Enhanced Image-Based Security: Integrating Cryptography and Steganography for Robust Data Protection

Dr. D. Vijaya Lakshmi[1], Baireddy Sai chandhan[2], Shriya Kalvakunta[3]
[1]*Professor & HOD, Mahatma Gandhi Institute of Technology*
[2,3]*UG Student, Mahatma Gandhi Institute of Technology*

Abstract: The increasing prevalence of digital communication has introduced significant security concerns, particularly regarding the confidentiality and integrity of sensitive data during transmission. Traditional encryption methods effectively ensure the confidentiality of messages but fall short in verifying data integrity and detecting tampering during transmission. Similarly, steganography techniques, while capable of concealing data within images, often do not offer adequate protection against tampering or unauthorized alterations. The challenge lies in developing a secure communication framework that not only protects the content of messages but also provides a reliable means of detecting any tampering or unauthorized modifications during the transmission process. To address these issues, we propose to develop a robust secure communication framework that integrates AES encryption, image-based LSB steganography, and fragile watermarking. This framework will ensure that the encrypted message is concealed within an image, maintaining its confidentiality while making it undetectable to unauthorized users. Simultaneously, the fragile watermark will serve as a tamper detection mechanism, allowing for the verification of the image's integrity. This multi-layered approach will address both confidentiality and integrity concerns, providing a comprehensive solution for secure data transmission. The proposed communication framework will offer an advanced method for ensuring the secure exchange of sensitive information, safeguarding against both unauthorized access and tampering.

keywords: Cryptography, Steganography, Watermarking, AES Encryption, Cipher Block Chaining, Least Significant Bit (LSB) Steganography, Fragile Watermarking, Tamper Detection, Confidentiality, Integrity Verification, Secure Communication, Image-Based Security, Stego Image

1. INTRODUCTION

The rise of digital communication has brought advanced methods of data exchange but also increased cyber threats like data breaches and tampering. Traditional security measures, such as encryption and steganography, safeguard confidentiality but often overlook data integrity and authenticity. This project addresses these gaps by combining AES encryption for confidentiality, image-based steganography for concealment, and dynamic fragile watermarking for tamper detection. This integrated approach ensures sensitive data remains hidden, secure, and protected from unauthorized alterations, enhancing communication security against evolving cyber threats.

The objective of this project is to develop a secure and robust communication system that integrates multiple layers of security to ensure both confidentiality and integrity during data transmission. The system combines Advanced Encryption Standard (AES) encryption for protecting the content of messages, Least Significant Bit (LSB) image steganography for hiding the encrypted message within an image, and

dynamic fragile watermarking to provide a means of detecting tampering or unauthorized alterations. AES encryption ensures that the data remains confidential, making it unreadable to anyone without the decryption key. The LSB technique embeds the encrypted data into an image, making it less detectable while leveraging the cover image's innocuous appearance to hide sensitive information. The dynamic fragile watermark embedded within the stego image adds a layer of protection by making any tampering with the image detectable. This watermark is designed to break or distort if any modification occurs, alerting the receiver to potential data corruption. By combining these methods, the project aims to provide a comprehensive communication system that addresses the limitations of traditional security methods, offering a high level of protection for transmitted data. The ultimate goal is to ensure that the messages not only remain confidential but also retain their integrity and authenticity, with a robust mechanism in place to verify their authenticity during transmission and reception.

2. EXISTING SYSTEM

The Synthesis-Mapping Hybrid Steganography Without Embedding (SMH-SWE) system is designed to conceal secret messages within images without directly modifying the container images. This is achieved through a two-stage framework involving an image synthesis module and an image mapping module. Adversarial networks are used to synthesize images and hide secret messages in their latent space. An auto-encoder (AE) is trained to disentangle the image structural and texture features. Then, the principal part of the secret message is hidden into the synthesized image by swapping the structural features. The key weakness of the synthesis based technique is that the secret message can hardly be recovered completely at the receiver side even without an attack. There is a chance of extraction error in the synthesis module. To ensure complete recovery of the secret message, the residual message parts are embedded into selected container images using statistical hash matching. The residual message part, which contains the extraction errors, is converted into a statistical hash representation. Candidate container images are selected from a database based on the similarity between their block statistical hashes and the hash of the compressed residual message. The residuals are then mapped to the chosen container images.

