Cryptographic Camouflage : Unveiling the Symphony of Steganography, Dual-Control Encryption and Visual Transformation

A Project Report submitted in partial fulfillment of the requirements for

Mini Project

Integrated Post Graduate M.Tech

.

By

Devnarayana : 2021IMT-028

Saumya Seetha : 2021IMT-087

Siddharth Goyal : 2021IMT-098

Umang Solanki : 2021IMT-106

Under the Supervision of

Dr. Anjali

Department of Information Technology

ABV-INDIAN INSTITUTE OF INFORMATION TECHNOLOGY AND MANAGEMENT GWALIOR

GWALIOR, INDIA

CANDIDATES DECLARATION

We hereby certify that the work, which is being presented in the report, titled **Cryptographic Camouflage : Unveiling the Symphony of Steganography, Dual-Control Encryption and Visual Transformation**, in partial fulfillment of the requirement for the award of the Degree of **Integrated Postgraduate Masters of Technology in Information Technology** and submitted to the institution is an authentic record of our own work carried out during the period March 2024 to May 2024 under the supervision of **Dr. Anjali**. We also cited the reference about the text(s)/figure(s)/table(s) from where they have been taken.

Date:

Name: **Signature of the candidate**

Name: **Signature of the candidate**

Name: **Signature of the candidate**

Name: **Signature of the candidate**

This is to certify that the above statement made by the candidates is correct to the best of my knowledge.

Dated: **Signature of supervisor**

Acknowledgements

We are highly indebted to Dr. Anjali, and are obliged for giving us the autonomy of functioning and experimenting with ideas. We would like to take this opportunity to express our profound gratitude to her not only for her academic guidance but also for her personal interest in our project and constant support coupled with confidence boosting and motivating sessions which proved very fruitful and were instrumental in infusing self-assurance and trust within us. The nurturing of the present work is mainly due to her valuable guidance, suggestions, astute judgment, constructive criticism and an eye for perfection. Our mentor always answered myriad of our doubts with smiling graciousness and prodigious patience, never letting us feel that we are novices by always lending an ear to our views, appreciating and improving them and by giving us a free hand in our project. It's only because of her overwhelming interest and helpful attitude, the present work has attained the stage it has.

Finally, we are grateful to our Institution and colleagues whose constant encouragement served to renew our spirit, refocus our attention and energy and helped us in carrying out this work.

Devnarayana

Saumya Seetha

Siddharth Goyal

Umang Solanki

Abstract

Steganography, an ancient art of covert communication, has found renewed relevance in the digital age, particularly within image concealment. This paper presents a rigorous investigation into image steganography methodologies, aiming to enhance data concealment efficacy while preserving visual integrity. Conventional techniques, exemplified by the Least Significant Bit (LSB) method, are functional yet susceptible to detection and may compromise image fidelity. To address these challenges, a novel methodology is proposed, integrating compression, encryption, and image manipulation techniques. The process begins with Deflate algorithm compression of confidential messages, followed by AES encryption for stringent confidentiality. Encrypted data is strategically embedded within an inverted input image, leveraging Image Pre-Processing methods like Image Negative to fortify security while preserving visual fidelity. Post-encoding, the image is restored to its original state, concealing encrypted data within pixels. Further security is ensured through meticulous encryption using a unique key derived from sender-provided characters and a secure server phrase. Empirical analysis underscores the efficacy of this approach in enhancing security while maintaining visual quality. Subsequent sections delve into methodology intricacies, algorithmic details, and experimental validation, affirming its relevance and utility in clandestine communication applications.

Contents

List of Figures

1

Introduction

Steganography, an age-old practice akin to cryptography, conceals information within seemingly innocuous data. In the realm of modern technology, steganography serves as a potent tool for covert communication, particularly within mediums such as images, audio, and video. Among these, image steganography reigns supreme, enabling the embedding of confidential messages into images without arousing suspicion.

In our endeavor, we delve into the intricacies of image steganography, with a specific focus on bolstering security through innovative methodologies. Our aim is twofold: to fortify the concealment of secret data and to minimize perceptible alterations to the host image. Traditional techniques, such as the Least Significant Bit (LSB) method, while effective, can be vulnerable to detection and may inadvertently distort the visual integrity of the image.

To address these challenges, we introduce a novel approach enriched with layers of security measures. At the heart of our methodology lies the fusion of compression, encryption, and image manipulation techniques. Firstly, the secret text undergoes compression via the Deflate algorithm, reducing its footprint while preserving its integrity. Subsequently, the compressed text undergoes encryption using the robust Advanced Encryption Standard (AES) algorithm, ensuring confidentiality and thwarting unauthorized access.

