Securing and Hiding Text Data Through Multimedia Steganography Using LSB and 3-Tier DWT with AES-256 Encryption

Ahmad Kashif
Department of Information and Communication Engineering
The Islamia University of Bahawalpur
Bahawalpur, Pakistan
ahmadkashifch8@gmail.com

Muhammad Hamza Shoukat
Department of Information and Communication Engineering
The Islamia University of Bahawalpur
Bahawalpur, Pakistan
hamzashoukat957@gmail.com

Muhammad Jameel
Department of Information and Communication Engineering
The Islamia University of Bahawalpur
Bahawalpur, Pakistan
jameelmuhammadjameel966@gmail.com

Abdul Rehman Chishti
Department of Information and Communication Engineering
The Islamia University of Bahawalpur
Bahawalpur, Pakistan
rehman.chishti@iub.edu.pk

***Abstract*—Concealing information inside of digital carriers is vital to safeguard data as it passes in and out of a network. The framework presented in this paper utilizes Least Significant Bit (LSB) substitution steganography for data embedding in image and 3-tier Discrete Wavelet Transform (DWT) methods for embedding in audio files. In order to improve security, the embedded data is encrypted using Advanced Encryption Standard 256 bits (AES-256) to make the data confidential, durable, and resistant to unauthorized detection. It proposes an improved method in data protection while guaranteeing the integrity of host media and more stability against steganalysis campaigns. The experimental results show that, under this approach, one achieves high PSNR and SSIM (i.e. high PSNR and SSIM), indicating not only the imperceptibility but also the robust security feature.**

***Index Terms*—Steganography, LSB, DWT, AES-256, Cybersecurity.**

I. Introduction

In steganography, by definition, we are speaking of secret communication, either of a message that has already been created, or even a message created and subsequently embedded, using digital media in such a way that obscures the existence of the message. Steganography is different from cryptography, which resembles encrypting content to conceal what is being said, whereas steganography conceals the very existence of a message. This paper presents technique which embeds hidden text in images through least significant bit (LSB) substitution and in audio using three tier discrete wavelet transform (3-tier DWT). In order to go one step further, a prior AES-256 encryption is applied before embedding. First, the proposed method achieves high detectability and security level levels that are suitable for confidential text communication in multimedia environment.

The rest of the paper is organized as follows: Section II reviews related work, Section III details the methodology, Section IV presents experimental results, and Section V concludes with future directions.

II. Literature Overview

In order to enhance the security of data and positioning accuracy of data within the image, a method utilizing Least Significant Bit (LSB) image steganography and a secret map technique is proposed as stated in [1]. The inadmissibility state is achieved at a reasonable cost and the embedding ability is high. But histogram based analysis can still be effective against it and robustness to common image transformation such as compression and format change are limited because of possible embedding behavior.

In [2], a method is suggested to help enhance visual quality and reduce the capability of detection by blending LSB steganography and Fibonacci sequences within the classical cryptography. The steganographic images provided by this method were indistinguishable visually to original. It does not include strong encryption schemes or resistance to cryptographic attacks, and therefore it is not suitable for high security situations.

The authors in [3] have suggested that a traditional LSB embedding scheme for hiding information in digital images offers simplicity and high data payload support. Although this method is easy to implement and computationally efficient, it is highly susceptible to statistical and structural attacks. Slight changes in pixel values—due to compression, resizing, or noise—can reveal hidden information or damage the embedded content.

Work cited in [4], a basic LSB-based embedding technique has been explored to hide data in uncompressed audio samples. This method is lightweight and easy to implement in practice. However, it does not tolerate signal loss due to compression,

DOI: https://doi.org/10.67535/tsp.000001.008
Published under the ICACNC 2025 Proceedings

noise addition, or filtering. Furthermore, if stego audio is compromised, the absence of encryption exposes the payload to interference and unauthorized access.

