2025 International Conference on Computing Technologies (ICOCT)
Bangalore, India. Jun 13-14, 2025

LSB-Based Image Steganography Using Image Enlargement

Ashwini Ravindra
Chouthamal
Dept of EDT, National Institute of Electronics and Information Technology
Aurangabad, Maharashtra, India
ashwinichouthamal01@gmail.com

Saurabh Bansod
Scientist- 'C'
Dept of EDT, National Institute of Electronics and Information Technology
Aurangabad, Maharashtra, India
saurabhbansod@nielit.gov.in

Shashank Kumar Singh
Scientist- 'B'
Dept of EDT, National Institute of Electronics and Information Technology
Aurangabad, Maharashtra, India
shashank@nielit.gov.in

2025 International Conference on Computing Technologies (ICOCT) | 979-8-3315-2794-5/25/$31.00 ©2025 IEEE | DOI: 10.1109/ICOCT64433.2025.11118799

***Abstract*— Today's computer users must be careful about protecting their data. Data can be sent across networks in a variety of secure ways. Image steganography is an effective technique for concealing sensitive information. A popular method for hiding data is the Least Significant Bit (LSB) technique. This method covers picture pixels for the mystery message bits. However, the steganography image's quality always declined because of the challenge of employing more bits for embedding. In this study, image pixels are inverted to enhance the quality of the steganography image. This study suggests a novel technique that involves inverting the LSBs of the cover image pixels and adding up the pairs. After the secret data are placed in pairs, the sum of each pair is calculated. The pixel bits are then inverted based on that total to embed the secret bits. Lastly, some inverted bits again for even better results. The suggested strategy outperforms the substitution LSB scheme, according to thorough tests conducted on benchmark datasets. It also shows how well the proposed method performs in obtaining a large payload with acceptable visual quality for steganography images that are invisible to the human eye when compared to the most sophisticated steganography techniques.**

Keywords*— *Steganography; Data Hiding; Least Significant Bit (LSB); LSB Matching.

I. INTRODUCTION

Globally, 4.93 billion people used the Internet in 2021 during the coronavirus pandemic Governments, businesses, ministries, and individuals are increasingly communicating online instead of in person. Therefore, secure communication is essential for safeguarding private data sent over the Internet. Steganography conceals private information in cover media, including text, audio, video, and images, enabling safe communication. Since text is used more frequently than other materials, it is the perfect medium for covering communication. as stated in Of US users, 50% used audio and video calls, 20% used social networking sites, and 63% used the Internet to send text messages and emails. Techniques for text steganography use text to provide safe online communication [1].

There are now significant risks to obtaining secure data communication and preventing unauthorized users due to advancements in data transmission. Two of the several strategies that have been proposed to address data security are data encryption and data concealing. The process of transforming confidential data so that only authorized individuals may decipher it is called data encryption, or cryptography. But the presence of the ciphertext always attracts notice. Consequently, it is essential to communicate in a method that is concealed from other people. Thus, data concealing. Techniques are required Data hiding has two subfields: steganography and watermarking. Despite their intimate relationship, each of them serves a distinct role [2, 3,4]:

This paper is split into Nine sections. The first part is called the introduction. The several steganography systems in use are described in the II section. The third portion discusses the general introduction and operation of the LSB technique. Section IV explains the suggested methodology. Section V discusses the proposed method and how steganography works. Section VI: Analysis of LSB-based image steganography. Results and application in VII Section. In VIII. Future scope. Section IX has the conclusion.

II. STEGANOGRAPHY SYSTEMS USED SOME TERMINOLOGIES

A. Cover medium:

The first medium (text, image, video, and audio) in which the hidden message has been embedded

B. Secret message:

This is the message that will be concealed within the cover media.

C. Stego Medium:

Stego Medium is the final file created once the cover medium's hidden message has been concealed; it should resemble the cover as much as possible.

D. Embedding algorithm:

Embedding algorithm is the procedure for concealing the cover medium's secret message.

