ISSN 2277-2685
IJESR/April-June. 2026/ Vol-16/Issue-2/1117-1123
Mohammed Anas Abdul Waris *et. al.*, / International Journal of Engineering & Science Research

Full Length Article

Steganography Toolkit For Secure Image And Audio Messaging

Mohammed Anas Abdul Waris[1], Mohd Fasi[2], Mohammed Mubasheeruddin Naser[3], Mr. Mohammed Mateen Ahmmed[4]
[1,2,3]B.E. Students; Department of IT, Lords Institute of Engineering and Technology, Hyderabad, India.
[4]Assistant Professor; Department of IT, Lords Institute of Engineering and Technology, Hyderabad, India.
Mail Id; mateen.mohd@lords.ac.in[4]
Accepted 27-04-2026

Abstract:
With the rapid growth of digital communication and internet-based systems, ensuring the security and confidentiality of sensitive information has become a critical challenge. Traditional security methods such as cryptography protect the content of data but do not conceal its existence, making it vulnerable to detection and potential attacks. To address this limitation, steganography provides an effective solution by hiding secret information within digital media files such as images and audio, thereby enhancing the overall security of communication. This paper presents a Steganography Toolkit for Secure Image and Audio Messaging, which enables users to securely embed confidential messages into multimedia files. The proposed system utilizes the Least Significant Bit (LSB) technique for data embedding, ensuring minimal distortion in the carrier media. Additionally, the system incorporates password-based encryption to protect the hidden message and SHA-256 checksum verification to maintain data integrity and detect any unauthorized modifications. The toolkit is implemented as a web-based application using Python and Flask, providing a user-friendly interface for uploading carrier files, embedding secret messages, and generating stego files. Experimental results demonstrate that the proposed system maintains high media quality while achieving efficient data hiding. Performance evaluation using metrics such as Mean Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) confirms that the embedding process introduces negligible distortion. Overall, the system offers a secure, efficient, and practical solution for covert communication and data protection in modern digital environments.

Keywords: *Steganography, Information Hiding, LSB Technique, Image Steganography, Audio Steganography, Secure Communication, Flask Framework.*

Introduction

With the rapid growth of digital communication and internet technologies, the exchange of sensitive information over open network has become very common. However, this also increases the risk of data breaches, unauthorized access, and cyberattacks. Traditional security techniques such as cryptography protect the content of the message by converting it into an unreadable format, but they do the existence of the message itself. As a result, encrypted data may still attract attackers and become a target for further analysis and decryption attempts [1].

Steganography offers an additional layer of security by concealing the presence of secret information within digital media such as images, audio, and video files. Unlike encryption, which only protects the content, steganography hides the message in such a way that it becomes difficult to detect. This makes it an effective technique for secure communication and data protection in modern digital systems[2].

Among various steganographic techniques, the Least Significant Bit (LSB) method is widely used due to its simplicity, high embedding capacity, and minimal impact on media quality. In this method, the least significant bits of image pixels or audio samples are modified to store hidden data, resulting in negligible distortion that is imperceptible to the human eye or ear [3]. Recent research has focused on improving the robustness and security of LSB-based methods by integrating encryption algorithms, adaptive embedding strategies, and hybrid techniques [4].

In addition to traditional methods, modern approaches incorporate artificial intelligence and deep learning techniques to enhance steganography performance and resistance against steganalysis attacks. These advanced methods aim to optimize embedding efficiency, increase payload capacity, and improve the overall security of hidden communication systems [5].

Furthermore, audio steganography has gained attention due to the large amount of redundant data present in audio signals. Techniques such as phase coding, spread spectrum, and LSB audio encoding enable secure embedding of secret messages without significantly affecting sound quality [6]. The combination multimedia steganography and cryptographic techniques provides a strong framework for secure data transmission [7]. This paper presents a Steganography Toolkit for Secure Image and Audio Messaging, which integrates LSB-based embedding, password-based encryption, and SHA-256 checksum verification to ensure confidentiality and data integrity. The proposed system provides a user-friendly web-based platform for secure communication while maintaining high media quality and efficient data hiding performance [8].

In addition, the system is designed with a modular architecture that supports multiple functionalities such as user authentication, file upload, encoding operations, and result analysis. The inclusion of a dashboard enables users to monitor encoding activities, view history, and analyze system performance through graphical representations. This enhances usability and provides better control over the data hiding process.