It has been demonstrated in [5] that a phase coding-based technique embeds data in the phase component of the audio signal, providing better resistance to perceptual distortion and increased inaudibility. This spectral domain approach is proven to be more robust than LSB-based methods. However, its reliance on DES encryption weakens its cryptographic strength, as DES is outdated and vulnerable to brute force and differentiation attacks.

According to the method outlined in [6], another approach introduces a smoothing-based method to embedding data in audio signals to improve the perceptual quality of stego audio. Although this method is successful in preserving sound quality and minimizing audible artifacts, it lacks robustness against common signal processing operations such as compression, resampling, or filtering. Furthermore, no encryption is implemented, making the embedded data susceptible to steganolysis.

The proposed method outperforms prior techniques by addressing their weaknesses, such as the vulnerability of traditional LSB methods to statistical analysis and brute force attacks, overcome by AES-256 encryption that secures hidden data even if detected. Unlike basic LSB audio steganography, our 3-tier DWT approach enhances robustness by spreading data across multiple frequency bands, ensuring imperceptibility and resilience to noise, compression, and signal processing threats. This hybrid system improves data confidentiality, steganalysis resiliency, and reliability compared to existing methods.

III. Proposed Methodology

A. LSB Steganography for Secure Image-Based Text Embedding

In contemporary cybersecurity, the safe and discrete transfer of data is very important for critical information. The solution of least significant bit (LSB) steganography is effective, and it embeds encrypted text to the digital image and keeps the data existence secret, confidentiality and integrity. Using this, pixel value is encoded in binary text by changing least significant bits with no conspicuous change in the image.

1) Embedding Process: The LSB method systematically adds encrypted text to the image as follows:

- **Text Encryption and Binary Conversion**: The text is first encrypted for security (for example, using AES), then converted to binary. For example, the character 'B' (ASCII 66) becomes 01000010.
- **LSB modification of pixels**: The red (R), green (G), and blue (B) pixel values of the image are extracted, and their LSBs are modified to store binary data. Example: A pixel (10101101, 11001010, 10011011) becomes 101 embedding bits (10101101, 11001011, 10011011).
- **Data distribution and stego image creation**: The binary message is divided into multiple pixels for embedding. The resulting stego image is stored and can be transmitted securely, with the hidden data undetectable without prior knowledge of the procedure.

2) Extraction Process: To recover the hidden text, the receiver uses the reverse process:

- **Stego Image Processing**: The stego image is loaded, and its RGB pixel values are accessed.
- **Binary Reconstruction**:The LSBs are sequentially extracted and concatenated (for example, 01000010 = 'B').
- **Decryption and Recovery**: The binary sequence is converted to text and decrypted using AES to obtain the original message.

3) Graphical Representation of Cover and Stego Images: The figures below (2, and 3) illustrate the structural patterns of cover and stego images after 777 KB data is embedded using the steganographic method. The *coolwarm* color map highlights the intensity variations in different regions of the images.

The minimal visible changes between the two graphs confirm that the steganographic method maintains inaudibility when embedding secret data.

4) Cybersecurity Implications: LSB steganography enhances data security with:

- **Discrete Communication**: It supports confidential applications such as secure messaging and intelligence operations.
- **Strong Confidentiality**: Combined with AES encryption, it ensures that the data cannot be read without the decryption key, even if steganography is suspected.

B. Three-Level DWT for Secure Audio Data Embedding

In cybersecurity, audio steganography embeds encrypted text into audio signals using a three-level discrete wavelet transform (3-level DWT), ensuring inaudibility and resilience against unauthorized access. This method hides sensitive data in high-frequency subbands, which enables secure communication while thwarting detection or tampering by adversaries.

The audio signal undergoes a 3-level DWT decomposition:

- **Level 1**: Split into low-frequency (A1) and high-frequency (D1) subbands.
- **Level 2**: A1 is split into A2 (approximate) and D2 (detail).
- **Level 3**: A2 is split into A3 (approximate) and D3 (detail).

