DOI: 10.24996/ijs.2025.66.2.22

ISSN: 0067-2904

Enhanced Medical Image Steganography Using Improved LSB With Conditional MSB Based on Color Vector Variety

Yasmin Alaa Hassan*[1,2], Abdul Monem S. Rahma[3]

[1] *Department of Computer Science, College of Science, University of Baghdad, Baghdad, Iraq*
[2] *Department of Computer Science, University of Technology*
[3] *Department of Computer Science, Al-Maarif University College, Al Anbar, Iraq*

Received: 17/9/2023 Accepted: 27/2/2024 Published: 28/2/2025

Abstract

Image steganography involves concealing various forms of information, such as text, images, or videos, within an existing image. The hidden data is embedded in a manner that remains imperceptible to human observers. In this paper, a stego image that successfully hides the secret information and renders it undetectable to others is created by embedding a hidden message into an original image. The secret message may be text (the doctor's report of the patient's case) or maybe a secret image (chest x-ray) or encrypted secret image to increase security and guarantee the patient's privacy. The cover images may be brain, breast, and lung images. An enhanced LSB technique is introduced, incorporating common LSB and conditional MSB, with a focus on the lowest energy (blue channel) in the RGB spectrum. This approach aims to maintain image quality and imperceptibility. The innovation lies in strategically combining conditional MSB with the selective use of the blue channel, enhancing security. The method demonstrates superior concealment of secret information, surpassing conventional LSB techniques. Additionally, the Structural Similarity Index (SSIM) reports a high value of 0.998, affirming the technique's success in concealing information while preserving image quality. Performance metrics show positive results due to minimal changes (2 LSB bits at most). The experiments demonstrated positive outcomes in comparison to prior studies in this field.

Keywords: Steganography, LSB, MSB, Medical Image, Patient Privacy, Imperceptibility, Security.

تعزيز تقنية التشفير المخبأ للصور الطبية باستعمال تقنية البت الاقل اهمية المحسن مع البت الاكثر اهمية الشرطي بناءً على تنوع المتجه اللوني

ياسمين علاء حسن[1,2]*، عبد المنعم صالح رحمة[3]

[1] قسم علوم الحاسوب، كلية العلوم، جامعة بغداد، بغداد، العراق
[2] قسم علوم الحاسوب ، الجامعة التكنولوجية
[3] قسم علوم الحاسوب، كلية المعارف الجامعة، الانبار ، العراق

*Email: Yasmin.a@sc.uobaghdad.edu.iq

الخلاصة

يتضمن إخفاء الصور إخفاء أشكال مختلفة من المعلومات ، مثل النص أو الصور أو مقاطع الفيديو ، داخل صورة موجودة. يتم تضمين البيانات المخفية بطريقة تظل غير محسوسة للمراقبين من البشر. في هذه الورقة ، يتم إنشاء صورة Stego التي تخفي المعلومات السرية بنجاح وتجعلها غير قابلة للاكتشاف للآخرين عن طريق تضمين رسالة مخفية في الصورة الأصلية. قد تكون الرسالة السرية نصية (تقرير الطبيب عن حالة المريض) أو ربما صورة سرية (أشعة سينية للصدر) أو صورة سرية مشفرة لزيادة الأمان وضمان خصوصية المريض. صور الغلاف عبارة عن صورة للدماغ والثدي والرئتين. تم تقديم تقنية LSB المحسنة، والتي تتضمن LSB الشائع وMSB المشروط، مع التركيز على أقل طاقة (القناة الزرقاء) في طيف RGB. يهدف هذا النهج إلى الحفاظ على جودة الصورة وعدم وضوحها. ويكمن الابتكار في الجمع بشكل استراتيجي بين MSB المشروط والاستعمال الانتقائي للقناة الزرقاء، مما يعزز الأمان. تُظهر هذه الطريقة إخفاءً فائقًا للمعلومات السرية، متجاوزًا تقنيات LSB التقليدية. بالإضافة إلى ذلك، سجل مؤشر التشابه الهيكلي (SSIM) قيمة عالية تبلغ 0.998، مما يؤكد نجاح التقنية في إخفاء المعلومات مع الحفاظ على جودة الصورة. تظهر مقاييس الأداء نتائج إيجابية بسبب الحد الأدنى من التغييرات (2 بت LSB على الأكثر). وأظهرت التجارب نتائج إيجابية مقارنة بالدراسات السابقة في هذا المجال.

1. Introduction

The rise of the internet has triggered a notable transformation in the methods of digital communication. While this development has made communication easier, it has also presented a challenge in securing messages transmitted over an open network [1, 2]. Data transformation from one device to another currently relies heavily on communication. A message is sent from one side to another, and the uninvited side may listen in and learn what the message is about. The message must thus be shielded from outside interference [3] [4].

Stenography and cryptography are used as techniques to prevent intruders or malicious tampering with secret messages [5, 6]. By converting the data into an unintelligible format, cryptography safeguards the information, while steganography protects the information by concealing the contents with an appropriate carrier [7] [8].

Steganography involves hiding the existence of information. It aims to make the information invisible or undetectable to anyone who might be monitoring or intercepting the communication [9]. The objective is to maintain the confidentiality of the message or data by ensuring its secrecy from unauthorized individuals or entities [10] [11].