3. LITERATURE SURVEY

In this paper Rong Huang, Chunyan Lian, Zhen Dai, Zhaoying Li, and Ziping Ma propose SMH-SWE, a two-stage hybrid framework for steganography without embedding, eliminating pixel modifications and making it immune to traditional steganalysis tools. The framework includes an image synthesis module, using a disentanglement auto-encoder to encode secret messages into structural features of synthesized images, and an image mapping module, compressing extraction errors as residuals matched to container images. This reduces the number of container images needed while ensuring full message recovery. However, SMH-SWE has limitations, including lower hidden capacity and vulnerability to compression, blurring, and sterilization attacks due to high-frequency component encoding. Future improvements involve advanced hiding techniques and adversarial learning to enhance robustness and capacity. [1]

In this paper, Shahid Rahman, Jamal Uddin, Habib Ullah Khan, Hameed Hussain, Ayaz Ali Khan, and Muhammad Zakarya (2022) propose an enhanced Least Significant Bit (LSB) substitution method for embedding secret messages in digital images. The technique introduces a Magic Matrix and a Modified Least Embedding Algorithm (MLEA) to improve the security, embedding capacity, and robustness of the steganographic process, while ensuring that the stego-image remains visually indistinguishable from the original image.

The authors highlight the strengths of their method, including enhanced data concealment and increased resilience against unauthorized access. However, they also acknowledge several limitations. The proposed method remains vulnerable to steganalysis attacks and its embedding capacity is constrained by the size and colour depth of the cover image. Additionally, the computational complexity of the technique may increase when dealing with larger datasets, potentially impacting its efficiency. Furthermore, the method's robustness is limited when the stego-image undergoes advanced image processing techniques, such as compression or noise attacks. The authors suggest that future work could focus on enhancing the robustness of the technique and extending its applicability to address these limitations. This study provides a valuable foundation for developing improved steganographic methods by balancing security, capacity, and efficiency in digital image steganography.[2]

In this paper, Sunpreet Sharma, Ju Jia Zou, and Gu Fang propose a novel multipurpose watermarking scheme designed to address challenges in image authentication and copyright protection, particularly in industrial environments within the context of Industry 4.0. The proposed method embeds two distinct watermarks: a robust watermark for copyright protection and a fragile watermark for tamper detection and localization. The robust watermark is embedded in the frequency domain using a novel mean-based coefficient selection procedure, enhancing imperceptibility and robustness against various watermarking attacks. The fragile watermark, embedded in the spatial domain through a self-generated halftone method and based on least significant bit (LSB) substitution, is designed to improve the fragility of the watermark, making it effective for detecting and localizing tampering. However, a significant limitation of the proposed scheme is its non-reversible nature, meaning it cannot restore or recover tampered regions, which may be a drawback in applications requiring image restoration. This limitation highlights the need for further research to address scenarios where recovery of the original image is critical.[3]

In this paper Arshiya S. Ansari, Mohammad S. Mohammadi, and Mohammad Tanvir Parvez propose the Generic Steganography Algorithm (GSA) to address the limitations of existing steganography methods that work with only one image format. GSA is a flexible approach that abstracts image components, allowing compatibility across formats like JPEG, Bitmap, TIFF, and PNG. It incorporates capacity pre-estimation, adaptive partitioning, and data spreading to embed data securely while preserving image quality. The algorithm also enhances security by selecting optimal cover formats based on data size and acceptable distortions, making it adaptable to diverse use cases.

Experimental results demonstrate that GSA improves PSNR values by at least 26%, enabling higher data embedding with minimal impact on visual quality. However, the authors note the need for further evaluation of its robustness against advanced steganalysis and compression techniques. Additionally, GSA's performance with less common or heavily manipulated images remains unexplored. Future work includes refining partition schemes and testing the algorithm with a wider range of formats and complex manipulations to enhance security and versatility.[4]

In this paper Jagan Raj Jayapandiyan, C. Kavitha, and K. Sakthivel propose the enhanced LSB (eLSB) algorithm to improve the traditional Least Significant Bit method for image-based text steganography. Operating in the spatial domain, eLSB optimizes embedding to enhance cover image quality. The algorithm involves two phases: embedding header information about the secret message and processing the message itself using a character sequence-based optimization technique.

This approach improves space utilization, reduces distortion, and increases embedding capacity. The eLSB algorithm also enhances security by preprocessing the secret message before embedding. Experimental results show it outperforms the traditional LSB method, achieving higher PSNR and lower MSE and RMSE values, indicating reduced noise and distortion. Tests with various cover images and message sizes confirm consistent improvements in stego image quality, demonstrating eLSB's effectiveness.[5]

In this paper Donghui Hu, Liang Wang, Wenjie Jiang, Shuli Zheng, and Bin Li propose a novel steganography method using Deep Convolutional Generative Adversarial Networks (DCGANs) under the category of Steganography Without Embedding (SWE). Instead of modifying a carrier image, their method generates a stego image directly from a noise vector representing the secret data using a DCGAN generator. A separate extractor network retrieves the hidden information with high accuracy, enhancing security and making the stego image resistant to advanced steganalysis. Despite its advantages, the method has limitations. Some generated stego images lack naturalness, risking detection, and the steganographic capacity is restricted due to the small size of generated images. While extraction accuracy is high, it is not flawless, suggesting a need for error-correction codes to improve recovery. Future work aims to address these issues and enhance robustness and capacity.[6]