The high-frequency subbands (D1, D2, D3) are used to embed AES-encrypted text, taking advantage of their fast fluctuations to mask changes, preserving audio quality.

1) Embedding and extraction process: Plain text is encrypted with AES, converted to binary, and embedded in the D3, D2, and D1 subbands. A marker (STEGO-MARKER-START) flags the start of the data. Stego audio is decomposed through a 3-level DWT. The marker searches for hidden bits in D3, D2, and D1, which are extracted and decrypted using AES to recover the original text.

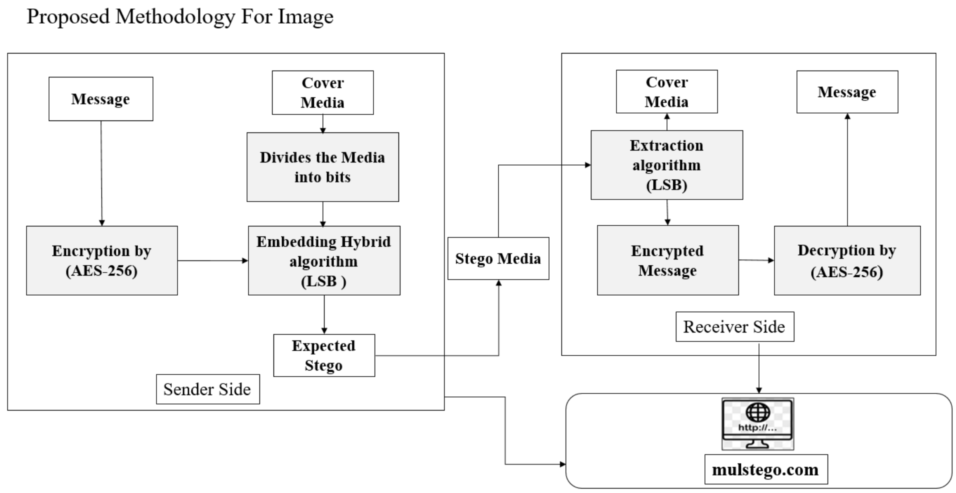

Fig. 1. Image Steganography

2) Waveform Analysis of DWT-Based Audio Steganography: Analysis of audio steganography figures below (5) cover and stego audio waveforms show strong visual similarity, indicating that the 3-level DWT embedding preserves the signal structure after embedding 165 KB data. The waveforms are almost undetectable with only minor differences in amplitude that are inaudible to human perception. This confirms minimal quality degradation and robust data hiding. Quantitative metrics SNR, MSE, PSNR, and PESQ further validate the effectiveness of the method, ensuring security, robustness, and undetectability while maintaining audio integrity.

3) Cybersecurity Implications: This 3-level DWT approach enhances secure communication, reinforces confidentiality, and resists eavesdropping. The combination of AES encryption with wavelet domain embedding ensures data security even if intercepted, while maintaining perceptual audio integrity. This is suitable for sensitive environments that require robust, discreet data transmission.

C. AES-256 Encryption Combined with Image and Audio Steganography for Secure Data Embedding

This work combines AES-256 encryption with image and audio steganography for secure data hiding. Plaintext is encrypted using AES-256 in CBC mode with PKCS7 padding, a 16-byte IV via `crypto.randomBytes(16)`.The 256-bit key is generated using `crypto.randomBytes(32)`, downloadable, with secure exchange assumed via external channels, ensuring resistance to brute force attacks. The ciphertext is embedded into image LSBs and audio high-frequency subbands via three-level DWT, maintaining visual and audio integrity while enhancing robustness. This method strengthens privacy for applications like digital fraud investigations, ensuring reliable, covert communication.

IV. Experimental Results

Quantitative metrics were used to evaluate the proposed AES-256 integrated steganography method by conducting experiments on images [7], [8] and audio datasets [9], [10], focusing on imperceptibility, robustness, and protection against steganalysis while ensuring high-quality embedding.

