LSB as a Steganography Tool in Information Security

Zainab Abdulhameed Alher[1], Basma M. Al Imran[2], Israa Al Ali[3]

[1] College of Education for the Humanities, University of Kerbala, Iraq.
[2] College of Computer Science & Information Technology, University of Kerbala, Iraq.
[3] University of Kerbala, Iraq.

***Abstract*— Least Significant Bit (LSB) method was used to encrypt and decrypt text in images to improve secret communication. An extensive investigation of the use, experimentation, and assessment of a hidden writing strategies to better understand how concealed communication promotes protected interaction and addresses ongoing difficulties. A retrospective and current analysis of concealing messages, practical application and appraisal of LSB approach, and a detailed review of its pros and cons. This examination delves deeply into steganography, specifically the technique of least significant bit encoding for concealing and revealing written messages within visual files, weighing both its potential benefits and disadvantages. Steganography study, safe messaging domain, visual and audio data encoding and decoding, strengthening online protection plans. Understanding and improving steganographic techniques can improve secure communication methods that could be used in future cybersecurity strategies and systems.**

***Index Terms*—Steganography, Embedding Extraction, Lsb, Cyber Security, Information Hidding, Information Security.**

I. INTRODUCTION

In an effort to shield texts within images, the Least Significant Bit (LSB) method emerged as a key player. A thorough probe into this tactic—its trials and evaluations—aimed at grasping how hidden writing strategies bolster secure exchanges while tackling current hurdles. Through a mix of reflection and contemporary scrutiny, messages tucked away via LSB were dissected; their merits and drawbacks thoroughly assessed. This inquiry plunged deep into steganography's realm, focusing sharply on LSB encoding. Herein lies the craft of embedding and unveiling text inside visual content; a balancing act between its upsides and pitfalls is crucial. Research in steganography strides forward: safeguarding messages becomes pivotal, with both image and sound files getting coded—and later decoded—to reinforce digital safety nets. As digital bonds strengthen worldwide, so does the need for data privacy in this era of online mingling. Born from necessity, cryptography encoded conversations to keep prying eyes at bay—a myriad of methods crafted to jumble yet also interpret words solely for intended recipients' understanding. Yet sometimes mere scrambling falls short. At such junctures, not just the message but its very transmission must stay unseen; herein lies steganography's purpose [1]. For ages untold, the art of hiding messages within harmless-looking carriers has stood strong as a key to safe info-keeping. As time has passed, steganography took on new forms; from ancient tactics of veiled messaging to its now digital state. With the tech boom came intricate methods like LSB (Least Significant Bit) steganography; it tucks away bits of data in media files such as pictures and sounds.

1. The Steganography as a Tool for Information Security

Our study dives deep into LSB steganography's role today—how vital it is for guarding secrets and its wide use in many fields. The toolkit for steganography is vast across varied sectors because it can hide facts inside normal media. Noteworthy uses include:

- Covert communication thrives through stegano-methods by sending secret notes hidden in visuals or audio, keeping under the radar.
- Digital watermarking with these techniques slips unseen marks into files—images, clips or tracks—to fend off theft and misuse while upholding copyright laws.

In military circles and spy work, this craft proves invaluable. By burying top-secret info well out of enemy reach—it boosts privacy greatly. Healthcare makes use of this too: embedding patient details inside scans or records keeps that data sealed tight (Protecting sensitive data). When we look at Authentication and secure access? Fascinating indeed!