As a related work, in [7], a steganography technique called the least significant bit was created. The program used this technique to create the stego image barcode by combining the cover picture, which was a false barcode, with the message image, which was the actual barcode, and the result was (PSNR = 53.32). [3] presents the least significant bit of the steganography technique to create a stego-key and conceal a hidden text message inside a cover image using the MSB, and the result was (PSNR = 77.9). [12] proposes a method for hiding binary-encoded secret information within DICOM images using the discrete wavelet transform (DWT). The process involves segmenting 3D-image slices, collecting a host image based on a key, selecting block and slice numbers, embedding in the low-high band after adding a generated number, and applying the Hessenberg transform to specific-sized partitions. The confidential information can be either an image or text (PSNR = 35.23). Various statistical measures, such as peak signal-to-noise ratio (PSNR), signal-to-noise ratio (SNR), structure similarity (SSIM), and bit error rate (BER), have been used to report the results [13]. Based on the experimental results, the proposed system is very effective and robust.

The rest of this paper is organized as follows: The fundamentals of steganography have been mentioned in Section 1.1, and the least significant bit approach has been presented in Section 1.2. Some steganography applications on medical images have been illustrated in Section 1.3. In Section 2, the proposed technique has been explained. In Section 3, the results have been presented and discussed using different evaluation metrics. At the end, the conclusions of this work are explained.

1.1 Steganography

The primary objective of a digital steganographic technique is to discreetly encode confidential or classified information within various types of cover media [12]. Hidden data can take the form of binary bits, text data, image files, video files, and more. Cover media can encompass popular digital content such as images, videos, or text [14]. The concealed information within the cover media is commonly known as "secret data," while the resulting media after embedding is referred to as "stego-media" [13].

1.2 Least Significant Bit Approach

The least significant bit (LSB) technique is commonly used for steganography, which involves hiding a message or data within another piece of content without raising suspicion [1]. In this case, the image is used as the cover, and the secret message is embedded by replacing the least significant bit of each pixel with a bit from the secret message's binary representation [15]. Since the least significant bit has the least impact on the overall color or brightness of the pixel, the modification is often imperceptible to the human eye. However, when the image is decoded, the secret message can be extracted by simply reading the LSB of each pixel [16].

1.3 Steganography Applications on The Medical Image

In medical image steganography, the process involves hiding secret information (such as text or another medical image) within a cover image. The cover image acts as a carrier for the secret data. The basic idea is to modify the pixels of the cover image in such a way that the changes are not easily perceptible to the human eye, but the hidden data can still be extracted by the intended receiver [17, 18]. Several applications may benefit steganography in the medical field, as mentioned below, to save the privacy of the patient so no one can see any information about the case:

1.3.1 Hospital Storage and Archive

The objective is to conceal sensitive patient information when storing or archiving medical records, ensuring patient privacy and data protection from unauthorized employees. Implement a secure storage system with appropriate access controls, encryption, and backups to safeguard sensitive patient information. Use robust security protocols and comply with relevant data protection regulations [19, 20].

1.3.2 Protect Patient Information Transition

The goal is to conceal patient-specific information, such as COVID-19 imaging data or cancer diagnosis, during the transition between healthcare providers or institutions. The secret information is to be hidden in the patient's cancer or COVID-19 imaging data, which may include X-rays, CT scans, or other medical images. The cover image metaphorically represents the measures taken to protect the patient's privacy during the transition [21] [22].

1.3.3 Provide Psychological Support

The objective is to conceal the case diagnosis from a patient to provide psychological support during the treatment period. The secret information to be hidden is, for example, the positive COVID-19 test result or cancer diagnosis. The cover image is a neutral image chosen to maintain the patient's peace of mind and reduce anxiety [23].

2. Methodology

A commonly used and straightforward technique in the spatial domain for data hiding is the least significant bit (LSB) technique. When working with colored images that have three channels (red, green, and blue), an enhanced approach can be employed to leverage the channel with the lowest value for embedding secret messages. In this experiment, the red channel, which is the highest channel, is not used for information hiding. This paper presents an improved LSB technique that incorporates a pre-check step to enhance security and robustness against unauthorized users attempting to expose the method. When employing the LSB technique, the least significant bit of the cover image is substituted with the most significant bit of the secret message. Prior to this process, an additional verification step is performed by examining the most significant bit of the cover image. If it is 1, then the first LSB of the cover image is replaced with a bit from the secret message. If it is 0, then the second LSB of the cover image is replaced. This technique ensures that the system remains imperceptible to the human eye since the first or second LSB holds minimal significance compared to the overall image values, as depicted in Figure 1.

