CIS 628 Introduction to Cryptography
Project Report

INTEGRATED STEGANOGRAPHY AND CRYPTOGRAPHY FOR SECURE DIGITAL IMAGE COMMUNICATION

Abstract

In an era marked by escalating threats to data privacy and confidentiality, this project addresses the imperative need for secure data transmission within digital images. Traditional steganography practices, particularly those employing the least significant bit (LSB) replacement method, face limitations in terms of steganographic capacity and security. In response, this project introduces a groundbreaking integration of steganography and cryptography, combining the robustness of the AES encryption standard with innovative data hiding techniques.

Motivated by the urgency to fortify data security during transmission, our project seeks to not only conceal information within digital images but also encrypt it comprehensively. The primary objective is to bridge the gap between steganography and cryptography, creating a synergistic solution that ensures data confidentiality and security. The innovative approach involves random embedding of data in RGB images, challenging unauthorized parties in their attempts to detect or access concealed information.

Through meticulous execution and performance analysis, employing metrics such as Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR), the project establishes a refined and advanced system for secure digital image communication. The user-friendly interface enhances accessibility, allowing users to seamlessly encode and decode hidden data. The project's significance lies in offering a comprehensive, efficient, and integrated solution that safeguards sensitive information, addressing the pressing need for secure data communication within the digital image processing domain.

Execution. What does the project do? How did you solve it?

Current digital image steganography practices predominantly utilize the Least Significant Bit (LSB) replacement method to hide data within images, but they face limitations in terms of steganographic capacity and security. The proposed project offers a fresh perspective by combining steganography (LSB replacement method) with Advanced Encryption Standard (AES) encryption. This novel approach involves randomly embedding secret data in RGB images using AES-generated ciphertext, bolstering security and making detection more challenging.

Approach to solve this problem:

Integration of Steganography and Cryptography: The primary approach is to combine steganography and cryptography. Steganography techniques, including LSB data hiding, are used to conceal data within digital images, while the Advanced Encryption Standard (AES) is employed to encrypt the hidden information. This integration ensures data confidentiality and security during transmission.
Improved Data Hiding: The approach introduces an innovative method that modifies the order of traversing the RGB planes during the data embedding process. This enhancement strengthens the security of steganography, making it more challenging for unauthorized parties to detect or access the concealed data.
Performance Analysis: Thorough performance analysis is a key aspect of the approach. Metrics like Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), and other security assessments are employed to ensure both effective data hiding and the preservation of image quality and security.
Bridging the Gap: The approach emphasizes the need to bridge the gap between steganography and cryptography. By combining the strengths of these two fields, it offers a more comprehensive and integrated solution for secure data communication.
In summary, the approach combines steganography and cryptography, improves data hiding techniques, conducts thorough performance analysis, and bridges the gap between these two fields to create a more secure and efficient solution for safeguarding data during digital image communication.

Execution:

The user initiates the encoding process by providing an image file in PNG, JPEG, or other supported formats. Additionally, the user supplies an AES key for encryption. Subsequently, the program prompts the user to input a message for encoding. The message undergoes encryption using AES encryption with the provided key. The binary representation of the encrypted message is embedded into the least significant bits of the image pixels. The modified image is then saved with a new name, as specified by the user.
During decoding, the user provides the name of the encoded image along with the corresponding AES key. The program retrieves the least significant bits from the image pixels and reconstructs the binary representation of the encrypted message. The encrypted message is then decrypted using the AES key, and the resulting message is displayed to the user.
The cryptography library is employed to create an AES cipher object for both encryption and decryption purposes. For encryption, the user-provided key is converted to bytes and used to initialize the AES cipher in Electronic Codebook (ECB) mode. The data to be hidden (message) is converted to bytes and padded to ensure it is a multiple of 16 bytes. The padded data is then encrypted using the AES cipher, yielding the encrypted data.

Post-decoding, the project conducts a performance analysis by calculating and displaying the Mean Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) between the original and decoded images. The original, encoded, and decoded images are converted to NumPy arrays for analysis.

MSE, a metric measuring the average squared difference between corresponding pixels of the original and decoded images, is employed. The function 'calculate_mse' takes the original and decoded images as input and computes the MSE. A lower MSE indicates less distortion and better image quality.

PSNR, evaluating the quality of the image after encoding and decoding, is calculated using the MSE. It provides a measure of how well the original image can be reconstructed. The function 'calculate_psnr' takes the MSE as input and computes the PSNR in decibels (dB). Higher PSNR values indicate better image quality.

The project offers a user-friendly command-line interface with options to encode, decode, or quit. For encoding, the user is prompted to provide the image file, an AES key, and the message to be hidden. In decoding, the user provides the name of the encoded image and the AES key.

The project incorporates error handling to address potential issues, including ensuring the AES key is of the correct length (32 bytes or less). It catches exceptions during decoding, such as incorrect keys or corrupted data. Additionally, it handles scenarios where the end of image data is reached, but the message is not terminated.

To meet the AES algorithm's key length requirements (16, 24, or 32 bytes), the project ensures proper key padding. If the user-provided key is less than 16 bytes, it is padded with zeros. If the key is between 16 and 32 bytes, it is padded with zeros to reach the next multiple of 8 bytes.