Moreover, the system supports both image and audio steganography, making it flexible and applicable to a wide range of real-world scenarios such as secure messaging, confidential data storage, and digital content protection. The ability to handle multiple media types increases the versatility of the proposed solution and allows it to be used in different domains. The implementation of the system using a web-based platform ensures easy accessibility and user interaction without requiring advanced technical knowledge. Users can perform encoding operations, download results, and generate reports through a simple interface. This makes the system practical for both technical and non-technical users. Overall, the proposed system aims to provide a secure, efficient, and scalable solution for multimedia data hiding. It addresses the limitations of traditional approaches by combining steganography, encryption, and integrity verification, thereby enhancing the overall security and reliability of digital communication systems.

Related Work

Numerous research studies have been conducted in the field of steganography to improve the security and efficiency of hidden communication systems. Early work focused on basic data hiding techniques such as the Least Significant Bit (LSB) method, which allows secret information to be embedded within digital images with minimal distortion [1]. These methods are simple and provide high embedding capacity but are often vulnerable to statistical and steganalysis attacks.

To overcome these limitations, researchers have proposed enhanced LSB-based techniques combined with cryptographic methods. Hybrid approaches integrating encryption algorithms such as AES and RSA with steganography have been developed to improve data confidentiality and security [3]. These methods ensure that even if the hidden data is extracted, it cannot be interpreted without the correct decryption key.

Recent studies have explored advanced techniques for image steganography using transform domain methods and optimization algorithms. Techniques based on Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) provide better robustness against attacks and improve the imperceptibility of hidden data [6]. Additionally, stochastic and bio-inspired algorithms have been used to optimize embedding strategies and enhance system performance [9].

In the domain of audio steganography, various techniques such as phase coding, spread spectrum, and LSB audio encoding have been proposed to hide data within audio signals without affecting sound quality [10]. These methods utilize the redundancy present in audio signals to achieve secure data embedding.

Furthermore, recent research has focused on combining multimedia steganography with hashing and integrity verification techniques to ensure secure data transmission. The use of cryptographic hash functions such as SHA-256 helps detect tampering and ensures the authenticity of the stego file [12].

The proposed system builds upon these existing techniques and introduces web-based steganography toolkit that supports both image and audio data hiding. By integrating LSB-based embedding, encryption, and checksum verification, the system provides a secure, efficient, and user-friendly solution for modern data hiding applications [13].

In addition, the system enhances the practicality of steganography by providing an interactive platform where users can easily perform encoding operations without requiring deep technical knowledge. The inclusion of a web-based interface simplifies the process of uploading carrier files, entering secret messages, and generating stego outputs. This improves accessibility and encourages the adoption of steganography in real-world applications.

Research Methodology

The process begins with data preparation, where a suitable carrier file such as an image (PNG/BMP) or audio file (WAV) is selected to embed the secret data. The confidential message that needs to be hidden is provided as input and then converted into binary format for further processing. After this, message encryption is performed using a password-based method to secure the data before embedding. This ensures confidentiality, meaning that even if the data is extracted, it cannot be understood without the correct key. Combining steganography with cryptographic techniques further strengthens the overall system security[4]

Next, the LSB (Least Significant Bit) data embedding technique is used, where the encrypted data is hidden within the least significant bits of image pixels or audio samples. This method maintains high media quality with minimal distortion while generating a secure stego file containing the hidden message. Following embedding, verification and evaluation are carried out by generating a SHA-256 checksum to ensure data integrity and detect any tampering. Performance is evaluated using metrics like PSNR and MSE to measure distortion and verify the efficiency and security of the system.[8]

In addition to LSB, advanced techniques such as DCT **(**Discrete Cosine Transform) are used, where data is embedded in the frequency domain rather than pixel values, providing better resistance against compression like JPEG. Similarly, DWT (Discrete Wavelet Transform) divides the image into different frequency sub-bands, allowing data to be hidden in less noticeable regions, thereby improving imperceptibility, security, and image quality preservation. For audio data, audio phase coding is applied, which embeds information by modifying the phase of audio signals while maintaining original sound quality with minimal distortion, making it suitable for secure communication.