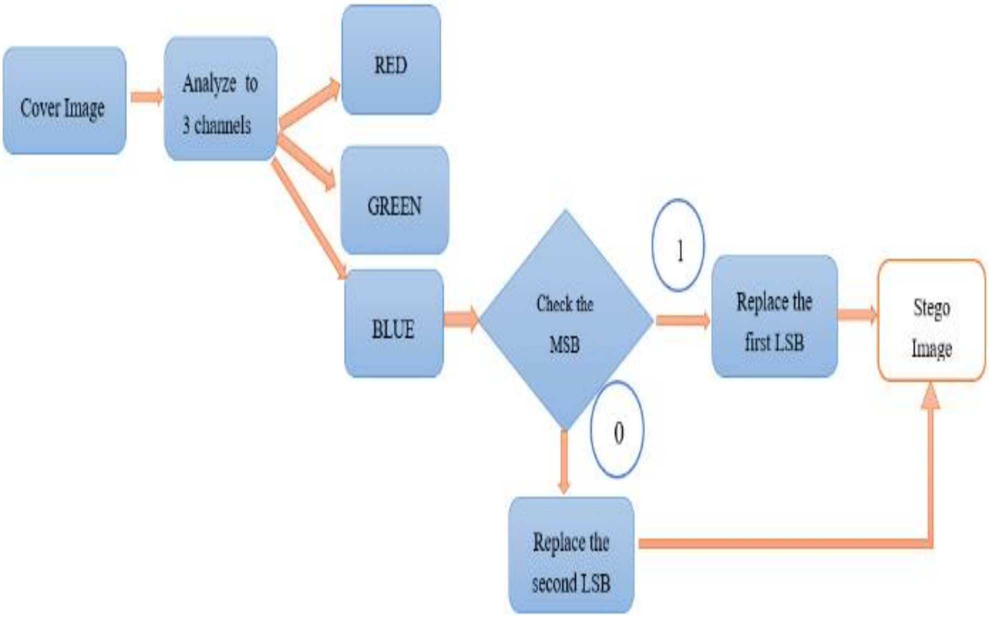


Figure 1: A block diagram that illustrates the encoding process on the sender side

On the receiver side, a similar procedure is applied. The stego image serves as input to the system, and the receiver verifies the image's integrity before extracting the secret message. If no tampering is detected, the receiver extracts the message from the stego image. The receiver accumulates the first or second LSB in a new array, which is then converted into a new image resembling the original secret message based on the most significant bit of the stego image, similar to what the sender performed as shown in Figure 2.

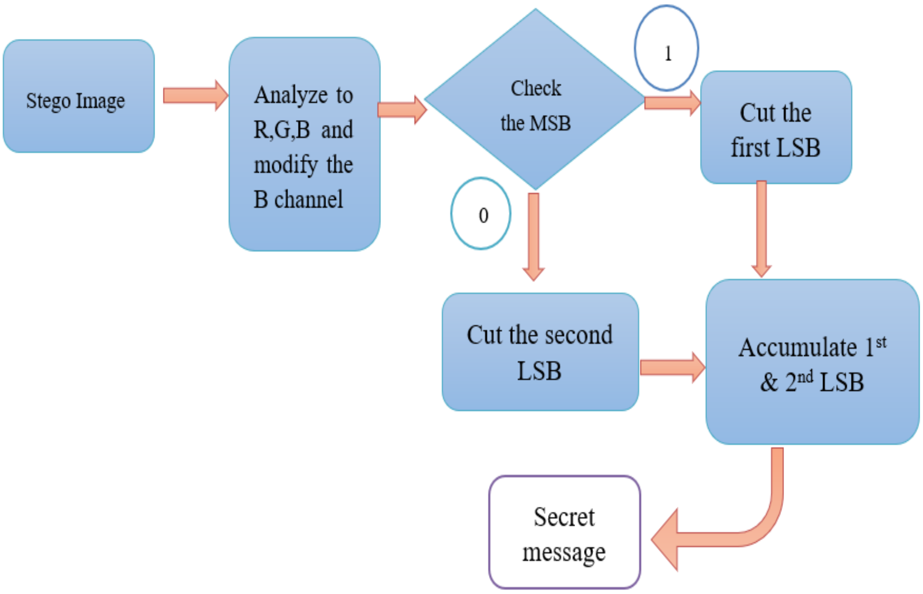


Figure 2: A block diagram that illustrates the decoding process on the receiver side

An example has been presented to explain the method of embedding the secret message on the cover image and distinguish between the traditional method and the proposed method.
Example:
In this steganography process, suppose the secret message starts with the first pixel value of 72, which in binary is represented as 0b01001000. The cover image's pixel values are converted to binary, and the steganography process is applied by embedding the bits of the secret message into the first or second least significant bits (LSBs) of each cover image pixel.
For example:
In the traditional method, the embedded watermark bit has always been added to the first LSB.
Cover Image Pixel: 135 (0b10000111) → Embed the first bit of the secret message in the LSB → Result: 134 (0b10000110)
Cover Image Pixel: 33 (0b00100001) → Embed the second bit of the secret message in the LSB → Result: 32 (0b00100000)

In the proposed method, the embedding process depends on the conditional MSB to thwart the unauthorized user.
Cover Image Pixel: 135 (0b10000111) → MSB=1 → Embed the first bit of the secret message in the first LSB → Result: 134 (0b10000110)
Cover Image Pixel: 33 (0b00100001) → MSB=0 → Embed the second bit of the secret message in the second LSB → Result: 35 (0b00100011)
The steganography process is repeated for all the pixels of the cover image and the secret message, resulting in a stego image that conceals the secret data within it. The embedded secret image remains hidden and imperceptible to human observers, ensuring the confidentiality and security of the information.
Traditional steganography provides simplicity in implementation, but it is vulnerable to detection; hiding information only in the LSB might be easily detected by analyzing statistical properties. Therefore, the proposed method (conditional MSB) adds a layer of security and complexity by considering the MSB condition.

The proposed method aims to enhance security by selectively embedding based on the MSB condition, making it more resilient against simple detection methods.

3. Experimental Results and Discussions

In this section, the results of our experiments have been presented and categorized into subsections for clarity: dataset, hiding text in medical images, and hiding images in medical images (grayscale and encrypted images).

3.1 Dataset

This project was implemented using the Python framework with 3 cover images (Lena, parrot, and pepper) as natural images. Brain, breast cancer, and X-ray chest images are used as medical images. The chest X-ray, a colored encrypted secret image, has been used as a secret image to be concealed within the cover image, and a segment of text used as a secret doctor report has been hidden in the cover image. The dimensions of the cover image were 1000×1000, and the secret image was 64×64 in size. Figure 3 illustrates the cover and secret images used in this work. The performance of the technique was evaluated using the peak signal-to-noise ratio (PSNR), signal-to-noise ratio (SNR), structural similarity index (SSIM), and bit error rate (BER).

