ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 11, Issue 5, May 2024

Strengthening Journalist Data Protection through Digital Image Steganography with 2LSB Embedding and Advanced Quality Metrics

[1] Sanderina Gladwin, [2] Jomol M J, [3] Rajalakshmi V R

[1] [2] [3] Department of CS&IT, School of Computing Amrita Vishwa Vidyapeetham, Kochi, Kerala, India

Corresponding Author Email: [1] sanderinavakayil@gmail.com, [2] jomolmj08@gmail.com, [3] rajalakshmi@kh.amrita.edu

Abstract— ***Information secrecy has grown more important in the world of digital communication, especially for journalists who handle sensitive material. Digital picture steganography provides a sophisticated method of encoding data into digital photographs while reducing perceptual modifications by utilizing the subtlety of the 2LSB (Two Least Significant Bits) embedding approach. A novel steganographic framework, which leverages sophisticated picture quality measurements–specifically the Peak Signal-to- Noise Ratio (PSNR) and Structural Similarity Index Measure (SSIM)–alongside robust Hamming code for error correction, to augment the 2LSB embedding process is presented in this work. Our research highlights the effectiveness of the framework in maintaining the integrity and accuracy of the hidden data through thorough empirical investigation. The outcomes signal a strong framework for the safe transfer of sensitive data, which represents a major advancement in the field of digital data protection.***

Index Terms—Digital Image Steganography, Information Se- crecy Techniques, 2LSB Embedding Approach, Hamming Code, Error Correction, Secure Data Transfer.

I. INTRODUCTION

The need to protect sensitive data is more than ever in this age of widespread digitalization, particularly for journalists who are frequently on the front lines of revealing facts that demand a high degree of secrecy. In this case, digital image steganography shows promise as a covert method of data protection by encoding important data into the digital picture canvas. In this regard, the 2LSB (Second Least Significant Bit) approach stands out in particular since it can mask massive data volumes within images with minimal effect on visual quality. By cleverly modifying the binary encoding of pixel values, this technique embeds information in a way that is nearly invisible to the unaided eye.

The work at hand integrates two critical quality criteria: The Structural Similarity Index Measure (SSIM) and the Peak Signal-to-Noise Ratio (PSNR) integrate: this integration aims at enhancing imperceptibility and reliability in steganographic data embedding. These measurements, playing a crucial role, ensure that an image's aesthetic integrity remains uncompro- mised by embedded data. While SSIM gives a more nuanced assessment of visual effect by analyzing the perceptual dif- ferences between the original and steganographically altered images, PSNR provides a quantitative estimate of the quality of the image reconstruction. Our method guarantees precise retrieval of data even in the event of probable transmission mistakes, while also securely enclosing it within the digital veil of images thanks to the error-correcting capabilities of Hamming code. This all-encompassing approach offers a forward-thinking response to the urgent problem of data protection in the digital era, particularly for journalistic pursuits that demand dependability and secrecy.

II. RELATED WORKS

Spearheading notable advancements in data security through their research published within the EVERGREEN Joint Jour- nal, Affiq S.M. Shaiden, Shayla Islam, and Kasthuri Subra- maniam [1]–esteemed researchers at the Institute of Computer Science Digital Innovation; UCSI University–presented a groundbreaking study titled ”Android-based Digital Steganog- raphy Application using LSB and PSNR Algorithm in a Mobile Environment.” Their work zeroes-in on our pressing need for robust data security as technology rapidly evolves [1]. The paper reveals the creation of an Android app that leverages algorithms, namely the LSB and PSNR, in active covert data embedding within photos. This advanced application enhances mobile communication security by streamlining the process of infusing data. Consequently, on popular platforms like WhatsApp and Instagram this work potentially revolutionizes sensitive information safeguarding; it highlights opportunities to enhance privacy during our digital age era.