A. Evaluation Metrics

The following standard metrics were used to evaluate the performance of the system, implemented using Python 3.9 with `numpy`, `scipy`, `scikit-image`, and `pypesq` for metrics evaluation, executed in Visual Studio Code:

1) For Image Steganography:

- **Mean Squared Error (MSE)**: Measures the mean squared difference between the cover and stego media. A low MSE indicates minimal distortion, which is important for insensitivity and detection resistance (see Table I).
- **Peak Signal-to-Noise Ratio (PSNR)**: Measures the quality degradation in decibels (dB), inversely related to MSE. A PSNR above 40 dB indicates excellent image quality protection, with 30-40 dB being acceptable for specific applications (see Table II) for a comparison of these differences.
- **Structural Similarity Index (SSIM)**: Evaluates perceptual similarity (0 to 1) based on brightness, contrast, and texture. Values close to 1 indicate high similarity, ensuring that the embedding avoids detecting noticeable artifacts by human vision or tools (see Table III).

2) For Audio Steganography:

- **Mean Squared Error (MSE)**: MSE quantifies distortion by averaging the squared differences between the original and stego audio samples. A low MSE ensures minimal, inaudible changes, which are important for avoiding detection by listeners or tools. Its low values in tests confirm preserved audio fidelity (see Table IV for comparative results between cover and stego audios).
- **Peak Signal-to-Noise Ratio (PSNR)**: PSNR measures quality retention in decibels (dB), comparing the peak power of the original signal to the embedding noise.