DOI:http://doi.org/10.24086/cocos2024/paper.1157

Embedding IDs into cards or systems adds another layer; discreetly hiding important stuff right within them! And let's not forget Secure online transactions—stegano-methods cover their tracks nicely in web banking, vote tech, or shopping sites by safeguarding sensitive deal specifics. Steganography veils messages within other data, unlike cryptography. This latter scramble text to hide its true meaning from prying eyes. Steganography remains under-researched; yet recently, academics have started recognizing its scholarly worth and are delving deeper into this field's promise. These two practices—steganography and cryptography—are not at odds but support each other well. Secret communicators often turn to cryptographic methods before burying their information deep within multimedia platforms like images or audio tracks. Such measures boost the security of the hidden message manifold (Simmons). If adversaries suspect or detect concealed info though, steganography loses its edge—even if they fail to unlock the actual content [2]. Drawing on Greek roots for "covered writing," steganography poses a challenge: it hides critical info in plain sight, which thwarts easy detection by malicious watchers (Alice). It demands ingenuity to blend sensitive details seamlessly with everyday digital carriers. Simmons penned down 'the prisoner's problem' back in 1983—marking an allegorical take on steganalysis versus steganography—a relentless game of camouflage and discovery (Bob). Herein lies a tale where Alice encodes secrets for Bob using cleverly disguised means: maybe through sheet music or visuals in plain view while only they grasp how to decode them. What could be an innocent picture might just carry layers beneath that casual glance. Steganalysis plays foil to this covert art—the act where Eve listens intently, seeking whispers among silence; she has her finger ready to sever any secret lines binding Alice and Bob together [3]. Theirs is a delicate dance—one wrong step could mean exposure—but played well? It's a symphony unheard by unwelcome ears.

2. The problem of detecting steganography as a problem for information security

- **Undetectability:** A fundamental aim of steganography is to ensure that concealed information goes unnoticed by human faculties and also goes undetected by means of statistical analysis. This pursuit of achieving a level of invisibility akin to secrecy remains an avid challenge that calls for perpetual innovation and refinement in the techniques utilized.
- **Payload Capacity:** Steganography relies on sufficient embedding capacity to accommodate the secret message. Maintaining a high payload while securely communicating constantly challenges spacecraft designers as priorities for communication security and maximum cargo capacity are regularly at odds.
- **Robustness:** Ensuring that the hidden information remains intact when the stego medium undergoes various transformations, such as compression, resizing, or cropping, is another challenge. Developing techniques that can withstand these alterations while maintaining the concealed data's integrity is crucial.
- **Adaptability:** With the continuous development of new file formats and multimedia technologies, steganographic techniques must adapt to stay effective. Developing methods that can work with a wide range of formats and are resistant to emerging steganalysis techniques is a significant challenge.
- **Computational Efficiency:** The art of steganography poses a constant challenge in the realm of technology, demanding both efficacy and efficiency during the arduous task of concealing and unveiling data. It is paramount to employ algorithms that optimize computations and streamline time management, as they form an indispensable part of this process. Hence, it is crucial to invest adequate effort into devising reliable methods of implementation that strike a balance between optimal efficiency and unsuspected effectiveness—an ongoing struggle for those practicing steganography [5].

II. Scientific Papers Survey on Modern Steganography

The scientific community's fascination with steganography techniques has recently experienced a singularly remarkable surge. This phenomenon is evidenced by the overflow of image-based steganography algorithms being actively developed. Some notable works in this field include:

1) W. Bender et al. [6] explored various data hiding approaches and evaluated them in the context of tamper-proofing, copyright protection, and augmentation data embedding.
2) H. Farid [7] Describes a new approach to detecting hidden messages in images. The approach uses a wavelet-like decomposition to build higher order statistical models of natural images. A Fisher linear discriminant analysis is then used to discriminate between untouched and adulterated images.
3) J. Fridrich et al. [8] proposed a reliable and accurate method for detecting non-sequential least significant bit (LSB) embedding in digital images, focusing on color and grayscale images.
4) The paper "Imagery Steganalysis in Practice" [9], addressed challenges associated with JPEG images,

DOI:http://doi.org/10.24086/cocos2024/paper.1157

universal blind detection techniques, and special cases like JPEG compatibility steganalysis.

5) W. Zhang et al. [10] introduced a two-layer "plus-minus-one" data encoding technique, which can hide messages longer than LSB embedding.

6) Westfeld and Pfitzsch [11] investigated various steganography attacks and their effectiveness against different steganographic techniques.