The encrypted text is then embedded within the inverted input image, a process augmented by Image Pre-Processing techniques such as Image Negative. This inversion not only enhances security but also minimizes visual artifacts, thereby maintaining the natural appearance of the image.

Following the encoding process, the inverted image is reverted to its original state, concealing the encrypted data within its pixels. To further fortify security, the encoded image undergoes encryption once again, this time utilizing a unique key derived from a combination of sender-provided characters and a partial phrase retrieved from a secure server.

This amalgamation of sender input and server-provided data ensures key diversity, rendering brute-force attacks unfeasible. The resultant encrypted image serves as a fortified

vessel, safeguarding the concealed data against unauthorized interception and decryption attempts.

In the subsequent sections of this report, we elucidate the intricacies of our methodology, exploring the underlying algorithms, implementation details, and experimental results. Through empirical analysis, we demonstrate the efficacy of our approach in enhancing security while preserving the visual fidelity of the host image.

2

Motivation

In this section, we delve into the underlying reasons that led us to choose our project topic and its relevance within our academic and professional journey.

2.1 Significance of Cybersecurity in Contemporary Context

In today's technologically driven world, the importance of cybersecurity cannot be overstated. With the increasing reliance on digital communication and data exchange, the risk of unauthorized access, data breaches, and cyber-attacks has become a prevalent concern. As aspiring engineers, we recognize the critical role of cybersecurity in protecting sensitive information and ensuring the secure transmission of data.

Our interest in cybersecurity stems from a combination of academic exploration and real-world implications. Through our coursework in Image Processing, Information and System Security, Cryptography, and Network Security, we have gained insights into the mechanisms that underpin secure communication protocols.

Furthermore, our fascination with the dynamic nature of cybersecurity motivates us to explore innovative solutions to address emerging threats. We view our final year project as an opportunity to delve deeper into this domain, applying our knowledge and skills to contribute meaningfully to the field.

2.2 Relevance to Academic and Professional Development

Undertaking a final year project focused on secure communication aligns with our academic pursuits and professional aspirations. By exploring image steganography enhanced with security measures, we aim to bridge theoretical knowledge with practical application.

Our project serves as a platform to develop essential skills such as problem-solving, critical thinking, and project management. Through hands-on experimentation and collaborative efforts, we seek to enhance our proficiency in various domains while gaining insights into secure communication protocols.

Moreover, the potential scalability of our project presents opportunities for future endeavors. As we consider proposing our solution to government agencies as a secure communication technique, we acknowledge the impact our project could have on national security infrastructure.

2.3 Envisioned Impact and Contribution

Beyond academic objectives, our project aims to make a tangible impact on society by enhancing data privacy and mitigating cyber threats. Through meticulous planning, rigorous execution, and effective documentation, we aspire to create a project that not only meets academic requirements but also addresses broader concerns regarding cybersecurity.

In subsequent sections, we outline our methodology, experimental findings, and implications for future research. Through transparent discourse and meticulous analysis, we seek to elucidate the nuances of our project and its potential implications for the field of cybersecurity.

2.4 Contributions

In this project contributions of the group members are as follows:-

- Devnarayana (2021IMT-028) - Image Processing Techniques and Image Inversion: Implemented image processing methods like geometric transformations and dynamic embedding using Python to enhance security measures.
- Suamya Seetha (2021IMT-087) - Integration of Cryptographic Algorithms: Integrated AES encryption within the steganography framework using Python for secure data concealment.
- Siddharth Goyal (2021IMT-098) - Algorithm Development and Optimization: Utilized Python for algorithm design, development, and optimization of steganography techniques.

- Umang Solanki (2021IMT-106) - Experimental Validation and Performance Evaluation: Conducted extensive testing and analysis in Python to validate the efficacy of the developed steganography framework, comparing it with existing techniques

3

Literature Survey

In the domain of image steganography, the endeavor is to encode textual data within images, primarily utilizing the Least Significant Bit (LSB) of the image and substituting it with the input data. Several scholarly works contribute to enhancing the security and efficacy of steganographic techniques, often integrating encryption algorithms such as Advanced Encryption Standard (AES) for added protection. Below is a synthesized overview of relevant literature contributing to the advancement of image steganography:

(i) **Enhancing Security with AES Encryption:** A paper proposes a methodology to bolster the security of messages transmitted via steganography by coupling it with AES encryption. This integration aims to fortify the concealment of data within images, ensuring confidentiality and resilience against unauthorized access.