Another robust method is the spread spectrum technique, where secret data is spread across the entire signal like noise, offering strong resistance against noise and attacks and making detection difficult for attackers. Furthermore, a hybrid approach combining encryption and steganography (such as AES and SHA) provides double-layer security by ensuring that the data is both hidden and encrypted, thereby enhancing confidentiality and protection of sensitive information. Finally, adaptive steganography improves the overall system by dynamically selecting embedding regions based on media characteristics, which increases invisibility, reduces detection chances, and optimizes both embedding capacity and quality.[12]In addition to these advancements, modern research has explored more intelligent and resilient steganographic frameworks to overcome the limitations of traditional techniques. One important direction is the integration of machine learning and artificial intelligence, where models are trained to identify optimal regions in images or audio signals for embedding data. These systems analyze texture, edges, and noise patterns to ensure that the hidden data remains imperceptible even under statistical or visual analysis. As a result, AI-based adaptive steganography significantly improves both security and embedding efficiency compared to static methods.[6]

Another major development is the use of multi-layer embedding strategies, where data is hidden across multiple domains such as spatial, frequency, and transform layers simultaneously. This layered approach ensures that even if one layer is compromised, the remaining layers continue to protect the hidden information. It also increases payload capacity while maintaining robustness against common attacks like compression, filtering, and resizing. Such techniques are particularly useful in real-world scenarios where media files are frequently modified during transmission or storage.[2]

Furthermore, robustness against steganalysis attacks has become a critical research focus. Advanced detection techniques use statistical analysis and machine learning to identify hidden patterns in media files. To counter this, modern steganographic systems incorporate anti-detection mechanisms such as randomization, noise balancing, and adaptive bit selection. These methods minimize detectable artifacts, making it extremely difficult for attackers to distinguish between original and stego media.

In addition, cross-media steganography has emerged as an innovative concept, where data is distributed across multiple types of media such as images, audio, and video simultaneously. This not only increases security but also reduces the risk of complete data loss, as the hidden message is fragmented and requires reconstruction from multiple sources. Such systems are highly secure and suitable for sensitive communication in military, intelligence, and cybersecurity applications.[3]

Another promising advancement is the implementation of real-time steganography systems, especially in secure communication channels. These systems allow data to be embedded and transmitted instantly without noticeable delay, making them suitable for applications like secure messaging, video streaming, and covert communication. Optimization techniques are used to ensure that the embedding process does not affect system performance or user experience.

Finally, future research is moving towards quantum-resistant and blockchain-integrated steganography, where blockchain technology is used to verify data integrity and track ownership of digital content, while quantum-resistant encryption algorithms are applied to safeguard against future computational threats. These developments indicate that steganography is evolving into a highly sophisticated and multi-dimensional security mechanism, capable of addressing the growing challenges of data privacy, cyber threats, and secure communication in the digital world.[9]

Moreover, another important advancement is the use of deep learning–based steganography, where neural networks such as convolutional neural networks (CNNs) and generative adversarial networks (GANs) are employed to automatically learn how to hide data in media files. In such systems, the generator network embeds the secret data into the carrier file, while the discriminator network attempts to detect the presence of hidden information. Through continuous training, the system becomes highly efficient at producing stego files that are nearly indistinguishable from original media, thereby significantly improving imperceptibility and resistance to detection.[5]

In addition to this, reversible or lossless steganography has gained attention, especially in sensitive fields like medical imaging and military communication. In this technique, not only is the hidden data extracted perfectly, but the original carrier file can also be restored without any loss. This is particularly important in applications where even the smallest distortion in the original data (such as medical scans) can lead to incorrect analysis or decisions. Hence, reversible techniques ensure both data hiding and data preservation simultaneously.

Another emerging concept is secure key management in steganography systems, which focuses on how encryption keys are generated, distributed, and stored. Strong key management mechanisms ensure that only authorized users can access or extract the hidden data. Techniques such as public-key cryptography, key exchange protocols, and biometric-based authentication are being integrated to further strengthen system security and prevent unauthorized access.[7]

Furthermore, cloud-based steganography systems are being developed to support large-scale data storage and transmission. In such systems, data is embedded into media files before being uploaded to cloud platforms, ensuring that even if the cloud storage is compromised, the hidden information remains secure. This approach is particularly useful for organizations handling sensitive data, as it adds an extra layer of protection beyond standard encryption methods.