7) X. Zhang and S. Wang [12] discussed efficient steganography embedding using modifications, emphasizing the vast number of redundant bits in digital images.

8) H. Zhang and H. Tang [13] developed a novel image steganography method based on statistical analysis, which allows for high-capacity message embedding in images while remaining undetectable by statistical tests like RS and Chi-square.

9) J. Kang et al. [2] presented a block-based adaptive threshold encoder and decoder design for image steganography.

10) N. Provos [14] proposed a statistical steganography approach, leveraging the large number of redundant bits in digital image representations and their widespread use on the Internet.

11) Shivendra Katiyar et al [15]. described an innovative steganography application in online voting systems, which merges the secret key with the cover image using the key image as a basis to create a virtually indistinguishable stego image.

The pursuits highlighted in these investigations, along with numerous others, aptly demonstrate the strides that have been made in steganography and the diverse spheres of knowledge wherein they hold exceptional prospects for utilization.

A. LSB (Least Significant Bit)

LSB (Least Significant Bit) encoding is a prevalent method in steganography for concealing messages or information within various digital media forms, including images, audio files, or videos. By modifying the least significant bits of the original data, which have the smallest influence on the appearance or quality, the hidden message can be embedded. As a result, the original data is altered to contain the secret message with minimal changes to its appearance or quality. As an illustration, a series of binary digits determines the color of each individual dot within a visual representation. The LSB of each color component (red, green, and blue) can be substituted with bits of the secret message, effectively integrating the message into the image. Typically, any modifications performed on the visual representation are often insignificant or may be indistinguishable to an unaided observer. Although LSB encoding is a popular steganography technique, it is not without its flaws. It can be detected using specialized software or by analyzing the digital media's statistical properties. Moreover, LSB encoding can degrade the original data quality, especially when encoding a large amount of information. In certain situations (Fridrich et al. [12]), the image's LSB is accessed randomly, and the pixel value may be slightly incremented or decremented.

LSB ADVANTAGES

The advantages of using the LSB (Least Significant Bit) technique in steganography include:

- **Simplicity**: Utilization of the LSB method is considered simple and does not require extensive expertise in coding or cryptography. This simplistic technique entails a substitution process whereby minute bits of digital media are exchanged with those mentioned within a covert message. This process targets vestiges that have a minimal impact on the medium.
- **Capacity**: The LSB method is capable of concealing a sizeable quantity of data in digital media, based on the magnitude and complexity thereof. Utilizing numerous LSBs to encode communications will lead to an enhanced capability for hiding substantial volumes of information within said digital medium.
- **Undetectability**: The LSB technique is often difficult to detect, especially if the changes made to the digital media are small and subtle. As the alterations affect only those bits with minimal significance, they may not be discernible to the naked eye of a human. This can pose an arduous task when attempting detection through conventional analysis apparatus.
- **Compatibility**: The scope of the LSB technique is broad and encompasses digital media that comprise images, audio files, and video files. Hence, it's a highly versatile approach that can be utilized in different contexts, such as clandestine communication or guaranteeing copyright protection.

LSB DISADVANTAGES

The LSB (Least Significant Bit) technique in steganography has some disadvantages and limitations, including:

DOI:http://doi.org/10.24086/cocos2024/paper.1157

- **Vulnerability to detection**: Although LSB encoding is often difficult to detect with the human eye, specialized software can be used to identify changes made to digital media. In addition, some types of compression and image editing software can inadvertently remove or alter LSB data.
- **Limitations in the amount of data that can be hidden**: Whilst the method of Least Significant Bit (LSB) operation can successfully conceal a substantial quantity of data within digital media, this is contingent upon both the size and number of bits that are modified without resulting in deterioration to the quality of said original media.
- **Potential quality degradation**: If too many LSBs are modified, the quality of the original media can be degraded. For example, changes to the LSBs of an image may result in noticeable color distortion or pixilation.
- **Lack of security**: The LSB technique does not provide any encryption or authentication of the hidden message. As is evident, it follows that whoever has access to the original media shall be able to perceive what has been concealed. This leaves no means of ascertaining its genuineness or soundness.
- **Difficulty in transmitting and receiving**: Since the LSB technique involves modifying the digital media, it can be difficult to transmit and receive the media without the risk of the message being lost or altered. This can make it challenging to use LSB encoding in some applications, such as covert communication.