(ii) **Utilization of Pycrypto/Pycryptodome Library:** Another study explores the practical implementation of AES encryption within the Python ecosystem, leveraging the pycrypto/pycryptodome library. The paper delves into the usage of AES methods and classes, offering insights into the application of cryptographic principles in steganographic frameworks.

(iii) **High-Capacity Embedding with AES-128:** Introducing a novel approach to image steganography, this research emphasizes high embedding capacity and security while maintaining image quality. By employing Variable Least Significant Bit (VLSB) embedding and AES-128 encryption, the methodology ensures robust concealment of audio or video data within images, evaluated based on criteria such as time complexity, quality, and security.

(iv) **Refined Techniques in Spatial Domain:** A refined steganographic technique is proposed, focusing on acceptable embedding capacity, security, and visual imperceptibility. The methodology incorporates random bit sequence generation and utilizes quadratic residues for embedding pixel location. Although limited to YCbCr color space, the approach achieves 100% embedding efficiency with minimal probability of detection.

(v) **Wavelet-Based Steganography with SVD:** This study introduces a unique technique leveraging discrete wavelet transformation and singular value decomposition (SVD) for image steganography. By altering specific frequency bands, particularly the HH band, the methodology ensures secure data hiding without compromising image quality. Experimental results demonstrate resistance to image processing attacks, highlighting the algorithm's robustness.

(vi) **Integration of Cryptographic Algorithms:** Offering a layered approach to data security, this paper combines LSB steganography with RSA, AES, DES, and Blowfish encryption algorithms. The methodology employs multiple layers of encryption and concealment, making it challenging for intruders to access the original data. Experimental analysis evaluates the quality of the final image and assesses factors such as encryption to decryption time and signal-to-noise ratio.

(vii) **Overview of Cryptography Techniques:** This study provides a comprehensive overview of cryptography techniques and their applications in data concealment. It discusses the distinction between steganography and watermarking, highlighting linguistic and technical approaches to encoding messages across different media types.

(viii) **Combining Cryptography and Steganography:** Proposing an algorithmic fusion of cryptography and steganography, this research emphasizes the utilization of multiple encryption keys for enhanced security. AES encryption, complemented by Discrete Cosine Transformation (DCT) for message encoding, forms the basis of this robust communication tool.

In conclusion, while significant progress has been made in the realm of image steganography, it is evident that existing systems still grapple with notable drawbacks, including computational complexity, distortion issues, and compromised image quality. These limitations impede the efficacy of concealment techniques and compromise data confidentiality. Moreover, a critical observation arising from the literature survey is the lack of

integration between image processing, encryption, and steganography methodologies in previous studies. The absence of such amalgamation renders these approaches less innovative, less secure, and more susceptible to detection. Consequently, future research endeavors must prioritize the exploration of integrated frameworks that seamlessly combine image processing, encryption, and steganography techniques to mitigate the identified limitations and advance the state-of-the-art in data concealment. By bridging these disparate domains, researchers can pave the way for more robust and resilient concealment strategies that uphold confidentiality while minimizing computational overhead and preserving image fidelity.

4

Methodology

4.1 Foundation of our Methodology

In a comprehensive review of LSB-based image steganography techniques, diverse methodologies leveraging various cryptographic algorithms have been explored. Previous research in this domain has investigated techniques for concealing data within images, encompassing LSB embedding, spatial domain methodologies, and frequency domain methods. Despite offering different balances between security, capacity, and visual quality, these approaches often contend with detectability issues or introduce visual artifacts. Our proposed methodology builds upon these foundational methods by integrating image inversion to augment security measures and minimize detection risks.

Our work is delineated based on the study of three crucial approaches:

4.1.1 Least Significant Bit Substitution Technique (LSB):

This technique involves modifying the LSBs of the pixel values in the cover image according to the message bits. LSB replacement, being the simplest of LSB steganography techniques, ensures minimal perceptible difference between the original and stego images.