A sophisticated steganographic method called ”High ca- pacity image steganography using LSB with modified binary addition on RGB indicator” was explored by A. Irwanto and B. Prasetiyo from the Computer Science Department at Universitas Negeri Semarang, Indonesia [2]. This research paper was published in the Journal of Physics Conference Series, showcasing their expertise in hiding information within images through advanced techniques. Their study sought to en- hance steganography through the application of an innovative technique - employing not only LSB but also integrating it with a modified binary addition approach on

RGB indicators. This unique strategy allows for concurrent insertion of two bits during encoding–a process that doubles message capacity when compared against conventional LSB methodologies. The empirical findings of the modified method specifically, a higher PSNR, an SSIM, and lower Mean Square Error (MSE) values demonstrate enhanced quality. This not only suggests reduced distortion but also superior preservation of the original image: indeed, this study underscores that incorporating advanced and secure steganographic techniques in digital communication is feasible.

Alade Oluwaseun Modupe, Amusan Elizabeth Adedoyin, Adedeji Oluyinka Titilayo, and Fenwa Olusayo Deborah con- ducted a comparative analysis research at Ladoke Akintola University of Technology in Nigeria. They focused on three image steganography techniques: Least Significant Bit (LSB), Most Significant Bit (MSB), and Pixel Value Differencing (PVD). The International Journal of Research and Review [3] published their findings; these underscored that employing an LSB approach yields superior results with a higher Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index Measure(SSIM)–an indicator of excellence in this field; con- currently, it exhibited lower Mean Squared Error(MSE). This translates to enhanced picture quality—less distortion—and improved similarity to the original. By paving a path for additional scrutiny into embedding capacity, security parame- ters' fine-tuning process alongside computational complexity assessment of steganographic techniques; this research bolsters data integrity within digital communication significantly.

Francesco Marchetti and Gabriele Santin dedicated their efforts to the challenging endeavor of picture similarity assessment, specifically through the application of Structural Similarity Index Measure (SSIM). They proposed an innovative approach - Continuous SSIM (cSSIM) for comprehensive image analysis at different resolutions; moreover, they formulated a Localized Weighted Variant that proves useful in real-world scenarios [4]. By establishing a rigorous connection between cSSIM-measured image similarity and the standard L2 norm, these scholars delineate boundaries and demonstrate equivalence under specific conditions. The research delves into the properties and limitations of SSIM, substantiating theo- retical conclusions through numerical trials; thus, it propels our comprehension in image quality assessment–specifically within the domain of image interpolation algorithms.

Ali Durdu presents a novel reversible picture steganography approach using RGB to embed images within images through a nested two-layer mechanism [5]. This methodology: it en- sures secure communication. How? By embedding a 24-bit hidden picture–using the LSB method–in a shrunken cover image; subsequently, this resized image undergoes further embedding into the original cover via a 4-bit process. The approach enhances steganography's security twofold—firstly, by introducing complexity to third-party detection; secondly, through increased capacity while maintaining pristine picture quality. Evaluations utilizing PSNR, SSIM, and chi-square analysis support its effectiveness. In summary, Ali Durdu's innovative solution provides secure hiding of high-quality images within other images. This technology is a game-changer in steganography, delivering enhanced security and increased capacity for digital communication.

Qusay S. Alsaffar, a professional from the Ministry of Higher Education and Scientific Research in Baghdad, Iraq, proposes a distinctive approach to improve data security by combining DNA encryption with GZIP compression to conceal messages within photos [6]. The Wasit Journal of Engineering Sciences published this paper that proposes a unique method: it encrypts messages using DNA techniques; compresses them with GZIP - and subsequently embeds the compressed mes- sage into images, employing the LSB methodology. This approach offers not only high levels of security but also achieves impressive data compression rates – up to 75%. Further, this technique maintains superb image fidelity as demonstrated by SSIM equaling 1 and PSNR values exceeding 68 dB. Punctuation Enhancement—this comprehensive secu- rity solution signifies a significant advance in safeguarding personal information throughout digital communication.