E. Extraction algorithm:

Extraction algorithm is the method for hiding the hidden message on the cover medium.

Image steganography is more common than other types of steganography. Due to the abundance of redundant information in photographs, it is easy to manipulate them to hide crucial information [5].

The principle of imperceptibility is the most important in steganographic systems since the resulting steganography

image should not exhibit any discernible distortion and should be able to conceal a significant amount of confidential information [6].

We presented a steganographic system [7] LSB matching approach. Determining the number of bits to be targeted for embedding at each pixel in the cover picture based on their similarity threshold is the foundation of the embedding process [7] technique. As a clue that this pixel contains concealed bits, the initial bit of the pixel utilized to embed data is inverted. Because the embedded pixel only changed the first least significant bit, the resulting steganography image is more visually and statistically similar to the original image. This maintains the highest embedding rate while achieving imperceptibility, the primary goal of all steganographic systems. Utilizing a picture enlargement technique. Here, image expansion is used to boost the proportions of a steganography image. Diffusion of the secret data over the image pixels in non-consecutive positions is an advantage of applying the enlargement procedure. It is more difficult to recover the embedded bits due to the spread of hidden data, which provides effective resistance to picture steganalysis.

III. THE LIST SIGNIFICANT BIT (LSB) TECHNIQUE

In digital steganography, the "Least Significant Bit (LSB) technique" is a technique that replaces the least significant bit of a pixel's color value in an image with a bit of secret data. This technique allows hidden messages to be embedded within the image without significantly changing its appearance to the unaided eye; in other words, it's a way to conceal information by deceptively changing the smallest detail of a pixel, which makes it a popular method for transmitting data covertly.

Think about a greyscale image where each pixel is represented by one byte to comprehend the LSB replacement approach. Assume that {P1, P2, P3} are the following greyscale pixels:

P2 = [11110010], P3 = [01001011], and P1 = [11011000] To incorporate the secret message M, where M is: M is equal to [010]. The bit stream M will be used instead of the LSBs of P1, P2, and P3. Consequently, P1= [11011000], P2=[11110011], and P3= [01001010] will be the embedded pixels.

Numerous enhanced LSB-based image steganography versions are released to boost efficiency. These methods are designed to increase capacity while maintaining the highest level of imperceptibility. A few of these methods, including [7, 8, 9, 10, 11, 12], are predicated on the idea of LSB matching. Some, including [13, 14, 15, 16, 17, 18], are based on the characteristics of edge pixels. Learning strategies like [19, 20] are being used by other researchers. Other methods are suggested that are based on the notion of image resizing [4, 21]. The suggested plan makes use of the idea of image resizing to increase the size of the image. Image resizing can be used to decrease or increase the size of an image.

IV. THE PROPOSED SCHEME

A. *The Embedding Phase:*

This phase entails searching each pixel of the cover image for matching bits. The number of bits that are marked for embedding is obvious by the similarity threshold; if a pixel is recycled to embed data, the first bit on it is balanced to indicate that it contains hidden bits. Once the embedding process is complete, the steganography image at large uses any image enlargement technique to distribute the embedded pixels over the final image. The algorithm for the embedding phase

B. *The Extracting Phase:*

This phase involves sending the steganography picture to the recipient after the embedding process has finished. A comparison between the received Stegano image and the cover image, which has been expanded using the same enlargement technique as in the embedding phase, is made to perform the extraction process. The threshold of similarity determines how many bits are appropriated from each pixel. The phase of extraction is shown in Figure [1.2] An observation of the LSB- based PDF insertion and extraction technique is shown in Figure 1.