The steganography approach described in the given passage involves concealing data within digital images by using the sensitivity of the human visual system (HVS). Specifically, the method takes advantage of the fact that the HVS cannot detect color vector brightness variations at higher visual frequencies. As the intelligence of the human eye may be limited, it is possible that fluctuations in chromatic depth might evade detection at particular thresholds. Within the realm of digital imagery, every single pixel is established through two antithetical concepts: a degree of "brightness" and an amount of "intensity." The scientific composition behind every single element that builds an image can be explained through these distinct values. This is represented through three color distinctions - red, green, and blue. Each one boasts a length typically consisting of 8 bits at maximum. This allows 28 unique shades of each color. Since the HVS may not detect subtle differences in color intensity, the least significant bit (LSB) of the color values can be used to encode additional information. For example, if the LSB of the blue color value is modified to encode data, the human eye may not notice the difference between blue intensity levels 11111111 and 11111110. This technique can be used to hide data in both bitmap and compressed images like JPEG, as the LSB of the discrete cosine transformed (DCT) components can be used to encode the hidden message. Overall, this steganography technique aims to exploit the limitations in order to hide data within digital images where the human eye cannot see it. By using the LSB of the color values, the technique allows for additional information to be encoded without significantly affecting the appearance or quality of the original image. The given passage describes the technique of Least Significant Bit (LSB) insertion for embedding data in a digital image. In the monochromatic image, each pixel's portrayal is framed by an octet, amounting to 8 bits. The binary sequence of eight digits determines the intensity and tone of every single pixel within a grayscale photo. Conversely, in an RGB-based color depiction, there are 24 bits assigned to each individual pixel, whereby each color has its own designated allocation of eight bits per pixel [16]. The LSB is based on the straightforward concept of replacing the final bit with the message bit. The LSB insertion method involves replacing the final bit of each color component with a message bit. Illustratively, if one were to consider an image of 800 by 600 pixels having a bit-depth of 24 bits, it would be capable of accommodating as much as approximately 180.000 bytes, or precisely 1440000 bits, worth of embedded data [8].