Ayesha Saeed and her colleagues present a unique im- age steganography technique that optimizes pixel selection based on texture complexity [7]. By using Complex Block Prior (CBP) criteria, they ensure minimal visual distortion and enhanced security when embedding data within images. Their research assesses texture complexity through image segmentation and adaptive techniques, resulting in higher image quality and improved steganographic security for hidden messages. The method's efficiency in preserving visual quality while maintaining robustness against steganalysis attacks is illustrated by their experimental results, which utilize typical image datasets. This marks a significant contribution to the field of secure digital communication.

In their work [8], Ke-Huey Ng, Siau-Chuin Liew and Ferda Ernawan put forth a groundbreaking approach to picture steganography. They utilize the Redundant Discrete Wavelet Transform (RDWT), QR decomposition, and a double entropy system in their innovative strategy; with an objective of concealing grayscale hidden images beneath other grayscale cover images - all through clever manipulation that leverages our human visual system. By segmenting images into blocks and utilizing entropy values for embedding, they achieve ex- ceptional imperceptibility with a PSNR value of 60.3773 and an SSIM of 0.9998. Their technology delivers a reliable and secure alternative for digital communication, with considerable advances in imperceptibility, computational efficiency, and the removal of false positives.

Bin Hureib and Gutub propose a powerful method for protecting medical data by combining Elliptic Curve Cryptography (ECC) with 1-LSB and 2-LSB picture steganography [9]. Their strategy bolsters the encryption process while concealing critical health records; this ensures top-tier security against unpermitted access. The utilization of ECC in encrypt- ing procedures—followed by concealing these encrypted data points within images through LSB techniques—showcases an impressive enhancement in protecting medical information. The dual-layer technique: it not only secures data, but also maintains image quality. In doing so–it presents a novel

solution for preserving critical healthcare information. Michael Pelosi, Nimesh Poudel, Pratap Lamichhane, Devon

Lam, Gary Kessler and Joshua MacMonagle [10] presented their research at the Annual ADFSL Conference on Digital Forensics Security and Law in 2018. They introduced a novel software concept - ”CounterSteg” - targeting specifically the identification and attribution of LSB image steganography through comparative analysis; this approach compares original images directly with suspected steganographic ones [10]. By leveraging sophisticated visualization tools that track bit and color-channel changes; this approach equips forensic profes- sionals to discern stenographic alterations created by diverse software applications effectively. This presents a significant countermeasure against potential misuse of stenography for embedding detrimental payloads within photographs. The find- ings emphasize an escalating issue within digital forensics due to steganography’s prevalence: particularly in malware propagation or data smuggling scenarios. This underscores not just its importance but also highlights requisite advanced technologies such as CounterSteg – crucial for bolstering both digital security protocols as wellas investigative procedures linked with these typesof crimes.

Mustansiriyah University researchers Zahraa Salah Dhaief, Raniah Ali Mustafa, and Amal Abdulbaqi Maryoosh [11] created a dual steganography method combining cryptogra- phy and steganography to improve security. Their solution employs the use of a chaotic map cipher for text encryp- tion; subsequently, LSB image steganography is utilized to embed the encrypted text within an RGB image. This method provides robust security while exhibiting minimal temporal complexity—an evident leap forward in secure communication technologies.

Yanting Wang, Mingwei Tang, and Zhen Wang from Xihua University advocate for a groundbreaking high-capacity adap- tive steganography approach: they integrate LSB replacement with Hamming code. Their method primarily enhances the em- bedding strength of secret data in images [12]. The key to their technique lies in focusing on edge areas — this not only boosts message capacity but also preserves image quality remarkably well, ensuring minimal distortion. Their rigorous testing has proven that this method significantly outperforms traditional techniques in terms of payload capacity, MSE (Mean Squared Error), PSNR, and histogram analysis - attesting its superior image fidelity and embedding capabilities. In the discipline of steganography, their study significantly enhances current practices by promising data hiding solutions that are not only more secure but also more efficient.