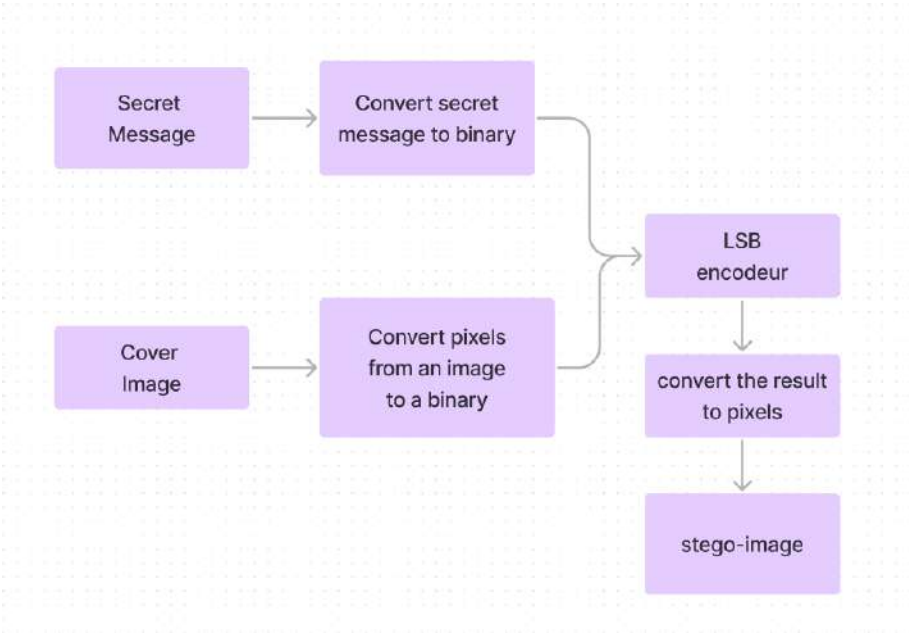

Figure 4.1: LSB technique to hide text message.

4.1.2 Pseudo-Random LSB Encoding Technique:

In this approach, a random key is utilized to select pixels randomly for message bit embedding. This randomness complicates the task of message bit identification for potential intruders. The use of this technique across the RGB color model makes it challenging for attackers to discern any hidden message patterns.

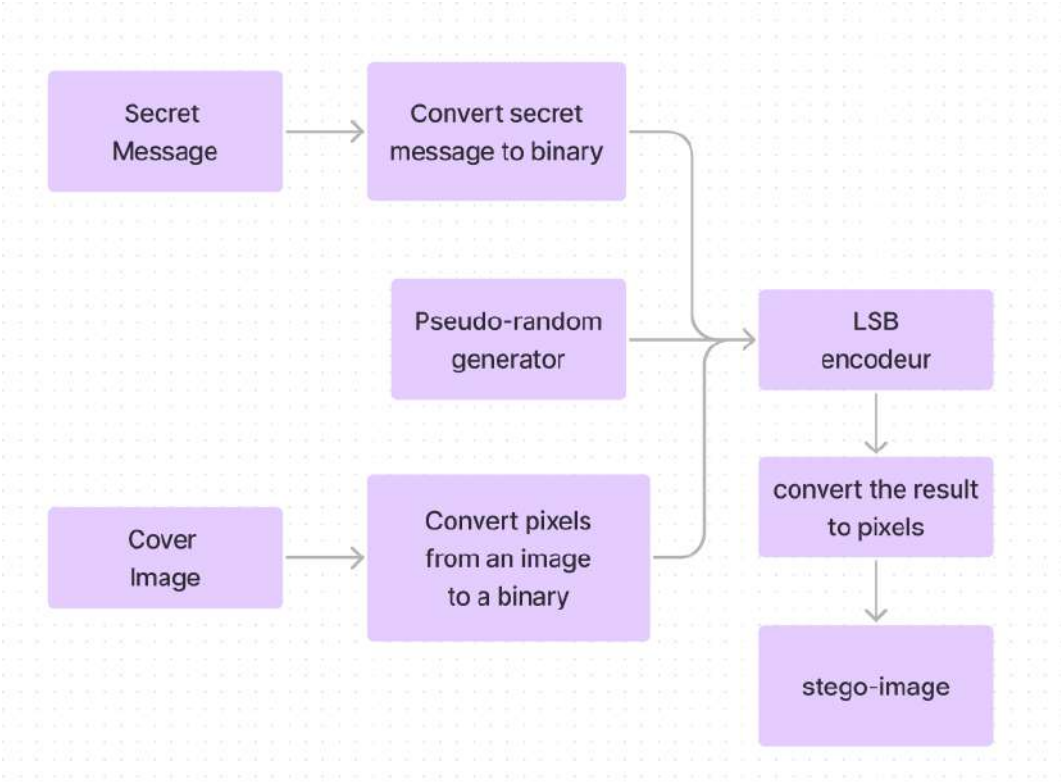

Figure 4.2: Improved Pseudo-Random LSB technique

4.1.3 Distortion Technique:

This methodology is a variation of the LSB substitution technique, wherein pixel value modification occurs only if the secret bit value is 1. Otherwise, the pixel value remains unchanged, diverging from the conventional LSB technique where every pixel value is modified regardless of the bit value. Employing a pseudorandom number generator facilitates the selection of cover pixels for information hiding, minimizing changes to the cover image.