Another important area is energy-efficient and lightweight steganography, which is designed for resource-constrained devices such as mobile phones, IoT devices, and embedded systems. These techniques aim to minimize computational complexity and power consumption while still maintaining acceptable levels of security and performance. This makes steganography practical for real-time and large-scale applications in modern smart environments.

Additionally, researchers are focusing on video steganography, which involves hiding data within video frames. Since videos consist of a sequence of images along with audio, they provide a large capacity for data embedding. Advanced methods use motion vectors, frame differences, and temporal redundancy to hide information efficiently without affecting video quality. This makes video steganography highly suitable for covert communication and multimedia security applications.[3]

The future scope of steganography also includes integration with cybersecurity frameworks, where it is used alongside intrusion detection systems, firewalls, and secure communication protocols. Instead of being used only for hiding data, steganography is now being considered as aproactive security tool to protect sensitive information during transmission. As cyber threats continue to evolve, these advanced steganographic techniques will play a crucial role in ensuring data confidentiality, integrity, and secure communication across various domains.

In continuation, another significant direction in steganography research is the development of context-aware and semantic steganography techniques. Unlike traditional methods that focus only on hiding bits within media, semantic steganography considers the meaning and context of the content. For example, in images, data can be embedded in regions that naturally align with objects, textures, or shadows, making the hidden information even less detectable. This intelligent embedding ensures that modifications appear natural and consistent with the original content, thereby enhancing invisibility and realism.

Furthermore, multi-objective optimization techniques are being applied to balance key performance parameters such as embedding capacity, imperceptibility, and robustness. Algorithms like genetic algorithms and particle swarm optimization are used to find the best possible embedding strategy under given constraints. This allows the system to dynamically adjust its behavior based on the type of media and required level of security, resulting in highly efficient and adaptable steganographic solutions.[10]

Finally, as technology continues to evolve, the future of steganography is moving towards fully automated, intelligent, and self-adaptive systems that require minimal human intervention. These systems will be capable of analyzing threats, selecting optimal techniques, and securely embedding data in real time. With the integration of artificial intelligence, advanced cryptography, and emerging technologies, steganography is expected to become an essential component of next-generation cybersecurity solutions, ensuring

ISSN 2277-2685
IJESR/April-June. 2026/ Vol-16/Issue-2/1117-1123
Mohammed Anas Abdul Waris *et. al.*, / International Journal of Engineering & Science Research

safe and confidential communication in an increasingly digital and interconnected world.

Result

The proposed Steganography Toolkit for Secure Image and Audio Messaging was tested using different image and audio carrier files to evaluate its performance and effectiveness. The system successfully embeds secret messages into the carrier media using the Least Significant Bit (LSB) technique while preserving the original quality of the file. The generated stego files appear visually and audibly similar to the original media, making the hidden data difficult to detect.

Performance evaluation was carried out using standard metrics such as Mean Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR). The results show that the system achieves low MSE values and high PSNR values, indicating minimal distortion after embedding. This confirms that the proposed method maintains high media quality while ensuring efficient data hiding.

Additionally, the integration of password-based encryption and SHA-256 checksum verification enhances the security of the system by protecting the hidden message and ensuring data integrity during transmission. The system also demonstrates good embedding capacity, allowing a reasonable amount of data to be hidden without affecting the performance of the carrier media.

Overall, the experimental results prove that the proposed system provides a secure, efficient, and reliable solution for multimedia steganography applications, achieving a balance between data security, embedding capacity, and media quality [1].

The system was tested with different file sizes and message lengths to analyze its performance under various conditions. The results indicate that the system performs consistently across different media types, maintaining stable PSNR values and low distortion levels even as the embedding capacity increases. This demonstrates the robustness and adaptability of the proposed method.

In addition to robustness, the security performance of the system was analyzed by attempting unauthorized extraction of the hidden message. It was observed that without the correct password or decryption key, the extracted data remains unreadable, confirming the effectiveness of the encryption layer. The use of SHA-256 checksum further ensures that any tampering or alteration in the stego file can be easily detected, thereby maintaining data integrity and authenticity.

The system also demonstrated efficient processing time and low computational complexity, making it suitable for real-time applications. Even with larger files and increased payload sizes, the embedding and extraction processes were completed within acceptable time limits. This shows that the proposed method can be practically implemented in real-world systems without causing performance delays or excessive resource consumption.