In their study [13], Sama N. M. Al-Faydi, Sahar Khalid Ahmed, and Heba N. Y. Al-Talb introduce a state-of-the- art technique in LSB image steganography; this method em- phasizes imperceptibility via an ideal cover-stego match: it prioritizes the concealment of secret data within innocuous areas of digital images–specifically targeting edge pixels for message insertion without compromising visual integrity - even after compression processes applied to generate stego-image.Leveraging both LZW compression method and fuzzy

edge detector yields remarkable picture quality metrics for this approach; PSNR levels reach infinity accompanied by SSIM and NCC values at one - thereby indicating perfect invisibility combined with accuracy. Delivering a significant leap in steganography, this approach offers an impressive balance: it provides ample capacity and robust security–all while preserving the image quality.

In their groundbreaking study on text steganography [14], Rafal Fadhil Jabbar and Osama Qassim Jumah Al-Thahab present a groundbreaking solution: harnessing the power of Radon and Barker code transforms. Their innovative method—designed to bolster security while amplifying data capacity—is based on leveraging the radon transform for text encoding; they deftly embed this within images using Barker code, guaranteeing flawless retrieval of encoded messages. This novel approach not only constitutes a major stride in steganography but also amalgamates extraction capabilities from Radon Transform with superior security provided by Barker Codes; consequently showcasing robustness against noise attacks without compromising high PSNR or acceptable SSIM values – thereby significantly propelling secure yet efficient data hiding techniques to new heights.

In their work [15], Ali Ahmed and Abdelmotalib Ahmed devise an enhanced secure picture steganography method: they utilize LSB and double XOR operations. The technique involves encrypting messages with a secret key - derived from the image’s MSB along with double XOR operations; subsequently, it embeds these encrypted entities into the image via LSB usage. This dual process of encryption and embedding significantly bolsters hidden message security. Presenting a novel strategy to secure data within images, their solution reinforces the security and integrity of concealed information; it exhibits promising results in PSNR and MSE measurements.

III. MATERIALS AND METHODS

This section outlines the thorough technique used in the investigation to improve the security of journalistic material using digital picture steganography. Subsections within the approach expound on the successive steps that comprise the steganographic technology, ranging from message preparation to quality assessment.

A. Message Preparation

The first step is to get the private message ready to be hidden in the digital format.

1) **Message Conversion:** The binary representation of the textual data is created to make the embedding process easier.

B. Hamming Code for Error Correction

To improve the data's integrity and dependability, error correcting coding is performed to the binary message before embedding.

1) **Encoding:** The Hamming code is used to encode the binary data, adding redundancy bits to allow for error detection and correction at the receiving end.

C. Steganographic Embedding

The embedding procedure, in which the encoded message is hidden within the digital image, is the central component of the approach.

1) **Cover Image Selection:** A suitable digital image is selected to serve as the steganographic process' cover medium.
2) **2LSB Embedding:** The encoded message is carefully put with little visible impact into the cover image's pixel values using the 2nd Least Significant Bit embedding technique.

D. Quality Assessment

The stego image is subjected to a stringent quality check after embedding to make sure the embedded data does not materially impair the image quality.

1) **Imperceptibility Measurement:** The imperceptibility of the embedding is measured using the Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM) metrics, which evaluate the visual similarity between the cover and stego images.

The methodological framework utilized in this investigation is shown visually in the following figure 1.