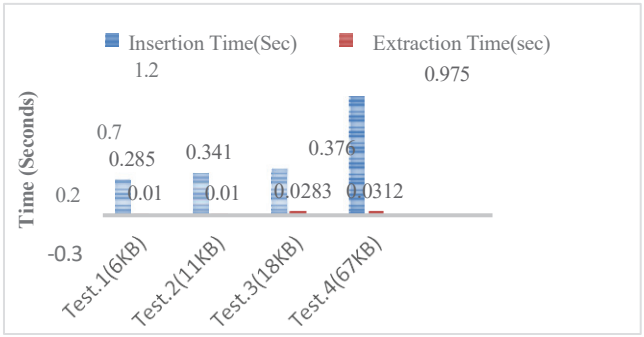

Fig. 1. LSB observation technique

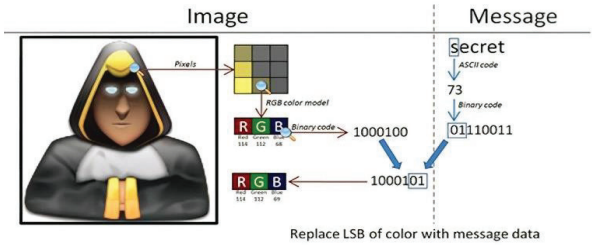

Fig. 2. Different methods for processing images and messages

V. THE PROPOSED STEGANOGRAPHY METHODOLOGY

The two algorithms that make up the suggested adaptive steganography scheme are the embedding method (Fig. 1) and the secret data extraction technique (Fig. 2). The embedding approach conceals secret information in the cover image by employing the HOG algorithm to choose a group of blocks of interest (BOI). The suggested method's HOG computation is regarded as the crucial stage, whereby the input cover image's horizontal and vertical gradient pictures are used to compute the gradient magnitude and angle.

The gradient angle is then quantized so that all angles fall within a predetermined fixed range (1, 2, 3, 4, 5). The quantized angle image's histogram of the orientated gradient is computed over a 2 x 2 block size to determine the dominating edge direction for every block. Next to applying an adaptive threshold value to each block's dominant magnitude value, One can select the block of interest. The PVD algorithm and in the habit of embeds secret data in the

dominant edge direction for each BOI, while LSB substitution is used to insert the remaining two pixels To absorb the entire secret message in the candidate blocks of the cover image, the threshold value is adaptively calculated based on the secret message's length. The primary actions of the suggested

VI. AN ANALYSIS OF IMAGE STEGANOGRAPHY BASED ON LSB

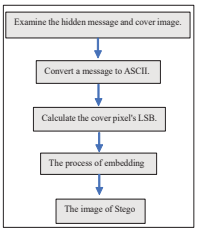

Fig.3. The embedding stage

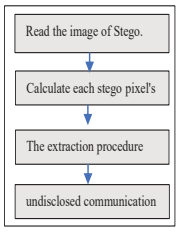

Fig.4. The extraction stage

1) While Figure 4 depicts the system's extraction phase, Figure 3 depicts the system's embedding phase. During the embedding phase, the system reads the cover image and the undisclosed message,
2) After that, it is transformed into ASCII. By substituting the concealed message bits for the cover picture's LSB, a secret writing image is produced.
3) Following the reading of the steganography image and the measurement of the LSB of each cryptography pixel
4) The outcome of the extraction operation is the undisclosed message that was first concealed.
5) The "embedding phase" of LSB (Least Significant Bit) steganography is the process of concealing secret information within a carrier image by substituting the secret message's least significant bits for each pixel. The "extraction phase" is the process of extracting the hidden message from the altered carrier image by reading and decoding the embedded LSBs.

VII. CATEGORIES OF GREYSCALE PICTURES

The greyscale images can be categorized based on the number of possible grey intermediate hues using a bit depth scheme. Below are the most widely used classifications:

Greyscale with 8 bits; The most widely used format, which is 6-bit and has 256 different shades of grey, offers greater contrast. With models, each pixel value can have any value between 0 and 255, making them quantitative in nature.

Greyscale 16-bit; offers 65,536 levels of grey, indicating both a larger intensity level and a higher capacity for differentiation.

Greyscale Floating Point; Its floating-point pixel intensity is positive, meaning that the theoretical number of grey levels is infinite. This kind is used in HDR photography and particular circumstances where precise image reproduction is crucial.