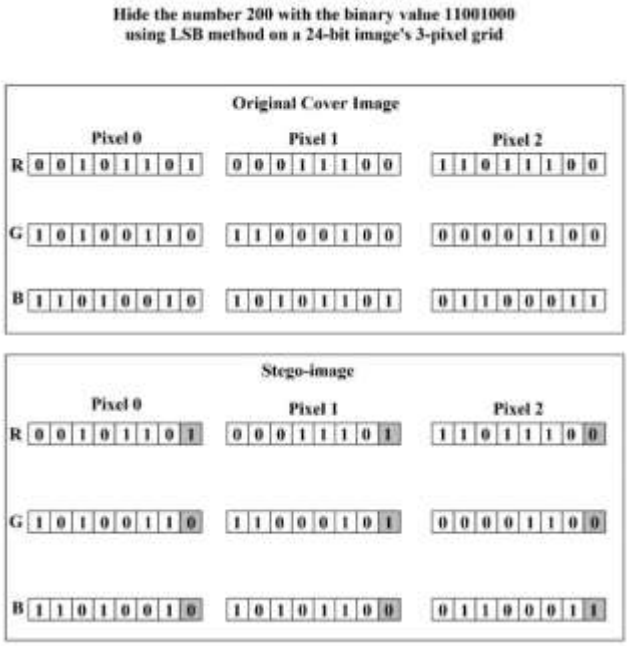

Figure 1 – Hiding a binary value using LSB method

DOI:http://doi.org/10.24086/cocos2024/paper.1157

Although the digits were embedded in the initial eight bytes of the lattice, only three bits caught one's attention and required revision to decrypt it. By utilizing cover sizes at their peak scale, only fifty percent of a picture's components are typically altered to conceal confidential messages [10]. Since there are 256 possible intensities for each primary color, modifying the least significant bit (LSB) of a pixel result in minute changes to the intensity of the colors. The message is successfully concealed because these alterations are imperceptible to the human eye. With a well-selected image, it is possible to conceal a message in the least and second-to-least significant bits without being able to distinguish between the two [16].

LSB based steganography Algorithm for embedding a text message

- Read the cover image and the text message to be hidden on the cover image.
- Convert the text message to binary.
- Calculate the LSB of each pixel of the cover image.
- Replace the LSB of the cover image with each bit of the secret message one by one.
- Write the stego image

LSB EXTRACTION ALGORITHM

- Read the stego image.
- Calculate the LSB for each pixel of the stego image.
- Extract the bits and convert every 8 bits to a character.

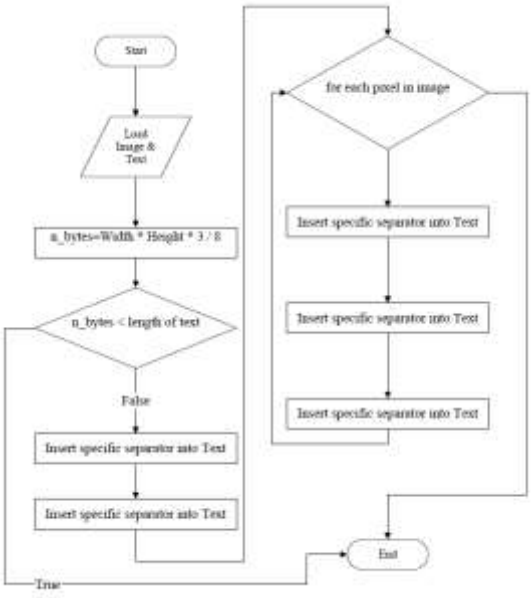

Figure 2 – LSB embedding block diagram

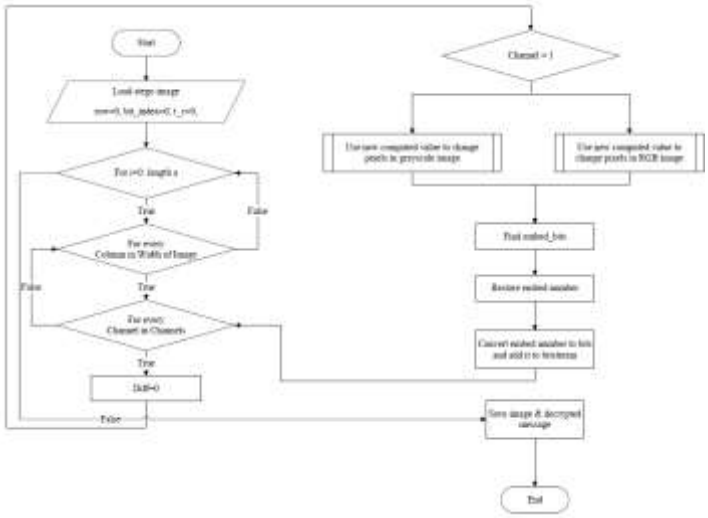

Figure 3 – LSB extracting block diagram

Table 1 – LSB method Testing Results Summary

Image Size	PSNR (dB)	MSE 0<MSE<255	SSIM 0<SSIM<1	BRISQUE (%)	Average Time (sec)
2040*1224	51.14	1.49	0.99	5.11	71.0
1020*768	51.15	1.49	0.99	9.83	44.0
680*452	51.13	1.50	0.99	12.33	27.0
510*339	51.14	1.49	0.99	6.38	32.0
255*169	51.11	1.51	0.99	4.16	22.0