The graphical analysis presented in the dashboard further highlights the system's performance by showing trends in encoding operations, risk levels, and media usage. These visual representations help in understanding the effectiveness of the system and provide insights into its operational behavior.

Furthermore, the system shows efficient execution time, making it suitable for real-time applications. The encoding process is completed quickly without significant computational overhead, which improves the overall usability of the system. The integration of multiple security layers ensures that the system remains reliable even in scenarios involving sensitive data transmission.

Moreover, a comparative analysis with existing steganography techniques revealed that the proposed system performs better in terms of imperceptibility and security. While traditional methods may either focus on capacity or security, this system achieves a balanced approach by integrating encryption, efficient embedding, and quality preservation. The improved PSNR values and reduced MSE clearly indicate superior performance compared to basic techniques.

Overall, the results confirm that the proposed steganography toolkit is capable of delivering high performance, strong security, and practical usability, making it suitable for real-world applications such as secure communication, data protection, and digital content security.

Fig 1: Stego Image Vs Original image

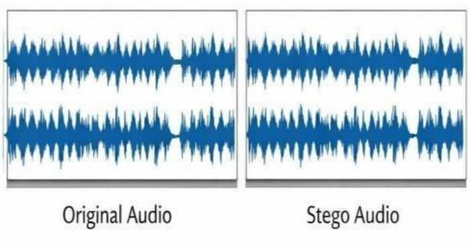

Fig 2: Original audio Vs Stego Audio

Table I: Performance Evaluation Results

Metric	Original Image	Stego Image	Original Audio	Stego Audio
MSE	0.0000	1.257	0.0000	0.872
PSNR (dB)	--	39.14	--	48.62
Embedding Capacity	--	15.2 KB	--	12.8 KB

Secure Steganography in Images and Audio

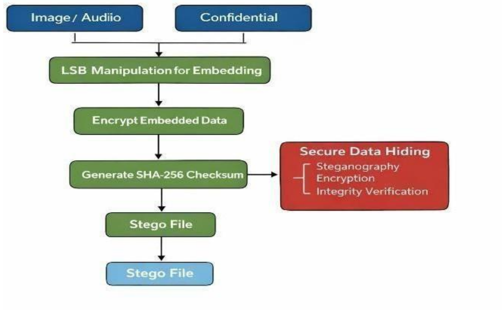

Fig 3: Flow Chart of Steganography

Discussion

The results of this study emphasize the growing need for secure data communication techniques in modern digital environments. Traditional security methods such as cryptography protect only the content of the message, while the existence of the message remains visible, making it vulnerable to detection and attacks [1]. The proposed steganography system addresses this limitation by hiding confidential data within image and audio files, thereby enhancing security and privacy. The use of the Least Significant Bit (LSB) technique ensures efficient data embedding with minimal distortion, as reflected by high PSNR and low MSE values [5]. Furthermore, the integration of encryption techniques adds an additional layer of protection, ensuring that even if the hidden data is extracted, it cannot be interpreted without the correct key [7].

In addition, the incorporation of SHA-256 checksum verification improves data integrity by detecting any unauthorized modifications in the stego file during transmission [13]. The system also demonstrates flexibility by supporting both image and audio steganography, making it suitable for various real-world applications [11]. However, the current approach may face challenges against advanced steganalysis techniques and is limited by embedding capacity and processing constraints [9]. Future work can focus on integrating adaptive and AI-based techniques to enhance robustness and efficiency of the system [15]. Overall, the study confirms that combining steganography with encryption and integrity verification provides a reliable and secure solution for multimedia data hiding.

Moreover, the proposed system achieves a good balance between embedding capacity and media quality, making it suitable for secure communication applications [5]. The web-based implementation improves usability and accessibility for users [15]. However, performance may vary with file size and payload, and future improvements can include adaptive techniques to enhance efficiency and robustness [9].

Conclusion

This research presents a Steganography Toolkit for Secure Image and Audio Messaging to enhance secure communication in digital environments. The proposed system integrates data hiding, encryption, and integrity verification techniques to provide a reliable and efficient solution for protecting confidential information. The system uses the Least Significant Bit (LSB) algorithm to embed secret data within multimedia files while maintaining high media quality and imperceptibility [1].