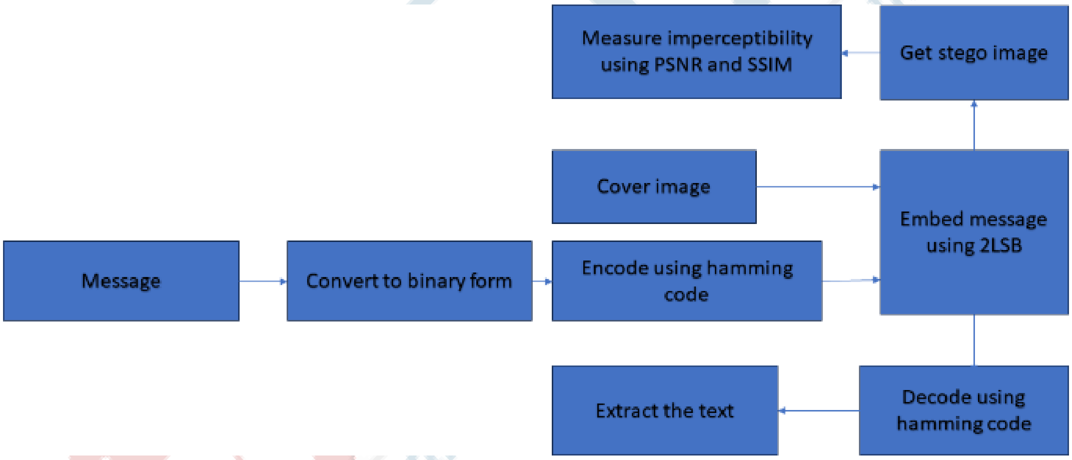


Fig. 1: Flowchart of the Steganographic Process

E. Accuracy Assessment

The precision of the data extraction procedure is crucial, in addition to assessing the Studying the steganographic image's imperceptibility through PSNR and SSIM measures. The percentage of all messages that are correctly decoded to all messages that are inserted and extracted is known as accuracy. This statistic makes sure that the encoded message is correctly and completely extracted from the stego image without any loss of data.

1) **Accuracy Measurement:** We calculate the proportion of successfully retrieved bits to total bits implanted in order to estimate the accuracy of our steganographic embedding. A 100% accuracy rate means that no errors were introduced during the embedding and extraction processes, resulting in a flawless message retrieval.

F. Data Extraction and Verification

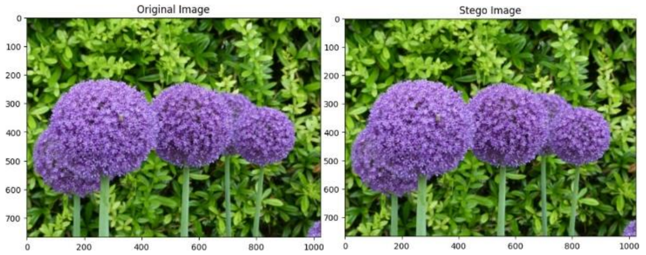
The message must be extracted from the stego image and its integrity must be confirmed in the last step.

1) **Decoding:** To fix any mistakes that might have happened during transmission or storage, the embedded message is recovered and decoded using the Hamming code.
2) **Text Extraction:** The original message is reliably retrieved by converting the rectified binary data back into text.

IV. RESULTS

The quantitative findings from the comparison of the stego images and the corresponding original photos demonstrate the efficacy of the digital image steganography technique used in this work. The outcomes indicate strong accuracy in extracting the embedded signals and the high degree of imperceptibility attained by the 2LSB embedding technique.

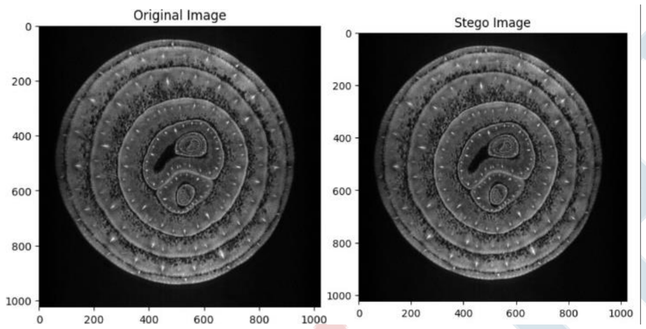
A. Image Analysis



(a)Original Image 1 (b) Stego Image 1

Fig. 2: Comparison of Original and Stego Image 1

A PSNR of 83.6632, an SSIM of 0.9999999968, and an Accuracy of 100% are reported in the first picture analysis, demonstrating the method's consistency in preserving image quality and message integrity.