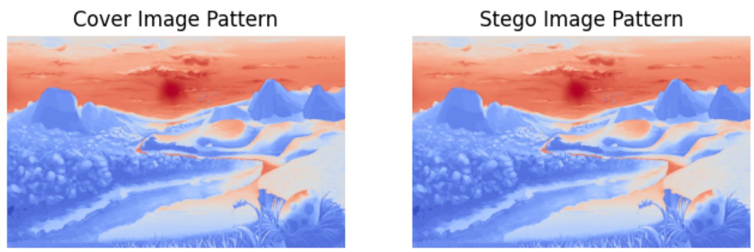

Fig. 2. Comparison of Cover and Stego Image 1

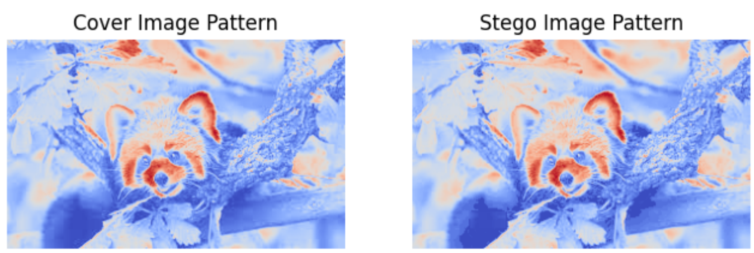

Fig. 3. Comparison of Cover and Stego Image 2

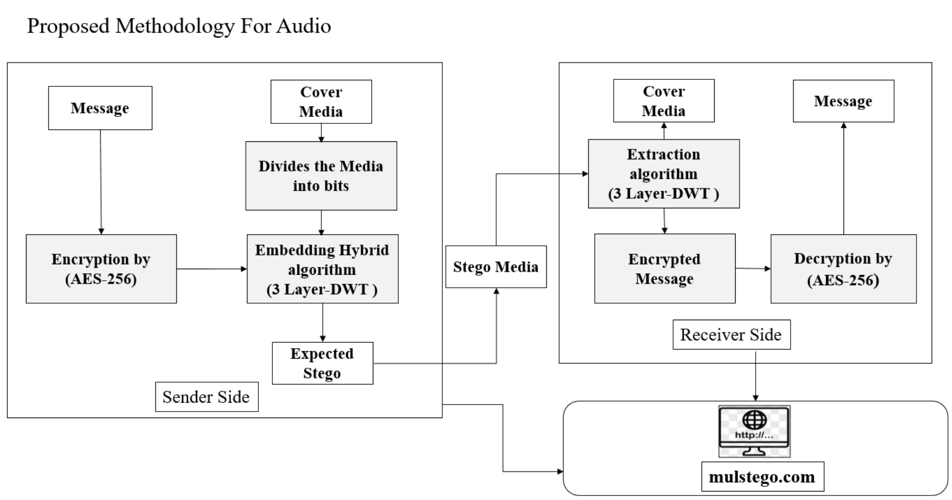

Fig. 4. Audio Steganography

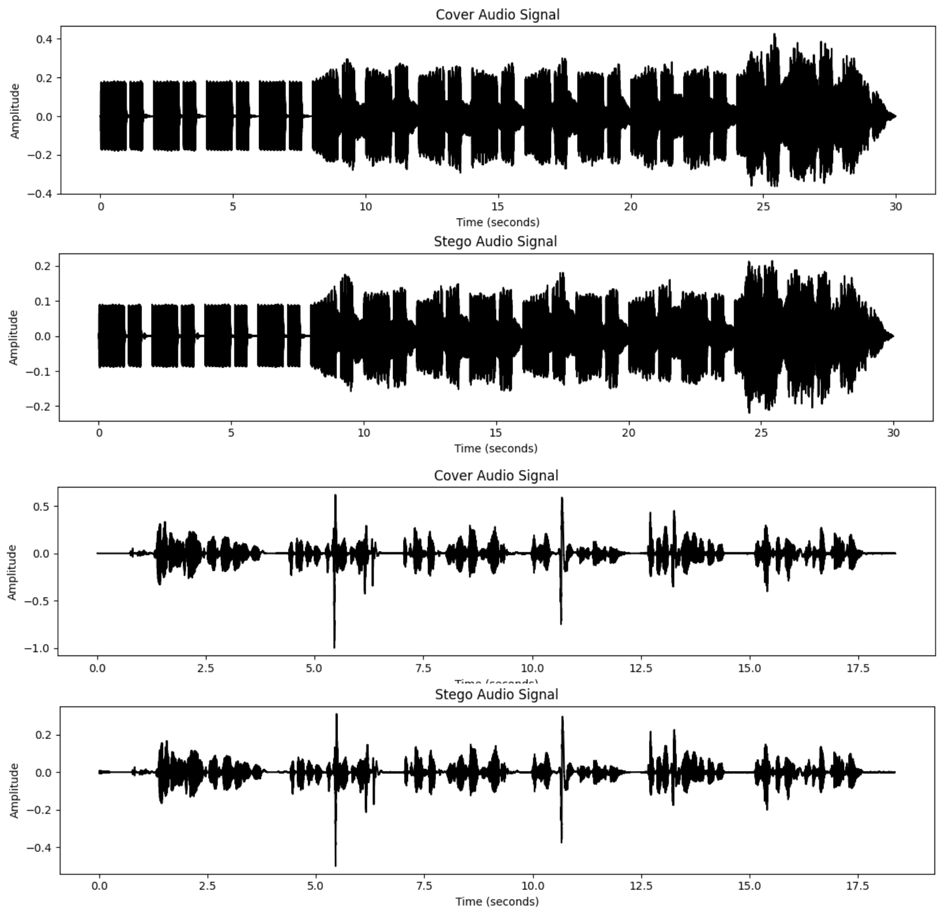

Fig. 5. Cover and Stego Audio Files

High PSNR values indicate nearly identical stego audio, with imperceptible distortion, increasing resistance to detection (see Table VI).