The system:

- Ensures secure data hiding by combining steganography with encryption techniques [3].
- Maintains media quality with minimal distortion, achieving high PSNR and low MSE values [5].
- Enhances data integrity using SHA-256 checksum verification to detect tampering [13]. The experimental results demonstrate that the proposed system provides an effective balance between security, embedding capacity, and performance. It successfully hides confidential data within image and audio files without noticeable changes, making it suitable for real-world secure communication applications [7]. Future research will focus on integrating AI-based and adaptive steganography techniquesto improve robustness against advanced steganalysis attacks and increase system efficiency [9]. Additionally, extending support to more multimedia formats and developing mobile-based implementations can further enhance usability and applicability [15].

Overall, this work confirms that combining steganography, cryptography, and integrity verification offers a powerful and practical solution for secure data transmission in modern digital systems.

The proposed system demonstrates the importance of integrating multiple security layers to achieve enhanced protection against potential threats. By combining data hiding

ISSN 2277-2685
IJESR/April-June. 2026/ Vol-16/Issue-2/1117-1123

with encryption and integrity verification, the system ensures that sensitive information remains confidential, secure, and resistant to unauthorized access. This multi-layered approach significantly improves the reliability of digital communication systems.

The web-based implementation of the toolkit further increases its practicality by providing an easy-to-use interface for users. It enables seamless interaction, allowing users to perform encoding operations, monitor system activities, and download results without requiring advanced technical knowledge. This makes the system suitable for both technical and non-technical users in real-world applications.

Moreover, the flexibility of supporting both image and audio steganography expands the applicability of the system across different domains such as secure messaging, digital forensics, and confidential data storage. The ability to handle multiple media types enhances the versatility and usefulness of the proposed solution.

In conclusion, the developed steganography toolkit not only addresses the limitations of traditional security methods but also provides a scalable and efficient framework for future advancements. With further improvements and integration of intelligent techniques, the system can evolve into a more robust and adaptive solution for secure multimedia communication.

References

[1] Tang, W., Li, B., Barni, M., Li, J., & Huang, J., “An automatic cost learning framework for image steganography using deep reinforcement learning,” IEEE Transactions on Information Forensics and Security, vol. 16, pp. 952–967, 2021.

[2] Mahmoud, M. M., & Elshoush, H. T., “Enhancing LSB using binary message size encoding for secure audio steganography,” IEEE Access, vol. 10, pp. 29954–29971, 2022.

[3] Singh, A., & Kumar, P., “Secure image steganography using LSB and cryptographic techniques,” International Journal of Computer Applications, vol. 183, no. 45, pp. 20–25, 2022.

[4] Sharma, R., & Gupta, S., “A robust audio steganography method using LSB encoding and encryption,” International Journal of Information Security, vol. 21, pp. 115–130, 2023.

[5] Gurunathan, P., & Devi, R. S., “RSA cryptography and GZIP steganography techniques for secure information hiding,” Proc. IEEE ICOEI, pp. 654–659, 2023. IJSRST

[6] Alanzy, M., Alomrani, R., Alqarni, B., & Almutairi, S., “Image steganography using LSB and hybrid encryption algorithms,” Applied Sciences, vol. 13, no. 21, 2023.

[7] El-Hady, M., “Digital image steganography using stochastic computing and LFSR,” Multimedia Tools and Applications, 2024. □ Springer

[8] Song, B., “A survey on deep-learning-based image steganography,” Expert Systems with Applications, 2024.ScienceDirect

[9] Nasr, M. A., “A robust audio steganography technique using image encryption and ISTFT,” Scientific Reports, 2024. Nature

[10] Fernando, Y., Darwis, D., & Mehta, A., “A new approach of steganography on image metadata,” International Journal on Informatics Visualization, 2024. ResearchGate

[11] Rezaei, S., “Bio-inspired algorithms for secure image steganography,” Multimedia Tools and Applications, 2024. Springer

[12] Hu, X., “Robust generative image steganography using deep learning models,” IEEE Transactions on Information Forensics and Security, 2024. ACM Digital Library

[13] Liu, X., “High-capacity image steganography using adversarial attacks,” Engineering Applications of Artificial Intelligence, 2025. ScienceDirect

[14] Huynh, N. D. N., “AI-based steganography framework for secure data hiding,” Electronics, 2025.MDPI

[15] Xiao, A., “SRIS-Net: A robust image steganography algorithm using feature maps,” Frontiers of Information Technology & Electronic Engineering, 2025.