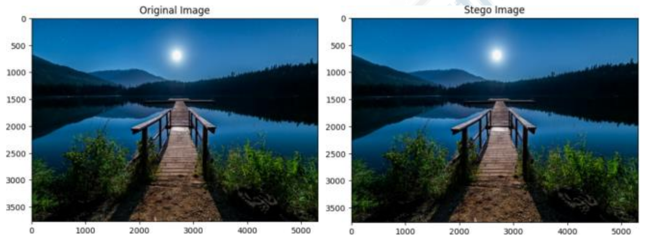


(a) Original Image 2 (b) Stego Image 2

Fig. 3: Comparison of Original and Stego Image 2

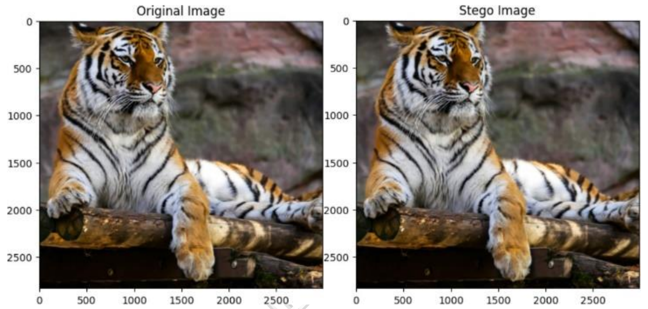
With a PSNR of 86.1271, an SSIM of 0.9999999746, and an accuracy of 100%, the second image analysis demonstrates imperceptible alterations and accurate message recovery.

The stego picture's remarkable fidelity to the original is confirmed by the third image analysis, which shows a PSNR of 98.0884, an SSIM of 0.9999999998, and an accuracy of 100%.



(a) Original Image 3 (b) Stego Image 3

Fig. 4: Comparison of Original and Stego Image 3



(a)Original Image 4 (b) Stego Image 4

Fig. 5: Comparison of Original and Stego Image 4

The results of the fourth image analysis indicate that the approach consistently preserves picture quality and message integrity. The PSNR is 94.01209121588226, the SSIM is 0.99999999957818, and the accuracy is 100%.

The aforementioned results demonstrate how well the used steganographic technique can incorporate messages within photographs with minimal influence on visual quality. Perfect precision and consistently high PSNR and SSIM values across several images validate the method's suitability for real-world scenarios demanding discreet and secure communication.

B. Discussion

This study's use of the steganographic method showcases an exceptional balance between imperceptibility and embedding efficiency. Specifically, the 94.01 PSNR score from the fourth image set suggests that this sophisticated embedding tech- nique effectively incorporates a secret message into a carrier image without significant degradation. Such preservation is vital to maintain stego-image's impervious aspect, serving as steganography's fundamental prerequisite.

The fourth image in the set demonstrates an SSIM value of 0.99999999957818, nearly equal to unity like all the other images; this suggests that during the embedding process, it retains not only its original structure but also brightness and contrast. This preservation becomes crucial when sophisticated steganalysis tools inspect potential abnormalities within these stego pictures based on image quality criteria such as these.

Our steganographic system incorporates a reliable error-correction code, evident from the consistent 100

Incorporating the Hamming code for error correction is a crucial element of this dependability: it ensures accuracy and prevents not only ordinary transmission faults, but also data loss or corruption–a prevalent issue in real-world applications.

C. Implications for Secure Communications

The field of secure communications significantly benefits from these findings: in scenarios where data leaks could yield disastrous effects–such as sensitive company communications or journalistic endeavors, effective information concealment becomes paramount. This method, with its potential for inclu- sion in activist and whistleblower tools; indeed—its applica- bility extends to broader applications like safe watermarking of digital content.

D. Directions for Future Research

While the encouraging results beckon further study, a focus on maximising embedding capacity without compromising image quality may be paramount; exploring adaptive steganog- raphy methods could also prove beneficial. Additionally, prob- ing into cryptography and steganography's combined use for layered security warrants investigation at this stage.