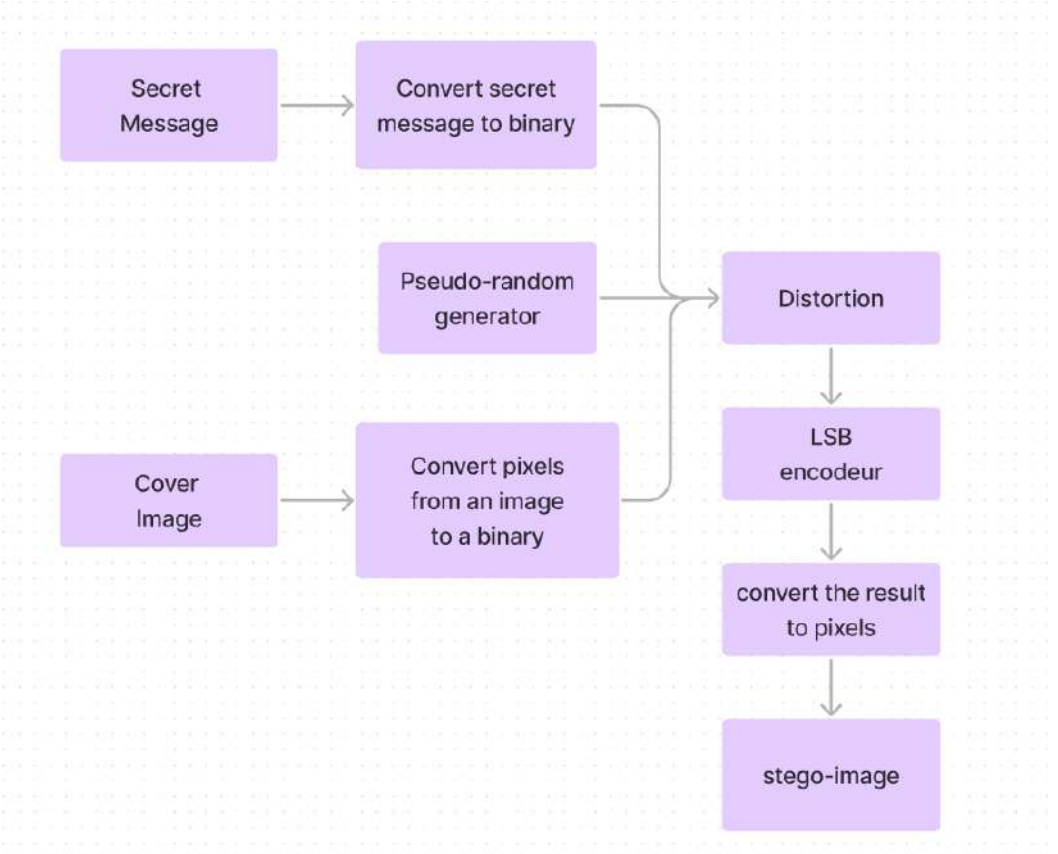

Figure 4.3: Distortion technique technique to hide text message.

4.2 OUR IMPROVED APPROACH

Our approach enhances the pseudo-random LSB encoding technique by focusing solely on message modification, which undergoes three distinct phases before injection into the cover image:

(i) **Message Compression:** The message undergoes compression using a lossless deflation algorithm to maximize information storage.

(ii) **Message Encryption:** The compressed message is encrypted using the AES algorithm (Advanced Encryption Standard), providing dual control over the key to ensure message security. AES is chosen for its speed and robust security features.

(iii) **Message Embedding:** The encrypted message is then converted into binary mode before being injected into the cover image.

Subsequently, our methodology combines LSB embedding with image inversion to achieve heightened security and visual quality. The process commences with loading the cover image, followed by its inversion to further obscure the presence of hidden data. A random key is employed to select pixels of the inverted image randomly for message bit storage, making it more challenging for intruders to locate the message bits, especially given their inclination to decode non-negative images. Additionally, utilizing the RGB color model enables data hiding in the LSB of any color space of the randomly selected pixels.

4.2.1 Embedding Algorithm:

(i) Get the cover image, secret message, and 4 characters for key generation.

(ii) Compress the message using a deflation compression algorithm. 3. Encrypt the compressed message using the AES algorithm with a key generated by combining partial phrases retrieved from the server and the 4 characters provided by the user.

(iii) Divide the message into bits, either as text or binary data.

(iv) Perform total inversion on the cover image, negating its values.