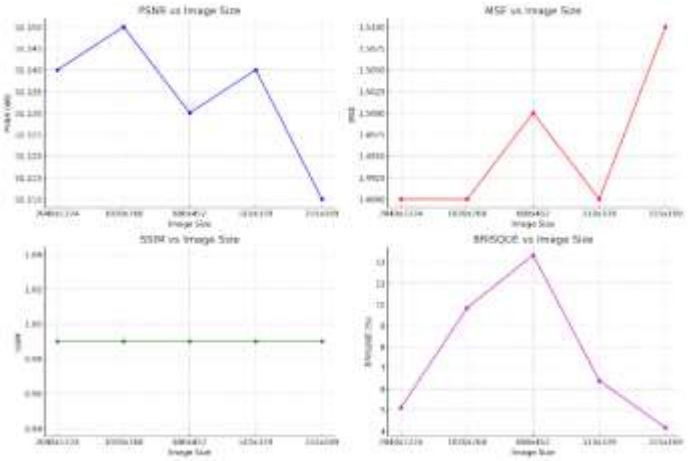

Figure 4: Line Graphs for PSNR, MSE, SSIM, and BRISQUE

DOI:http://doi.org/10.24086/cocos2024/paper.1157

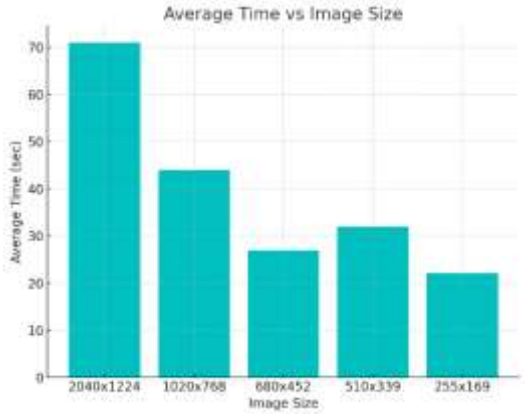

Figure5: Bar Chart for Average Time

LSB Method in Steganography	
Advantages	**Disadvantages**
Simplicity: Easy to implement, minimal coding	Vulnerability to detection
High Capacity: Hides significant data.	Data volume limitations
Undetectability: Hard to detect	Quality degradation risk
Compatibility: Works with many digital media	Lack of security: No encryption
	Transmission difficulties