Fig 5. picture in greyscale

An image is represented as an array in the graphic above, with intensity is assigned to each pixel, with sections that are slightly lighter having a high intensity and those that are slightly darker having a low intensity. As mentioned before, the image's colour tones are entirely greyscale, with no differences.

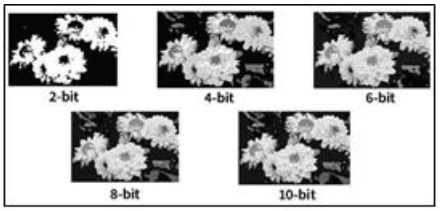

Fig.6. Various representations of bit depth

The above graphic illustrates how the bit depth in a greyscale image influenced the maximum number of greyscale shades. Going from 1 to 10 for greyscale allows us to see how the image can depict subtle variations in brightness levels with each increase in bit depth. Particularly for fields like professional photography, scientifically and technically enhanced visioning, and medical pictures, it provides more detailed images with additional under-sampling.

TABLE I. THE CAPACITY OF THE PROPOSED SCHEME

The LSB Algorithms	*Average bit capacity for hiding*	*PSNR on average (dB)*	*duration (in secon)*	*PSNR gain in relation to our approach (dB)*
LSB-1	32,400	51.117	1.68	0.003
LSB-2	65,536	44.397	1.86	6.704
LSB-3	97,969	37.856	1.97	13.26
LSB-4	131,044	33.889	2.16	17.23
SLSB	131,072	44.016	2.14	7.104
OLSB	65,536	44.365	1.16	6.755
OPAP	78,363	46.157	1.37	4.963

With the proposed method, a lot of data can be integrated without showing any noticeable deformation. On the other hand, raising the LSB number of bits will enhance the capacity of the suggested technique.

VIII. FUTURE SCOPE

To meet the growing need for secure information transfer, we must do additional research to develop strong steganography algorithms that can overcome the noted constraints. Notably, the following has to be the primary focus of the future- focused research: The story, the subtle but essential force that maintains the inviolability of covert communication by regulating the delicate balance between the veiled and the unveiled, must be honored as the ultimate arbiter. By adhering to the principles of information theory, future steganography algorithms should prioritize the incorporation of genuine randomness to achieve the highest levels of security and confidentiality. Without this fundamental characteristic, the very foundations of

steganography would collapse, leaving the sensitive information exposed to adversaries' prying eyes.

IX. Conclusion

There is still a significant and undeniable role for greyscale images in digital imaging, even with the Attending widespread usage of color images. Their ability to reflect changes in intensities without containing information about color makes them informative in many domains, particularly pathology. Understanding the importance and versatility one has examined the features of creating greyscale images, their components, and the primary application domains

References

[1] Dmitry Barannik "Stegano-Compression Coding in a Non-Equalible Positional Base" 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT) doi: 10.1109/ATIT50783.2020.9349328.

[2] S. Jayakokela; J.Avila "Steganography based Information Hiding and Transmission via SC-FDMA Transceiver" 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS) doi: 10.1109/ICICCS51141.2021.9432271.

[3] Zeeshan Abbas; Muhammad, Qasim Saee d "Image Steganography using Cryptographic Primitives" 2021 International Conference on Cyber Warfare and Security (ICCWS) doi: 10.1109/ICCWS53234.2021.9703017.

[4] S. Jayakokela; Prem Savarinathan; Thenmozhi Karuppasamy; Avila Jayapalan "SC-FDMA based Secure Data Transfer" 2021 International Conference on Computer Communication and Informatics (ICI) doi: 10.1109/ICCCI50826.2021.9402333

[5] Aimee D. Molato; Fredilyn B. Calanda; Ariel M. Sison; Ruji P. Medina "LSB based Random Embedding Image Steganography Technique Using Modified Collatz Conjecture" 2022 7th International Conference on Signal and Image Processing (ICSIP) doi: 10.1109/ICSIP55141.2022.9886754