(v) Initialize a random key, seed, and randomly identify pixels in the inverted cover image for LSB modification. This seed is used to generate the same set of random values every time by using random number generator.

(vi) Modify the LSBs of randomly located pixels according to the message bit values, beginning with the Red color space pixels and repeating the process for Green and Blue spaces.

(vii) Feed the modified pixel values back to their respective positions based on the size of the message data.

(viii) Take the negative of the stego-image.

(ix) Save and transmit the negative stego-image.

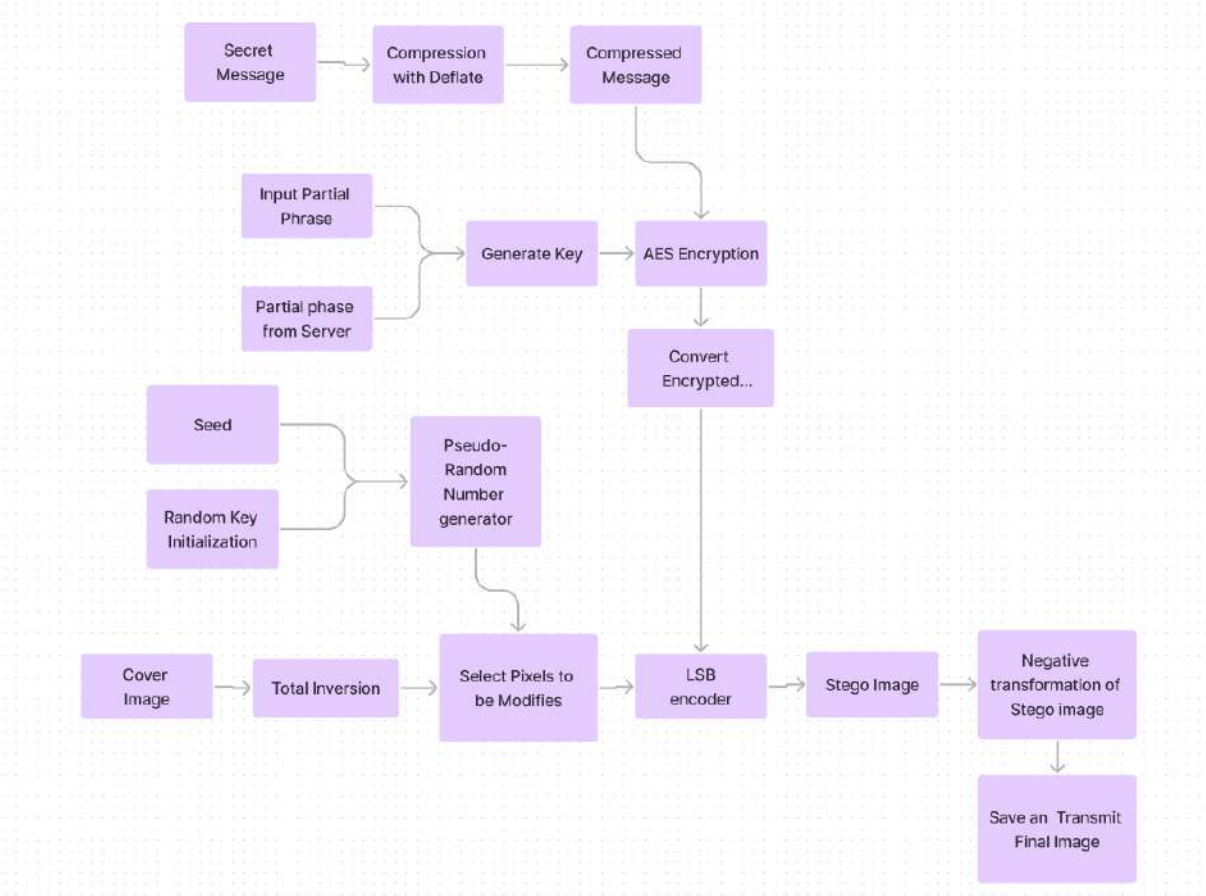

Figure 4.4: Flow Chart Representation of Our Approach to hide the secret message

4.2.2 Algorithm to Retrieve Text Message:

(i) Input the stego-image and 4 characters for key generation.

(ii) Negate the input stego-image.

(iii) Initialize the random key and randomly identify pixels of the cover image, using the same random key used during embedding.

(iv) Read the LSB of each identified pixel in the negative stego-image.

(v) Generate the key using the 4 characters inputted by the user combined with a partial phrase from the server. Use this key generated to decrypt using the AES algorithm.

(vi) Decompress each byte using the deflation compression algorithm.