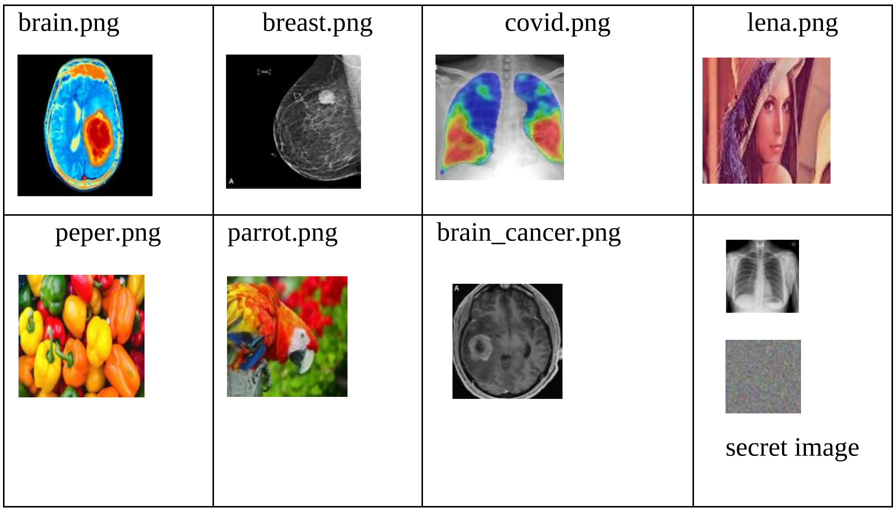


Figure 3: The cover and secret images used in this work

3.2 Hide a Text in Medical Image

In Table 1, a report of a doctor used as a secret message has been hidden in the tested brain image, along with tumor, breast, and chest x-ray images, to inform the specialist doctor about the patient's case. The secret messages concealed in the brain, breast, and chest X-ray images were:

Text1 (1305 bytes):

Subject: Cancer Diagnosis Report
Dear [Patient Name],
I am writing to inform you about the results of your recent medical tests. After careful examination, we have identified the presence of cancer cells in your brain. Based on the analysis of the biopsy samples, it has been confirmed that you have been diagnosed with [type of cancer]. I understand that this news may be overwhelming, but please remember that early detection is crucial for effective treatment. In the coming days, we will schedule an appointment to discuss the diagnosis in detail and provide you with a comprehensive treatment plan. Our team of oncologists and specialists will work closely with you to ensure the best possible outcome. It is essential to

stay positive and seek support from your loved ones during this challenging time. Remember that we are here to provide you with the necessary care and support throughout your treatment journey. If you have any immediate concerns or questions, please do not hesitate to contact our office. We are dedicated to guiding you through this process and addressing any uncertainties you may have. We remain committed to your well-being and will do everything possible to ensure the best course of treatment. Together, we will fight this battle against cancer.
Sincerely,
[Doctor's Name]

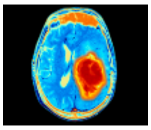
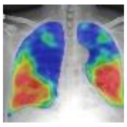
Text 2 (273 bytes):

This report confirms the diagnosis of breast cancer in the patient. The biopsy results indicate the presence of malignant cells in the breast tissue. Further evaluation and treatment planning are recommended to determine the stage and appropriate management of the cancer.

Text3 (38 bytes):

The test result of COVID-19 is POSITIVE

Table 1: Performance evaluation of the proposed technique using a text secret message

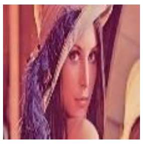
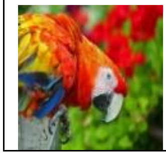
The cover image	The secret text message length	PSNR	SNR	SSIM	BER
	Text 1 1305 bytes	77.40	46.24	1.000	0.000016
	Text 2 273 bytes	87.41	56.24	1.000	0.000009
	Text 3 38 bytes	98.44	70.37	0.999	0.000005

From Table 1, the results are better when the secret message length is shorter and the differences are less from the original cover image. In general, shorter secret message lengths can have advantages in terms of data storage capacity, transmission speed, and decoding complexity. Shorter messages require fewer bits or characters, making them more efficient for various applications.

3.3 Hide a Grayscale Secret Image in a non-medical Image

In Table 2, a chest x-ray has been covered up with a non-medical image to keep the patient in the dark about their situation while offering crucial psychological support.

Table 2: Performance evaluation of the proposed technique using grayscale secret medical images

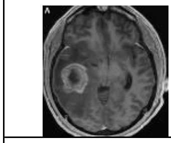
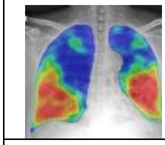
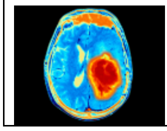
The cover image	The secret image	PSNR	SNR	SSIM	BER
		53.52	23.68	0.9982	0.000335
		53.66	25.92	0.9984	0.000216
		53.45	25.58	0.9982	0.000483

In terms of PSNR, SNR, SSIM, and BER, hiding grayscale chest images in pepper images seems to work better than the other experiments. This suggests that it strikes a good balance between image quality, structural similarity, and accuracy in keeping the hidden information.

3.4 Hide an Encrypted Image in a Medical Image

In Table 3, a colored and grayscale medical image hides a colored encrypted image using any method. It is obvious that when the cover image and the secret image were colored, the outcomes became worse because many alterations had an impact on the cover image's original details.