- **Signal-to-Noise Ratio (SNR)**:SNR measures signal power against added noise, with high values indicating intact audio clarity and reduced detection (see Table V). Audio 2's negative SNR (-0.0 dB) stems from its speech nature, featuring soft parts and pauses with low signal power, making it sensitive to embedding noise.In contrast, Audio 1's ringtone, with high uniform signal power, retains a positive SNR (0.24 dB).Table V includes a footnote with verified `numpy` calculations to clarify this behavior.
- **Perceptual Assessment of Speech Quality (PESQ)**: PESQ evaluates the perceptual quality of stego audio by simulating human hearing. Higher scores indicate fidelity to the original, reducing suspicion of hidden data (see Table VII for results comparing cover and stego audio).

B. Results

- LSB image steganography achieved high PSNR and SSIM, indicating minimal distortion and low detection.
- DWT audio steganography outperformed traditional time-domain methods in robustness against compression and format shifts.
- Low MSE values for both image and audio confirmed negligible media change after embedding.
- AES-256 encryption ensured that the extracted data remained secure, undetectable without the key.
- Resistance tests showed strong defense against detection devices and statistical analysis, which is ideal for secret communications.

These results highlight the proposed AES-256 integrated LSB and DWT steganography as a secure, undetectable solution for data embedding in cybersecurity.

V. Conclusion

This study introduces a robust multimedia steganography framework combining LSB image steganography, DWT audio steganography, and AES-256 encryption. It ensures confidentiality, attack resistance, and data indecipherability while achieving high values of PSNR, SSIM, and SNR. These results confirm the effective hiding of sensitive data with minimal impact on media quality, which is reinforced by AES-256 protection against unauthorized access.

Future efforts will extend this methodology to video steganography, preserving audiovisual integrity by embedding protected data in motion frames. Furthermore, quan-

TABLE I
MSE COMPARISON FOR IMAGE STEGANOGRAPHY

Figure Name	Cover Image MSE	Stego Image MSE
Image 1	112.4106	0.0003
Image 2	105.2737	30.1436

TABLE II
PSNR COMPARISON FOR IMAGE STEGANOGRAPHY

Figure Name	Cover PSNR	Stego PSNR
Image 1	∞	83.2172
Image 2	∞	33.3389

TABLE III
SSIM COMPARISON FOR IMAGE STEGANOGRAPHY

Figure Name	Cover Image SSIM	Stego Image SSIM
Image 1	1.0000	1.0000
Image 2	1.0000	0.9815

TABLE IV
MSE COMPARISON FOR AUDIO STEGANOGRAPHY

Audio Name	Cover Audio MSE	Stego Audio MSE
Audio 1	0.0077	0.0021
Audio 2	0.0031	0.0007

TABLE V
SNR COMPARISON FOR AUDIO STEGANOGRAPHY

Audio Name	Cover SNR	Stego SNR
Audio 1	5.84	0.24
Audio 2	6.02	-0.0

TABLE VI
PSNR COMPARISON FOR AUDIO STEGANOGRAPHY

Audio Name	Cover Audio PSNR	Stego Audio PSNR
Audio 1	19.52	13.55
Audio 2	26.9	20.87

TABLE VII
PESQ COMPARISON FOR AUDIO STEGANOGRAPHY

Audio Name	Cover Audio PESQ	Stego Audio PESQ
Audio 1	4.6438	3.4008
Audio 2	4.6438	4.6383

tum steganography will be explored, incorporating quantum cryptography to combat emerging quantum computing threats. These developments aim to strengthen data security, resilience, and real-time performance for post-quantum secure communication systems.

REFERENCES

[1] A. Alabaichi, M. A. A. K. Al-Dabbas, and A. Salih, "Image steganography using least significant bit and secret map techniques," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 1, pp. 935–946, Feb. 2020. doi: 10.11591/ijece.v10i1.pp935-946.