(vii) Convert each set of 8 bits into characters to reconstruct the secret message.

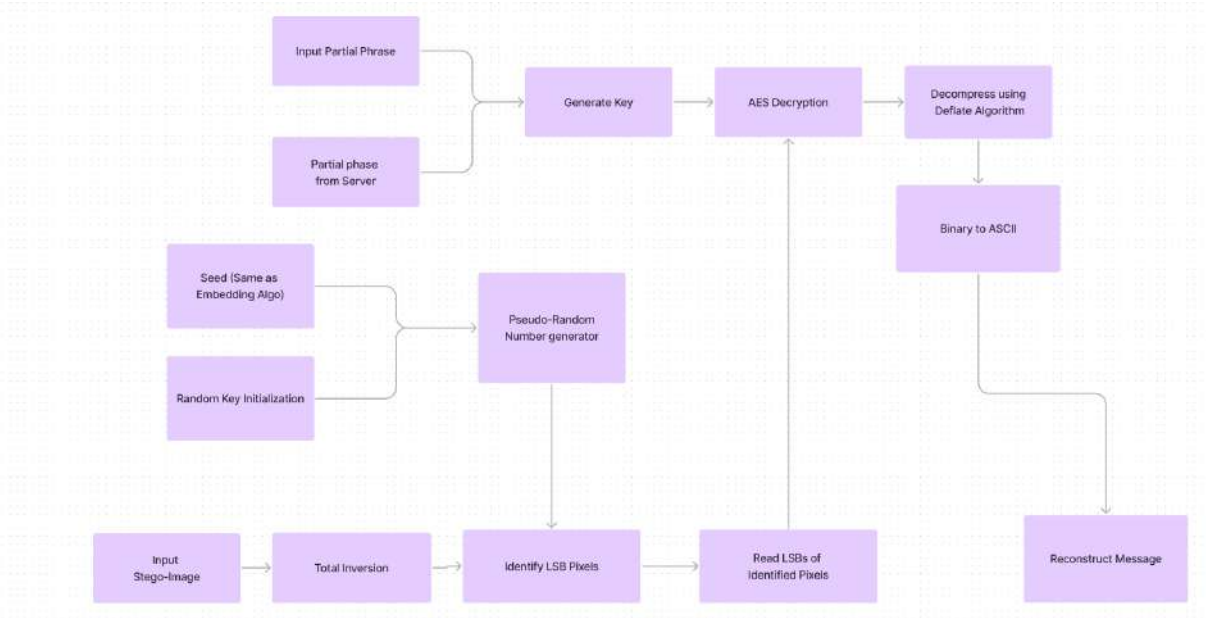

Figure 4.5: Flow Chart Representation of Our Approach to retrieve the secret message.

This refined methodology integrates advanced encryption and data compression techniques with LSB embedding and image inversion, thereby enhancing the security, confidentiality, and visual fidelity of the steganographic process.

5

Results and Discussions

5.1 Experimental Results and Discussion:

Our experimental results demonstrate the efficacy of our proposed method in concealing information within images while preserving image quality. By combining LSB embedding with image inversion, we achieved improved security against detection techniques, resulting in stego-images with fewer visual artifacts compared to conventional LSB embedding methods.

Additionally, we implemented AES encryption with dual control, utilizing both a partial phrase retrieved from the server and a 4-character user input to generate the encryption key. This dual control mechanism enhances the security of our steganographic technique by mitigating various cyber attacks:

- **Resistance to Brute Forcing:** The AES encryption key, generated from a combination of the partial phrase and the user input, is significantly longer than traditional keys. This length increases the complexity of brute force attacks, making them impractical and time-consuming.

- **Protection Against Guessing Attacks:** Even if an attacker manages to guess the user's 4-character input, the partial phrase retrieved from the server remains concealed. This ensures that the encryption key cannot be easily deduced, enhancing the overall security of the system.

- **Ease of Use:** The use of a 4-character user input simplifies the process for both the sender and receiver, eliminating the need for complex passwords while maintaining a high level of security.

- **Resistance to Man-in-the-Middle (MITM) Attacks:** The dual control mechanism adds an extra layer of protection against MITM attacks, as intercepted communication would require knowledge of both the user input and the server's partial phrase to decrypt the hidden message.