4. PROPOSED SYSTEM

The proposed system addresses critical challenges in secure communication, such as unauthorized access, message confidentiality, image tampering, and integrity verification. Existing systems often fail to provide a robust mechanism for ensuring both message security and reliable tamper detection. They primarily focus on message concealment without effectively verifying image integrity, making them vulnerable to unauthorized modifications and tampering. Additionally, traditional methods lack precise feedback on the extent of tampering, limiting their ability to identify and quantify security breaches. The proposed system overcomes these limitations by integrating AES encryption in CBC mode to ensure message confidentiality, Least Significant Bit (LSB) steganography for securely embedding encrypted messages into images, and a fragile watermarking technique to detect tampering. The fragile watermark is embedded into the image using LSB, ensuring any alterations distort the watermark, enabling tamper detection. The system incorporates secure user interactions through sender and receiver management functionalities, ensuring messages are exchanged only between authorized users. Image integrity is verified by comparing the extracted watermark with the original, providing insights into tampering by calculating the extent of modifications. By combining AES encryption for security, LSB steganography for concealment, and fragile watermarking for integrity verification, the proposed system delivers a comprehensive solution for secure message transmission, tamper detection, and integrity verification.

5. SCOPE OF THE PROJECT

The project focuses on developing a secure communication framework that combines AES encryption, LSB-based image steganography, and fragile watermarking to ensure both confidentiality and integrity in transmitted messages. The key components of this system include:

- Encryption: Implementing AES (Advanced Encryption Standard) in CBC mode to securely encrypt plaintext messages before transmission.
- Image Steganography: Using the Least Significant Bit (LSB) technique to embed the encrypted text into randomly generated images, ensuring the message is concealed within the image without significant impact on its visual quality.

- Watermarking: Embedding a fragile watermark into the same image (which already contains the encrypted text) to detect any tampering. The watermark is spread across the image using LSB manipulation.
- Tamper Detection: Verifying the integrity of the transmitted image by comparing the extracted watermark with the original stored watermark. Any discrepancy in the watermarks provides a clear indication of tampering.
- Decryption: If the watermark matches 100%, the system extracts the embedded encrypted message and decrypts it using the AES algorithm. The system is designed for scenarios where secure communication and tamper detection are critical, such as confidential messaging, document transmission, or secure data storage.

6. CONCLUSION

The proposed system successfully integrates AES encryption, LSB-based image steganography, and dynamic fragile watermarking to address the critical need for secure and tamper-evident communication. By combining these three techniques, the system ensures that sensitive data is protected from unauthorized access while also verifying its integrity. AES encryption provides robust confidentiality by converting plaintext messages into unreadable ciphertext, ensuring that only authorized parties can decrypt the data. The LSB technique embeds the encrypted message into a cover image, enabling covert communication without drawing suspicion. Furthermore, the addition of dynamic fragile watermarking enhances tamper detection, ensuring that any unauthorized modification to the stego image can be identified. This multi-layered security mechanism not only conceals the presence of data but also guarantees that the message remains unaltered throughout transmission. The system is therefore highly effective in scenarios where confidentiality, integrity, and authenticity are paramount, such as secure messaging, digital document protection, and confidential data exchange. Overall, the project achieves its objective of providing a secure, reliable, and tamper-evident communication solution.

REFERENCES

[1] Rong Huang 1, Chunyan Lian, Zhen Dai1, Zhaoying Li, And Ziping Ma, “A Novel Hybrid Image Synthesis-Mapping Framework for Steganography Without Embedding”, Journal, 2023.

[2] Shahid Rahman, Jamal Uddin, Habib Ullah Khan, Hameed Hussain, Ayaz Ali Khan, Muhammad Zakarya, “A Novel Steganography Technique for Digital Images Using the Least Significant Bit Substitution Method”, Journal, 2022.

[3] Sunpreet Sharma, Ju Jia Zou, Gu Fang, “A Novel Multipurpose Watermarking Scheme Capable of Protecting and Authenticating Images With Tamper Detection and Localization Abilities”, Journal, 2022.

[4] Arshiya S. Ansari, Mohammad S. Mohammadi, Mohammad Tanvir Parvez, “A Multiple-Format Steganography Algorithm for Color Images”, Journal, 2020.

[5] Jagan Raj Jayapandiyan, C. Kavitha, K. Sakthivel,” Enhanced Least Significant Bit Replacement Algorithm in Spatial Domain of Steganography Using Character Sequence Optimization”, Journal, 2020.

[6] Donghui Hu, Liang Wang, Wenjie Jiang, Shuli Zheng, Bin Li, “A Novel Image Steganography Method via Deep Convolutional Generative Adversarial Networks”, Journal, 2018.