Table 2: Advantages & Disadvantages of LSB method

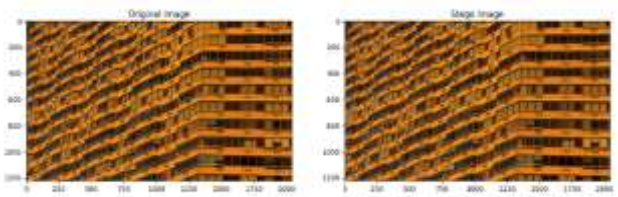

Figure 6 - Image comparison based on LSB algorithm

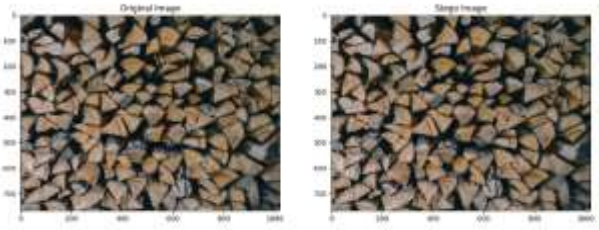

Figure 7 - Image comparison based on LSB algorithm

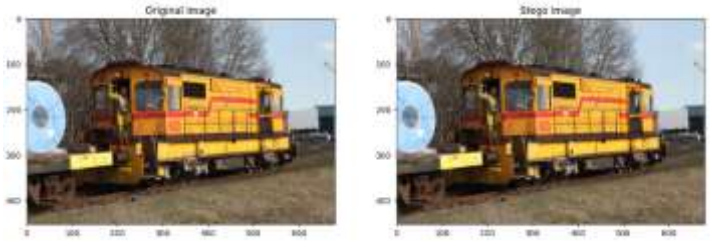

Figure 8 - Image comparison based on LSB algorithm

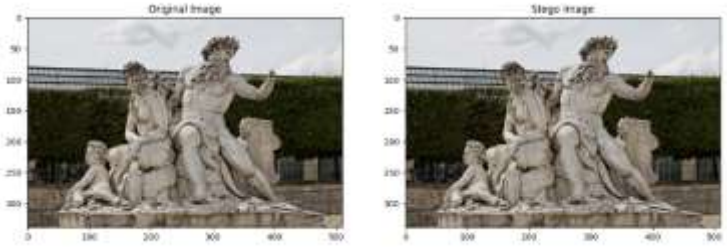

Figure 9 - Image comparison based on LSB algorithm

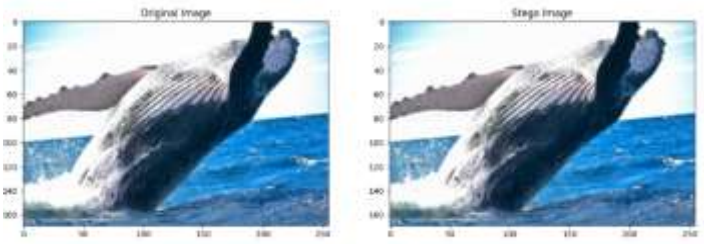

Figure 10 - Image comparison based on LSB algorithm

The Mean Squared Error (MSE) is used to gauge how well a steganographic image compares to the original image when the objective is to conceal information inside an image. Because the stego image is so similar to the original, a smaller MSE makes concealed data less detectable. A stego image created by a perfect steganography algorithm would be imperceptibly similar to the source image. To put it differently, a human observer should not notice any inconsistencies between the two photographs upon visual examination. In this application where the human visual system is typically insensitive to slight fluctuations in pixel values, an MSE sufficiently tiny so as not to be noticeable to the human eye would commonly be deemed "good" owing to our lack of acuity for modest deviations in individual pixel intensities. While mean squared error provides a simple way to measure error, it is important to remember that it does not necessarily reflect human perception of differences or quality, as there can be shortcomings when relying solely on a basic mathematical approach to evaluate something as complex as human vision. Because of this, MSE is frequently used with additional metrics like the Structural Similarity Index

DOI:http://doi.org/10.24086/cocos2024/paper.1157

Measure (SSIM) in steganography. An MSE near to zero would be desirable in the case of steganography, indicating that there is essentially no perceived difference between the stego image and the original. While an acceptable mean squared error is contingent on various influences, such as the steganography approach employed, the image's substance, and the amount and character of the concealed information, determining what constitutes a "good" MSE can differ dependent on several considerations. A tool for assessing how similar two photographs are is called the Structural Similarity Index (SSIM). The range of the SSIM result is from -1 to 1, with 1 denoting full structural similarity, or the equivalence of the two images. A very high degree of similarity between the two photos is shown by the SSIM result of 0.99 that we received. While the two images share a highly similar structure, brightness, and contrast, achieving a perfect match of 1.0 remains elusive as subtle differences persist between them. It's crucial to realize that SSIM is a perception-based model that seeks to gauge how the human eye would interpret a perceived change in the image's structural information. Therefore, a high SSIM score denotes that the differences (if any) between the photos are such that a human observer would not readily detect them. We propose a natural scene statistic based Blind/ Reference less Image Spatial QUality Evaluator (BRISQUE) which extracts the point wise statistics of local normalized luminance signals and measures image naturalness (or lack thereof) based on measured deviations from a natural image model. We also model the distribution of pairwise statistics of adjacent normalized luminance signals which provides distortion orientation information. Although multi scale, the model uses easy to compute features making it computationally fast and time efficient. The frame work is shown to perform statistically better than other proposed no reference algorithms and full reference structural similarity index (SSIM) [16]. This estimation is often used for distortion identification within different classification methods. The BRISQUE value is scaled between 0 and 1 (or 0 and 100%), where lesser the score, better the subjective quality of image. BRISQUE is computationally quite efficient making it an attractive option for use in practical applications.