Figure 5.1: Cover Image

Figure 5.2: Negative Cover Image

Figure 5.3: Encoded Image

Figure 5.4: Final Output(Negative Encoded Image)

Figure 5.5: Cover Image

Figure 5.6: Negative Cover Image

Figure 5.7: Encoded Image

Figure 5.8: Final Output(Negative Encoded Image)

Furthermore, our method combines elements of cryptography with LSB-based steganography, resulting in minimal degradation of the cover image and good embedding capacity. The use of the 256-bit AES algorithm ensures strong encryption, providing robust protection for the hidden message. In summary, our enhanced steganographic approach offers several advantages, including minimal visual distortion, strong encryption, and ease of use, while mitigating various cyber threats such as brute force attacks, guessing attacks, and MITM attacks. Our experimental evaluation confirms the effectiveness of our method compared to existing techniques, highlighting its suitability for secure communication and data concealment applications.

6

Conclusion and Future Scope

6.1 Conclusion:

In conclusion, our innovative fusion of advanced image processing and steganography techniques represents a significant advancement in the field of secure data concealment. By incorporating sophisticated image transformations and dynamic embedding strategies, we have achieved a delicate balance between security, visual quality, and data capacity. Our approach demonstrates enhanced resilience against steganalysis techniques, ensuring the confidentiality of hidden messages while minimizing visual distortion in the cover image.

6.2 Future Scope:

Looking ahead, there are several avenues for future research and development:

(i) **Integration of Multiple Encryption Algorithms:** Expanding our approach to incorporate multiple encryption algorithms such as AES, RSA, and ECC can further enhance security without significantly increasing computational complexity. By leveraging the strengths of each algorithm, we can create a more robust encryption framework.

(ii) **Exploration of Advanced Image Transformation Techniques:** Investigating advanced image transformation methods like rotation, scaling, and Fourier transform can diversify image embedding strategies and improve resilience against steganalysis. These techniques can provide additional layers of security while maintaining visual fidelity.

(iii) **Optimization of Key Management Protocols:** Developing optimized key management protocols for secure key generation, distribution, and storage is crucial for long-term security. By implementing efficient key management practices, we can ensure the integrity and confidentiality of encrypted data.

(iv) **Dynamic Embedding Strategies:** Developing dynamic embedding strategies that adapt to image content and characteristics in real-time can further enhance security and minimize detection. Integration of machine learning algorithms can optimize embedding processes and improve embedding locations based on image analysis.

(v) **Exploration of Novel Security Layers:** Exploring additional layers of security, such as encoding data into pre-selected images and lossless compression before embedding into user-input images, can further enhance data confidentiality and resilience against attacks. This approach can provide an additional barrier against unauthorized access and ensure the integrity of hidden messages.

In future work, the development of a comprehensive communication channel incorporating our steganographic techniques could revolutionize secure communication in various domains, including government and defense organizations. This integrated communication platform would streamline the process of secure data concealment and facilitate seamless communication while maintaining a high level of security.

Overall, our research opens up exciting possibilities for advancements in secure data concealment and communication, paving the way for innovative solutions to address emerging challenges in the digital age. Through continued exploration and refinement, we aim to contribute to the development of robust and resilient security mechanisms for safeguarding sensitive information.

Bibliography

[1] A. K. H. B. B. Zaindan, "an overview on hiding information techniques in images," *journal of applied sciences*, 2010.

[2] J. Hossain, "Information-hiding using image steganography with pseudorandom permutation," *Bangladesh Research Publications Journal*, 2014.

[3] M. S. R. S. M. Masud Karim and M. I. Hossain, "A new approach for lsb based image steganography using secret key," *14th International Conference on Computer and Information Technology (ICCIT 2011)*, 2011.

[4] S. N. Gowda, "An advanced diffie-hellman approach to image steganography," *2016 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, 2016.

[5] S. Levine, "Learning hand-eye coordination for robotic grasping with deep learning and large-scale data collection." *The International Journal of Robotics Research, 37(4-5), 421-436.*, 2018.

[6] X. B. Peng, "Deepmimic: Example-guided deep reinforcement learning of physics-based character skills." *ACM Transactions on Graphics (TOG), 37(4), 1-14.*, 2018.

[7] N. Heess, "Learning and transfer of modulated locomotor controllers." *arXiv preprint arXiv:1707.05363.*, 2017.

[8] T. D. Kulkarni, "Hierarchical deep reinforcement learning: Integrating temporal abstraction and intrinsic motivation." *In Advances in neural information processing systems (pp. 3675-3683).*, 2016.

[9] J. Schulman, "Proximal policy optimization algorithms." 2017.

[10] S. Russell, "Deep successor reinforcement learning." *arXiv preprint arXiv:1801.06471.*, 2018.

[11] D. Silver, "Mastering the game of go with deep neural networks and tree search." *Nature, 529(7587), 484-489.*, 2016.