V. CONCLUSION

Conclusively, this work: it has formulated a steganographic technique–an effective and imperceptible method for conceal- ing data within digital photos. The resilience and reliability of the implemented approach prove advantageous in high- security scenarios; this is evident through the PSNR, SSIM, and accuracy metrics. This innovative technique could poten- tially serve as an instrument—a step forward—in ensuring secure communication during our digital age; its success thus furthers information security significantly.

Employing sophisticated steganographic techniques in real- world scenarios proves viable, a finding that signals the potential for further advancements in secure data transfer: this study indeed underscores such feasibility. As our digital world evolves–an ongoing process of development and expansion– the importance of these methods will inevitably amplify; thus, it underlines the imperative nature for continual research within this critical realm of investigation.

REFERENCES

[1] A. S. Shaiden, S. Islam, and K. Subramaniam, "Android based digital steganography application using lsb and psnr algorithm in mobile environment," 2021.

[2] A. Irwanto and B. Prasetiyo, "High capacity image steganography using lsb with modified binary addition on rgb indicator," in *Journal of Physics: Conference Series*, vol. 1918, no. 4. IOP Publishing, 2021, p. 042150.

[3] A. O. Modupe, A. E. Adedoyin, A. O. Titilayo, and F. O. Deborah, "A comparative analysis of lsb, msb and pvd based image steganography," *Int. J. Res. Rev*, vol. 8, no. 9, pp. 373–377, 2021.

[4] F. Marchetti and G. Santin, "Convergence results in image interpolation with the continuous ssim," *SIAM Journal on Imaging Sciences*, vol. 15, no. 4, pp. 1977–1999, 2022.

[5] A. Durdu, "Nested two-layer rgb based reversible image steganography method," *Information Technology and Control*, vol. 50, no. 2, pp. 264– 283, 2021.

[6] Q. Alsaffar, "An encryption by using dna algorithm for hiding a compressed message in image," *Wasit Journal of Engineering Sciences*, vol. 10, no. 1, pp. 1–10, 2022.

[7] A. Saeed, M. J. Khan, H. Shahid, S. I. Naqvi, M. A. Riaz, M. S. Khan, Y. Amin *et al.*, "An accurate texture complexity estimation for quality- enhanced and secure image steganography," *IEEE Access*, vol. 8, pp. 21 613–21 630, 2020.

[8] K.-H. Ng, S.-C. Liew, and F. Ernawan, "An improved rdwt-based image steganography scheme with qr decomposition and double entropy," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 3, 2020.

[9] E. S. Hureib and A. A. Gutub, "Enhancing medical data security via combining elliptic curve cryptography and image steganography," *Int. J. Comput. Sci. Netw. Secur.(IJCSNS)*, vol. 20, no. 8, pp. 1–8, 2020.

[10] M. Pelosi, N. Poudel, P. Lamichhane, D. Lam, G. Kessler, and J. Mac- Monagle, "Positive identification of lsb image steganography using cover image comparisons," 2018.

[11] Z. S. Dhaief, R. A. Mustafa, and A. A. Maryoosh, "Hiding encrypted text in image using least significant bit image steganography technique," *International Journal of Engineering Research and Advanced Technol- ogy (IJERAT)*, vol. 6, 2020.

[12] Y. Wang, M. Tang, and Z. Wang, "High-capacity adaptive steganography based on lsb and hamming code," *Optik*, vol. 213, p. 164685, 2020.

[13] S. N. Al-Faydi, S. K. Ahmed, and H. N. Al-Talb, "Improved lsb image steganography with high imperceptibility based on cover-stego matching," *IET Image Processing*, vol. 17, no. 7, pp. 2072–2082, 2023.

[14] R. F. Jabbar and O. Q. J. Al-Thahab, "Text steganography in image depending on radon barker code transforms," in *Journal of Physics: Conference Series*, vol. 1963, no. 1. IOP Publishing, 2021, p. 012106.

[15] A. Ahmed and A. Ahmed, "A secure image steganography using lsb and double xor operations," *International Journal of Computer Science and Network Security*, vol. 20, no. 5, pp. 139–144, 2020.