III. CONCLUSION

The study demonstrated through consistently high Peak Signal-to-Noise Ratio values and remarkably low Mean Squared Error scores across all tested image dimensions that the Least Significant Bit Method can retain exemplary image quality with its steadfast constancy, as judged by these metrics. The near-perfect Structural Similarity Index (SSIM) values indicate that image quality remains virtually unaffected following LSB steganography application, demonstrating the method's success in retaining image visual integrity while embedding concealed information. However, the processing time, which ranges from 22 to 71 seconds, may be a constraint in circumstances requiring rapid data handling. Despite this, the LSB method's ability to embed safe, substantial data into many digital media formats, as well as its resistance to detection via the human visual system, highlights its promise as a steganographic tool in modern cybersecurity measures. The trade-offs between steganographic stealthiness and computational efficiency must be considered. Future work may concentrate on optimizing these features, possibly by incorporating advanced algorithms or machine learning techniques to improve both speed and security. As digital media permeates all parts of modern communication, the significance and use of steganography, particularly approaches like LSB, is certain to grow, necessitating continuing research and development in this fascinating subject of information security.

REFERENCES

1. Morkel T., Eloff J. H. P., Olivier M. S. An overview of image steganography //ISSA. – 2005. – T. 1. – №. 2. – C. 1-11.
2. Wang H., Wang S. Cyber warfare: steganography vs. steganalysis //Communications of the ACM. – 2004. – T. 47. – №. 10. – C. 76-82.
3. Bernard S. Digital images steganography using adversarial embedding : dis. – Centrale Lille Institut, 2021.
4. Techniques S. their use in an Open-Systems Environment-Bret Dunbar //The Information Security Reading Room, SANS Institute. - 2002.
5. Chang K. C. et al. A Novel Image Steganographic Method Using Tri-way Pixel-Value Differencing //Journal of multimedia. – 2008. – T. 3. – №. 2.
6. Lee CF, Chen HL A novel data hiding scheme based on modulus function //Journal of Systems and Software. - 2010. - T. 83. - No. 5. - S. 832-843.
7. Wang C. M. et al. A high quality steganographic method with pixel-value differencing and modulus function //Journal of Systems and Software. – 2008. – T. 81. – №. 1. – C. 150-158.
8. Artz D. Digital steganography: hiding data within data //IEEE Internet computing. – 2001. – T. 5. – №. 3. – C. 75-80.
9. Shih FY Digital watermarking and steganography: fundamentals and techniques. – CRC press, 2017.
10. Gene Carter, Peter Jenney NXP & Security Innovation Encryption for ARM MCUs.
11. Wallace GK The JPEG still picture compression standard //IEEE transactions on consumer electronics. - 1992. - T. 38. - No. 1. - C. xviii-xxxiv.

DOI:http://doi.org/10.24086/cocos2024/paper.1157

12. Farid H. Detecting hidden messages using higher-order statistical models //Proceedings. International Conference on Image Processing. - IEEE, 2002. - V. 2. - P. II-II.
13. Zhang HJ, Tang HJ A novel image steganography algorithm against statistical analysis //2007 International Conference on Machine Learning and Cybernetics. - IEEE, 2007. - T. 7. - S. 3884-3888.
14. Mandal J. K., Das D. Steganography using adaptive pixel value differencing (APVD) of gray images through exclusion of overflow/underflow //arXiv preprint arXiv:1205.6775. – 2012.
15. Mamta Yadav, Amita Dhankhar Image Steganography Techniques: A Review // IJIRST –International Journal for Innovative Research in Science & Technology. 2015. № 2 (2).

DOI:http://doi.org/10.24086/cocos2024/paper.1157