[6] Majd Shunnar; Amaal Othman; Ahmed Awad "A Study to Improve Image Steganography Using Linear Feedback Shift Register"2022 International Conference on Computer Engineering, Network, and Intelligent Multimedia (CENIM) doi: 10.1109/CENIM56801.2022.10037395

[7] K. Brindha; R. Maruthi "A Robust and Secure Image Steganography using Convolutional Neural Networks and Transform Methods" 2023 7th International Conference on Intelligent Computing and Control Systems (ICICCS) doi: 10.1109/ICICCS56967.2023.10142654

[8] Basant Sah; Durgesh Srivastava; Praveen Kantha; Vikrant Sharma; Amit Garg "A novel approach to data hiding using high payload capacity" 2023 IEEE Fifth International Conference on Advances in Electronics, Computers, and Communications (ICAECC) doi: 10.1109/ICAECC59324.2023.10560158

[9] Nitish Kumar; Vasu Lakhani; Karanveer Singh; Mahim Bhardwaj; Shubham Raj "Development of LSB Based Steganography Method for Video and Image hiding"2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO) doi: 10.1109/ICRITO61523.2024.10522364

[10] Nishita N Murthy; Vinay Hegde " Secure Data Hiding: A Comprehensive LSB-Based Steganography Framework With Cryptographic Enhancements" 2024 8th International Conference on Computational System and Information Technology for Sustainable Solutions (CSITSS) doi: 10.1109/CSITSS64042.2024.10817051

[11] Keka Mukhopadhyaya; Anushree M; Bhargav M; Anusha E; Vikas MR " Combining Steganography and Cryptography Simultaneously to Safely Mask Data in Graphics" 2024 International Conference on IoT Based Control Networks and Intelligent Systems (ICICNIS) doi: 10.1109/ICICNIS64247.2024.10823259

[12] Angelina George; F Ashik; Alphonsa Jose; C R Kavitha "TripleACrypt: Cryptography and Steganography for the Preservation of Ancient Discoveries" 2024 8th International Conference on Computational System and Information Technology for Sustainable Solutions (CSITSS) doi: 10.1109/CSITSS64042.2024.10816889

[13] Jyoti Kanjalkar; Ajay Talele; Pramod Kanjalkar; Harshada Dhobale; Shrushti Gavali; Akhilesh Pimple; Nikita Waghmare "Random Pixel Embedding: A Novel Approach to Image Steganography" 2024 2nd World Conference on Communication & Computing (WCONF) doi: 10.1109/WCONF61366.2024.10692304

[14] Jingyi Qiu "Generative Image Steganography Scheme Based on Deep Learning" 2022 International Conference on Education, Network and Information Technology (ICENIT) doi: 10.1109/ICENIT57306.2022.00049

[15] Yara Hemavardhan Ram; Chilamanthula Ashritha; Posa Achyutha; Gowra Hardik; K. Vishnu Raj; V. S. Kirthika Devi "Image Steganography with Dual Encryption" 2024 2nd International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS) doi;10.1109/ICSSAS64001.2024.10760499

[16] Monalisa Sahu; Neelamadhab Padhy; Sasanko Sekhar Gantayat; Aditya Kumar Sahu "Performance analysis of various image steganography techniques" 2022 Second International Conference on Computer Science, Engineering and Applications (ICCSEA)doi: 10.1109/ICCSEA54677.2022.9936446

[17] Yang Wencui; Zhu Tingge; Liu Ying 2024 6th International Conference on Natural Language Processing (ICNLP)"A Review of Deep Learning Based Image Steganography Methods" DOI: 10.1109/ICNLP60986.2024.10692322

[18] Jyoti Kanjalkar; Ajay Talele; Pramod Kanjalkar; Harshada Dhobale; Shrushti Gavali; Akhilesh Pimple; Nikita Waghmare "Random Pixel Embedding: A Novel Approach to Image Steganography" 2024 2nd World Conference on Communication & Computing (WCONF) doi: 10.1109/WCONF61366.2024.10692304