor to evaluate between the cover image and stego image and implement this method in language matlab2021b.

Fig.5.a, Fig.5.b and Fig.5.c show the cover images with its stego images. The MSE values have been shown between original cover images and stego images and their histogram also shown.



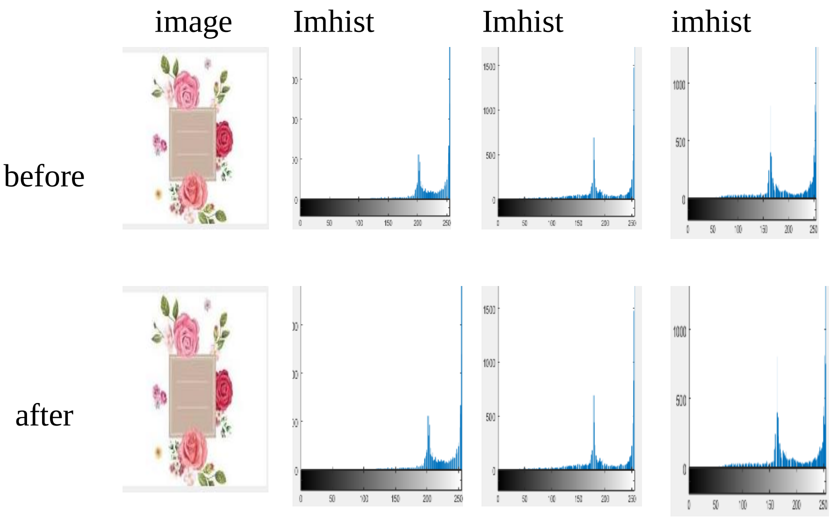
The MSE is 0.006652

Figure 5-a. Image & histogram before &after hiding



The MSE is 0.0116

Figure 5-b. Image & histogram before &after hiding



The MSE is 0.00195

Figure 5-c. Image & histogram before &after hiding

تم استلام الورقة بتاريخ:23/ 6 /2024م وتم نشرها على الموقع بتاريخ: 20/ 7/2024م

Discussion

In this paragraph, the results are discussed, as the data was hidden in a set of images using the proposed method, and the results were excellent, as the image in Figure 5-a was seen by the naked eye without change before and after hiding, as the HISTOGRAM for the three colors was unchanged, and the MSE = 0.006652. Likewise, the image in Figure 5b, we notice that there is no change in the original image and the image after hiding and the HISTOGRAM for the three colors was unchanged and the MSE = 0.0116, and in Figure 5-c, we notice that there is no change in the original image and the image after hiding and the HISTOGRAM for the three colors was unchanged and the MSE = 0.00195 . The results of Rajkumar (2023), "A NEW METHOD FOR IMAGE STEGANOGRAPHY USING THE COMBINATION OF LSB AND MSB", study for image 1 were mse= 0.0071 and also for image 2 mse= 0.0044 and thus the proposed method is considered to have excellent results with increased security using the secret key[1].

Conclusion and Future Work

In this paper, a new approach to image hiding is presented. This is done by using a secret key to represent the data and thus increasing the effectiveness. In addition, in case of knowing the algorithm, the data cannot be extracted without knowing the secret key. The MSE values were also calculated and the results show that this method is effective. We recommend a method to extract meanings from the password to determine the addresses. Thus, even in the case of discovering the password, the message cannot be extracted unless knowing what the meaning refers to

تم استلام الورقة بتاريخ:23/ 6 /2024م وتم نشرها على الموقع بتاريخ: 20/ 7/2024م

References

[1] Rajkumar, Rajkumar. (2023). A new method for image steganography using the combination of lsb and msb. International journal of computer science and mobile computing, doi: 10.47760/ijcsmc.2023.v12i02.002

[2] Sally, A., Mahdi. (2021). An Improved Method for Combine (LSB and MSB) Based on Color Image RGB. Engineering and Technology Journal, doi: 10.30684/ETJ.V39I1B.1574

[3] Anderson , R. J. and Petitcolas, F. A.P. (1998) "On The Limits of Steganography", IEEE Journal of Selected Areas in Communications, Vol.16 No.4, pp.474-481, ISSN 0733-8716.

[4] Y. P. Astuti, E. H. Rachmawanto, and C. A. Sari, "Simple and secure image steganography using LSB and triple XOR operation on MSB," in 2018 International Conference on Information and Communications Technology (ICOIACT), pp.191-195, 2018.

[5] S., M., Masud, Karim., Md., Saifur, Rahman., Md., Ismail, Hossain. (2011). A new approach for LSB based image steganography using secret key.
doi: 10.1109/ICCITECHN.2011.6164800

[6] Gowtham, Prasad, T, V, S., S, Varadarajan., S.A.K, Jilani., G, N, Kodandaramaiah. (2013). Image Steganography Based On Optimal LSB Pixel Adjustment Method. doi:10.24297/IJCT.V5I1.4380

[7] Kamaldeep, Joshi., Rajkumar, Yadav. (2015). A new LSB-S image steganography method blend with Cryptography for secret communication. doi: 10.1109/ICIIP.2015.7414745