Table 3: Performance evaluation of the proposed technique using a colored encrypted secret image

The cover image	The secret image	PSNR	SNR	SSIM	BER
		50.64	22.26	0.9998	0.000009
		46.59	18.52	0.9978	0.000056
		41.54	10.38	0.9807	0.000007

The comparison between grayscale and encrypted images in our study reveals intriguing insights. Grayscale images exhibit superior steganographic performance, highlighting the efficacy of these techniques in simpler, monochromatic scenarios. However, when introducing encrypted images, an additional layer of security comes into play, albeit with a slight compromise in steganographic effectiveness. This delicate balance prompts thoughtful consideration of application requirements. If the priority is seamless information concealment with minimal visual impact, grayscale images stand out. On the other hand, situations demanding heightened security may lean towards encrypted images, even with a marginal reduction in steganographic robustness. Our research sheds light on the nuanced interplay between security and steganographic performance, providing valuable guidance for practitioners navigating the complex landscape of information concealment.

Table 4 illustrates a comprehensive comparison between our study and previous research endeavors across both image and text hiding schemes. This comparative analysis serves to contextualize the advancements and contributions made in this work within the broader landscape of steganography.

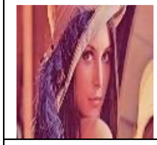
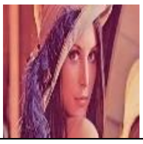
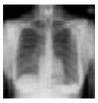
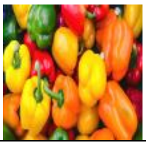
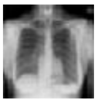
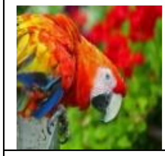
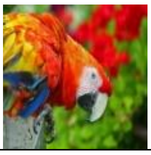
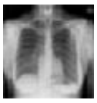
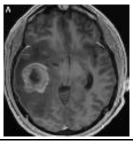
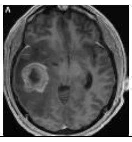
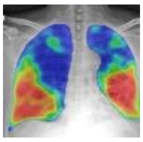
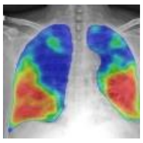
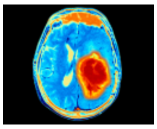
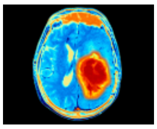
Table 4: Comparison with previous studies, including text and image hiding

Reference	Average PSNR for Image Hiding	Average PSNR for Text Hiding
[24]	36.71	-
[25]	-	71.83
[26]	30.95	-
[27]	49.51	-
[12]	35.23	38.75
[28]	-	83.25
[3]		77.90
[15]	-	38.4
Proposed method	53.54	87.74

3.3 Robustness Evaluation

In the evaluation of the proposed system, multiple metrics have been employed to comprehensively assess its performance. The average accuracy of this system stands at 98.7%, highlighting its efficacy in accurately recovering the hidden information compared to the original secret data. This metric is crucial for ensuring the reliability of the extraction process. The structural similarity index (SSIM) yielded a high value of 0.99, indicating a strong similarity between the original and the stego images. Additionally, the peak signal-to-noise ratio (PSNR) reached a remarkable value of 53.54 dB, underscoring the quality of the stego image compared to the original. While accuracy, SSIM, and PSNR primarily focus on the fidelity of the extracted information, integrity, an equally critical metric, examines the quality of the recovered data (NC=0.99). Integrity, as measured through pixel-wise comparisons, ensures that the extracted information aligns closely with the original secret content. Furthermore, combining encryption and steganography enhances the overall security and confidentiality of hidden information by encrypting the secret image before embedding it in the cover image. It provides protection not only against the detection of the presence of hidden information (through steganography) but also against understanding its meaning without the appropriate decryption key (through encryption). When these metrics come together, they create a strong framework for judging the steganographic system's accuracy, fidelity, and security, making sure it works well in many areas of performance.

Table 5: *NC* and extraction time values

Cover image	Secret image	Stego image	Extracted secret image	Accuracy	Normalized Correlation *(NC)*	Extraction time in seconds
				99.1%	0.998	0.4852
				98.8%	0.992	0.4135
				99.3%	0.984	0.4622
				98.5%	0.985	0.3221
				98.2%	0.997	0.3947
				98.4%	0.914	0.3955

Figures 4, 5, and 6 illustrate the results of this work visually because the human's eyes perceive the facts as images better than writing text for more clarity and effectiveness.

The utilization of the blue channel in this study has proven to yield favorable outcomes in terms of imperceptibility, ensuring that the resulting stego image remains indistinguishable from the original cover. This success can be attributed to the inherently low energy of the blue channel, as evidenced by the energy visualization depicted in Figures 7 through 11. These figures vividly demonstrate that the blue channel possesses the lowest energy among the channels considered. Consequently, the alterations made exclusively in the two least significant bits (LSBs) at most contribute to maintaining the visual integrity of the original image. The concealment of the hidden image is executed with precision, rendering it undetectable to unauthorized users and underscoring the efficacy of the proposed steganographic approach.