[2] C. A. Sari, M. H. Dzaki, E. H. Rachmawanto, R. R. Ali, and M. Doheir, "High PSNR Using Fibonacci Sequences in Classical Cryptography and Steganography Using LSB," *International Journal of Intelligent Engineering and Systems*, vol. 16, no. 4, pp. 568-578, 2023. doi: 10.22266/ijies2023.0831.46.

[3] S. A. Jebur, A. K. Nawar, L. E. Kadhim, and M. M. Jahefer, "Hiding Information in Digital Images Using LSB Steganography Technique," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 17, no. 07, 2023. doi: 10.3991/ijim.v17i07.38737.

[4] F. S. Mohamad and N. S. M. Yasin, "Information Hiding Based on Audio Steganography using Least Significant Bit," *International Journal of Engineering and Technology*, vol. 7, no. 4.15, pp. 536-538, 2018.

[5] M. H. Sayed and T. M. Wahbi, "Information Security for Audio Steganography Using a Phase Coding Method," *European Journal of Theoretical and Applied Sciences*, vol. 2, no. 1, pp. 634-647, 2024. doi: 10.59324/ejtas.2024.2(1).55.

[6] T. Ahmad, M. H. Amrizal, W. Wibisono, and R. M. Ijtihadie, "Hiding data in audio files: A smoothing-based approach to improve the quality of the stego audio," *Heliyon*, vol. 6, no. 3, e03464, Mar. 2020. doi: 10.1016/j.heliyon.2020.e03464.

[7] OpenGameArt, "Landscape," *OpenGameArt.org*, [Online]. Available: https://opengameart.org/content/landscape. [Accessed: Apr 2, 2025].

[8] The Red Panda Swag, "Cute Red Panda Wallpaper 2," *theredpandaswag.wordpress.com*, [Online]. Available: https://theredpandaswag.wordpress.com/cute-red-panda-wallpaper-2/. [Accessed: Apr 2, 2025].

[9] File Examples, "Sample WAV Download," *file-examples.com*, [Online]. Available: https://file-examples.com/index.php/sample-audio-files/sample-wav-download/. [Accessed: Apr 5, 2025].

[10] C. Chirita, "Sample WAV Audio Files," *Kaggle.com*, [Online]. Available: https://www.kaggle.com/datasets/crischir/sample-wav-audio-files. [Accessed: Apr 5, 2025].

[11] N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography," *IEEE Security & Privacy*, vol. 1, no. 3, pp. 32-44, 2003.

[12] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Processing*, vol. 90, no. 3, pp. 727-752, 2010.

[13] H. Wang and S. Wang, "Cyber warfare: Steganography vs. steganalysis," *Communications of the ACM*, vol. 47, no. 10, pp. 76-82, 2004.

[14] R. Panigrahi and N. Padhy, "An effective steganographic technique for hiding the image data using the LSB technique," *Cyber Security and Applications*, vol. 3, p. 100069, 2025. doi: 10.1016/j.csa.2024.100069.

[15] S. Rahman, J. Uddin, H. Hussain, S. Shah, A. Salam, F. Amin, I. de la Torre Díez, D. L. Ramírez Vargas, and J. C. Martínez Espinosa, "A novel and efficient digital image steganography technique using least significant bit substitution," *Scientific Reports*, vol. 15, no. 107, 2025. doi: 10.1038/s41598-024-83147-3.

[16] M. Alanzy, R. Alomrani, B. Alqarni, and S. Almutairi, "Image Steganography Using LSB and Hybrid Encryption Algorithms," *Applied Sciences*, vol. 13, no. 21, p. 11771, Oct. 2023. [Online]. Available: 10.3390/app132111771.

[17] O. Veselska, O. Lavrynenko, R. Odarchenko, M. Zaliskyi, D. Bakhtiiarov, M. Karpinski, and S. Rajba, "A Wavelet-Based Steganographic Method for Text Hiding in an Audio Signal," *Sensors*, vol. 22, no. 15, p. 5832, 2022. doi: 10.3390/s22155832.