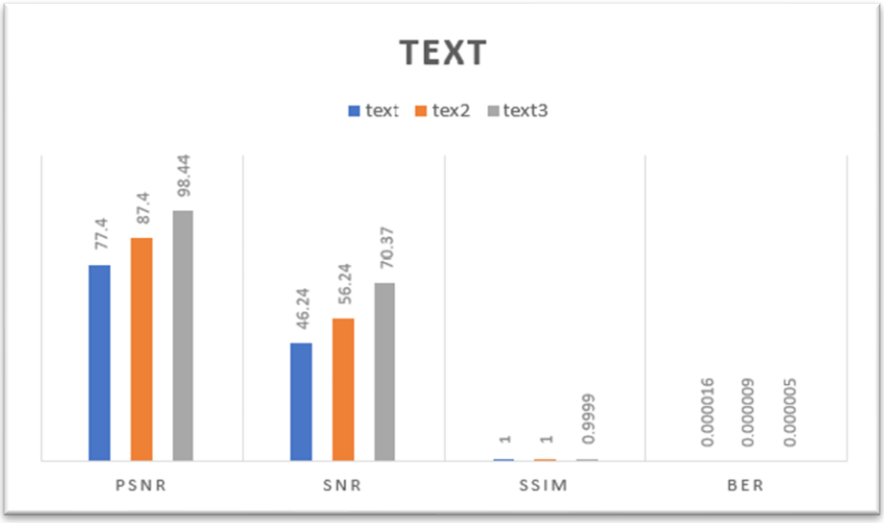


Figure 4: Experimental results of hiding text in a cover image

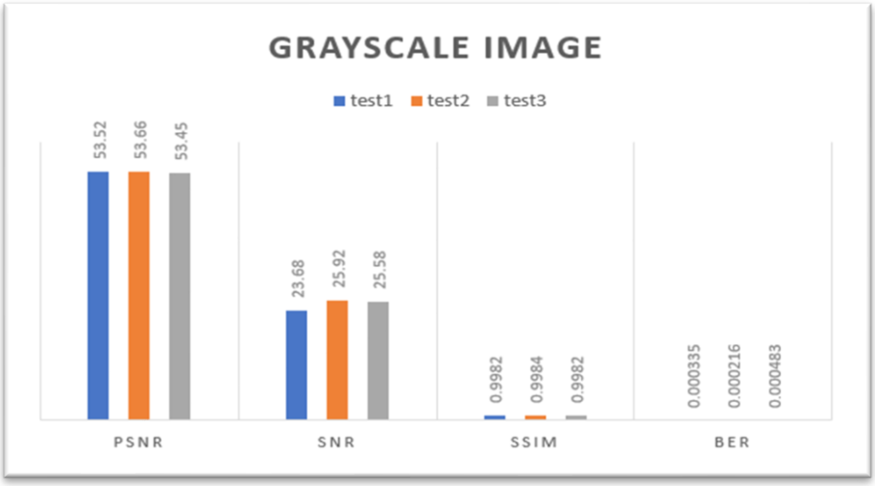


Figure 5: Experimental results of hiding a grayscale secret image in a cover image

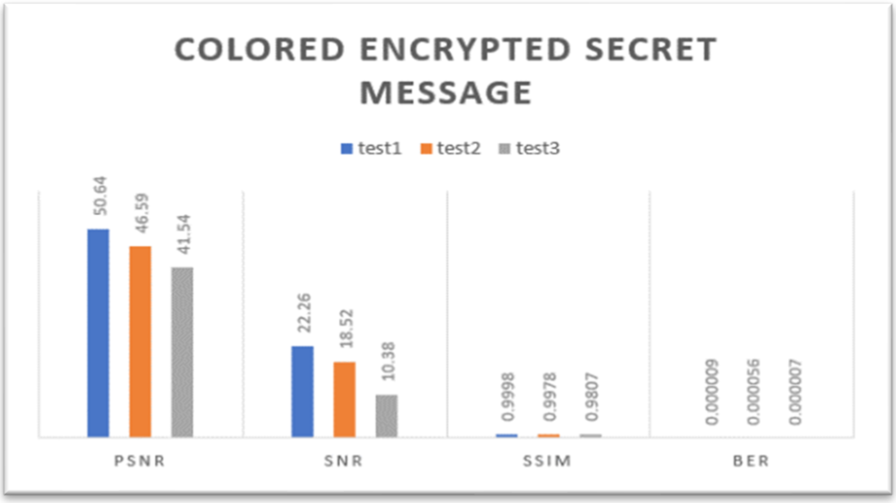


Figure 6: Experimental results of hiding a colored encrypted secret image in a cover image

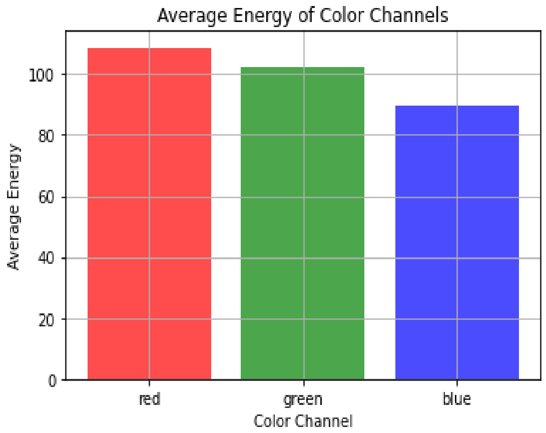


Figure 7: Illustrates the color energy of image parrot.png

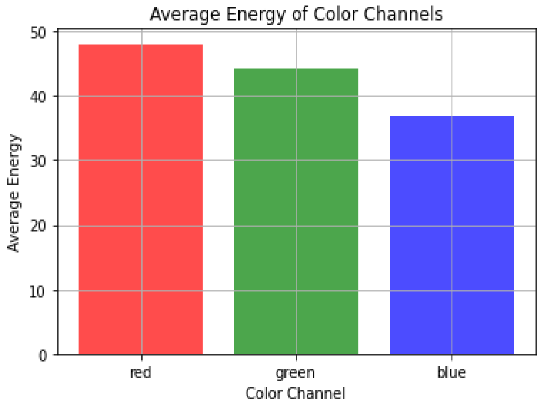


Figure 8: Illustrates the color energy of image brain.png

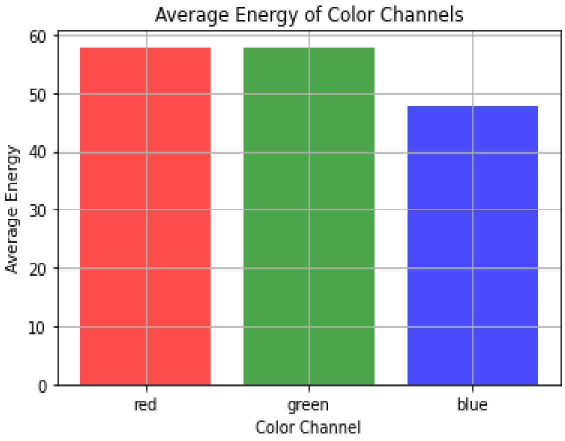


Figure 9: Illustrates the color energy image breast.png breast

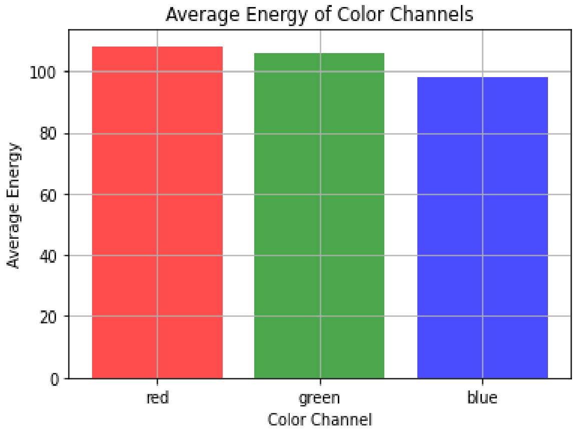


Figure 10: Illustrates the color energy of image brain_cancer.png breast

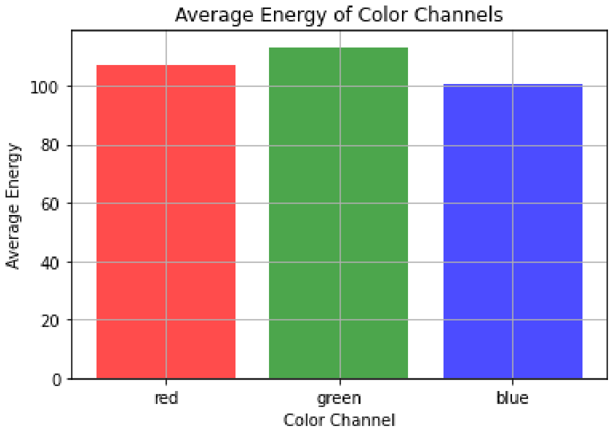


Figure 11: Illustrates the color energy of image covid.png

4. Conclusion

Digital image steganography plays a vital role in contemporary applications by enabling secure communication, thereby ensuring the importance of safeguarded transmission. The blue channel of the image can be beneficial to use as the location for hiding the secret image because it has the lowest energy and does not affect the human eyes. Therefore, to ensure imperceptibility, save the quality of the image, and at the same time improve the security of the secret information that has been transmitted, a blue channel shows good results. The utilization of a conditional most significant bit (MSB) ensures that the alterations made to the stego image, in comparison to the original cover image, are confined to a maximum of two least significant bits (LSBs). These LSB changes represent only a small fraction of the overall image values, which are predominantly composed of larger values. At last, the LSB, a common method with a conditional MSB, is simple and practically applied today but gives an effective application with results (PSNR = 53.54). The limitation was when using colored images for both the secret image and cover image, showing a low result compared to other tests. At last, medical images are very important data and should be treated with no loss in their value to save accuracy, integrity, confidentiality, and patient privacy.

5. Disclosure and conflict of interest

“Conflict of Interest: The authors declare that they have no conflicts of interest.”

References

[1] P. C. Mandal, I. Mukherjee, G. Paul, and B. Chatterji, "Digital image steganography: A literature survey," *Information Sciences,* vol. 609, pp. 1451-1488, Sept. 2022. https://doi.org/10.1016/j.ins.2022.07.120.

[2] S. Tyagi, R. K. Dwivedi, and A. K. Saxena, "A High Capacity PDF Text Steganography Technique Based on Hashing Using Quadratic Probing," *International Journal of Intelligent Engineering & Systems*, vol. 12, no. 3 , pp. 192-202, 2019. DOI: 10.22266/ijies2019.0630.20.

[3] M. M. Msallam, "A development of least significant bit steganography technique," *IRAQI JOURNAL OF COMPUTERS, COMMUNICATIONS, CONTROL AND SYSTEMS ENGINEERING*, vol. 20, no. 1, pp. 31-39, 2020.

[4] P. D. Shah and R. S. Bichkar, "Secret data modification based image steganography technique using genetic algorithm having a flexible chromosome structure," *Engineering Science and Technology, an International Journal*, vol. 24, no. 3, pp. 782-794, 2021.

[5] Z. H. Ali, H. M. Salman, and A. H. Harif, "SMS Spam Detection Using Multiple Linear Regression and Extreme Learning Machines," *Iraqi Journal of Science*, vol. 64., no. 10, pp. 6342-6351, 2023.

[6] M. Hashim, M. S. MOHD RAHIM, and A. A. ALWAN, "A REVIEW AND OPEN ISSUES OF MULTIFARIOUS IMAGE STEGANOGRAPHY TECHNIQUES IN SPATIAL DOMAIN," *Journal of Theoretical & Applied Information Technology,* vol. 96, no. 4, pp. 956-977, 2018, 2018.

[7] A. Alma, R. W. Wardhani, S. Muhasyah, and M. Delina, "Least significant bit steganography method for the digital data protection in the barcode," in *AIP Conference Proceedings*, 2019, vol. 2169, no. 1: AIP Publishing LLC, p. 040009.

[8] O. Hosam, "Attacking image watermarking and steganography-a survey," *International Journal of Information Technology and Computer Science*, vol. 11, no. 3, pp. 23-37, 2019.

[9] M. Mohan, S. KV, and D. B. Banagar, "An Efficient Framework to Protect Medical Images," *International Journal of Online & Biomedical Engineering,* vol. 16, no. 4, pp. 143–154, Mar. 2022.

[10] Y. A. Hassan and A. M. S. Rahmah, "An Overview of Robust Video Watermarking Techniques," *Iraqi Journal of Science,* vol. 64, no. 7, pp. 3613–3624, Jul. 2023.

[11] D. Megías, W. Mazurczyk, and M. Kuribayashi, "Data Hiding and Its Applications: Digital Watermarking and Steganography," vol. 11, Switzerland, ed: MDPI, 2021, p. 10928.

[12] B. A. Hameedi, M. M. Laftah, and A. A. Hattab, "Data Hiding in 3D-Medical Image," *International Journal of Online & Biomedical Engineering",* vol. 18, no. 3, p. 72, 2022, https://doi.org/10.3991/ijoe.v18i03.28007.

[13] H. M. Pandey, "Secure medical data transmission using a fusion of bit mask oriented genetic algorithm, encryption and steganography," *Future Generation Computer Systems,* vol. 111, pp. 213-225, 2020.

[14] J. Vivek and B. Gadgay, "Video Steganography Using Chaos Encryption Algorithm with High Efficiency Video Coding for Data Hiding," *International Journal of Intelligent Engineering & Systems,* vol. 14, no. 5, pp. 15-24, 2021.

[15] M. A. Hussein and S. Al-Momen, "Linear Feedback Shift Registers-Based Randomization for Image Steganography," *Iraqi Journal of Science,* vol. 64, no. 8, pp. 4131–4146, Aug. 2023.

[16] A. K. Sahu and G. Swain, "A novel n-rightmost bit replacement image steganography technique," *3D Research,* vol. 10, pp. 1-18, 2019.

[17] M. M. Hashim, A. A. Mahmood, and M. Q. Mohammed, "A pixel contrast based medical image steganography to ensure and secure patient data," *International Journal of Nonlinear Analysis and Applications,* vol. 12, no. Special Issue, pp. 1885-1904, 2021.

[18] A. Alabaichi, "Concealing a secret message in a colour image using an electronic workbench," *Iraqi Journal of Science,* vol. 26, no. 12, pp. 4964-4977, 2021.

[19] A. Vijayarangan, K. Sekar, and R. Srikanth, "Hybrid Steganography deployed in hospitals for compression of medical images," *Cryptology ePrint Archive,* 2021.

[20] M. A. Mohammed and H. B. Abdul Wahab, "A Novel Approach for Electronic Medical Records Based on NFT-EMR," *International Journal of Online & Biomedical Engineering,* vol. 19, no. 5, pp. 93-104, 2023.

[21] N. H. Hussein and M. A. Ali, "Medical Image Compression and Encryption Using Adaptive Arithmetic Coding, Quantization Technique and RSA in DWT Domain," *Iraqi Journal of Science,* vol. 63, no. 5, pp. 2279–2296, 2022. https://doi.org/10.24996/ijs.2022.63.5.38

[22] S. Arunkumar, V. Subramaniyaswamy, V. Vijayakumar, N. Chilamkurti, and R. Logesh, "SVD-based robust image steganographic scheme using RIWT and DCT for secure transmission of medical images," *Measurement*, vol. 139, pp. 426-437, 2019.

[23] J. Ripp, L. Peccoralo, and D. Charney, "Attending to the emotional well-being of the health care workforce in a New York City health system during the COVID-19 pandemic," *Academic medicine,*

[24] X. Duan, K. Jia, B. Li, D. Guo, E. Zhang, and C. Qin, "Reversible image steganography scheme based on a U-Net structure," *IEEE Access,* vol. 7, pp. 9314-9323, 2019. https://doi.org/10.1109/ACCESS.2019.2891247

[25] S. Bhargava and M. Mukhija, "HIDE IMAGE AND TEXT USING LSB, DWT AND RSA BASED ON IMAGE STEGANOGRAPHY," *ICTACT Journal on Image & Video Processing,* vol. 9, no. 3, pp. 1940-1946, 2019. DOI: 10.21917/ijivp.2019.0275

[26] Z. Fu, F. Wang, and X. Cheng, "The secure steganography for hiding images via GAN," *EURASIP Journal on Image and Video Processing,* vol. 2020, no. 1, p. 46, 2020.

[27] P. Pan, Z. Wu, C. Yang, and B. Zhao, "Double-matrix decomposition image steganography scheme based on wavelet transform with multi-region coverage," *Entropy,* vol. 24, no. 2, p. 246, 2022.

[28] K. N. Jassim *et al.*, "Hybrid cryptography and steganography method to embed encrypted text message within image," in *Journal of Physics: Conference Series*, 2019, vol. 1339, no. 1: IOP Publishing, p. 012061.