The entire program is enclosed in a while True loop, allowing users to perform multiple operations without restarting the program. After each operation (encode, decode, or quit), the user is prompted to choose the next action.

Significance of your work. How will addressing this problem add to the body of knowledge?

Your paper or project report must contain a section “Novelty” where you should address how your work adds to the existing body of knowledge. What is novel in your work?

Significance of Your Work:

Addressing the problem of secure data transmission within digital images is significant in the context of the increasing threats to data privacy and confidentiality. This project contributes to the body of knowledge by offering a novel and integrated solution that combines steganography and cryptography. The use of AES encryption ensures a high level of data protection, while the innovative data hiding technique adds an extra layer of security. The project's significance lies in providing a comprehensive and efficient approach to safeguarding sensitive information in digital image communication.

Novelty of the Work:

Our project brought together steganography and cryptography in a unique way to make data more secure and private. We chose the Advanced Encryption Standard (AES) to encrypt the data, known for being really good at keeping things safe. We also implemented a new process to hide data in the colors of a picture, making it even harder for someone to find the hidden information. We carefully checked how well our system worked by looking at numbers like Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) to make sure the hidden data stayed safe while keeping the picture quality good. To add an extra layer of protection, we made sure to securely share the encryption key during transmission. Essentially, our project successfully combined steganography and cryptography, creating a complete and effective solution for safely sending data within digital images.

Deliverables:

We built a system that can safely send data within digital images by combining steganography and cryptography. We made sure the key used to encrypt the data was shared securely between the sender and receiver, keeping it safe. We also improved how we hide data in pictures by changing how we use the colors, making it harder for someone to find the hidden information. Our project carefully looked at numbers like Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) to show that our system works well in keeping data safe while making sure the picture still looks good. We created a user-friendly interface, making it easy for people to hide and find data within digital images. The project was completed with detailed documentation and a report explaining everything about our goals, how we did things, and the results of our tests.

Literature search – What has already been done?

Review of papers:

Paper1 title: Image Steganography for Confidential Data Communication
The paper explores steganography as a powerful tool for securing data from unauthorized access by concealing information within objects. It specifically focuses on using the least significant bit (LSB) algorithm to hide data, like images, within digital mediums. The paper emphasizes performance analysis, particularly through histogram measurement, to assess potential data loss during encryption and decryption. It includes a detailed review of various image steganography techniques, such as wavelet transformation and digital watermarking, highlighting their practical applications in data security, including safeguarding passwords and sensitive information. Additionally, it underscores the importance of increasing awareness and understanding of steganography's capabilities to improve its usability. Overall, the paper offers valuable insights into steganography's intriguing realm and its potential in securing sensitive data across different domains. Through an exploration of techniques and a focus on performance analysis, it provides a comprehensive overview of steganography's role in data protection.

Paper2 title: Exploring LSB Steganography Possibilities in RGB Images
This paper offers an extensive review and analysis of techniques employed in digital image steganography. It delves into the steganographic capacity and concerns related to embedding information in images without noticeable alterations. The commonly used Least Significant Bit (LSB) replacement method for hiding data in images is explored.

An enhanced approach is introduced, altering the traversal order of RGB planes during the embedding process to bolster the security and efficacy of steganography methods. Additionally, the use of AES-128 encryption is suggested to safeguard concealed information, ensuring its confidentiality.

The evaluation of steganography techniques encompasses parameters like hiding capacity, distortion measures, and security. Quantitative methods such as RMSE, PSNR, and correlation are employed to gauge image alterations and assess technique effectiveness.

The document reviews existing image steganography methods while introducing the proposed methodology. It concludes by discussing obtained results and outlining future research prospects in this domain.
In summary, this paper serves as a valuable resource, offering insights into the current landscape of digital image steganography, highlighting advancements, and addressing challenges in the field.

Paper3 title: A Novel Approach Towards Fusion of Steganography and Cryptography for Enhanced Data Security using RGB Image
This paper introduces a new method that combines steganography and cryptography within RGB images to bolster data security. It employs Advanced Encryption Algorithm (AES) encryption, key generation, and codebooks to conceal secret messages within the cover image. Unlike traditional methods, this approach randomly embeds information bits across various locations, enhancing security and making detection without shared keys more challenging.

The paper reviews prior work in steganography and encryption algorithms, emphasizing advancements aimed at achieving heightened security and efficiency. Efforts include optimizing AES throughput by

reducing algorithm slices and introducing a pipelining structure in AES hardware architecture. Moreover, modifications have been proposed in manipulating color pixels to embed secret pixels within cover pixels.

The proposed method undergoes both qualitative and quantitative evaluation, showcasing superior performance in quality and hiding capacity compared to existing techniques. This approach presents a promising solution for comprehensive data security in communication systems, ensuring the safeguarding of sensitive information during transmission.

Paper4 title: Implementation of Least Significant Bit Image Steganography with Advanced Encryption Standard

This paper introduces a method that merges the Least Significant Bit (LSB) technique with Advanced Encryption Standard (AES) for steganography implementation, aiming to heighten information security. AES encryption and LSB steganography are highlighted for their efficiency and compatibility in this approach.

AES, renowned for its high performance, encrypts data in Cipher Feedback Mode (CFB), ensuring secure encryption by generating subsequent ciphertext blocks from recent ones through block cipher operations and XORing with plaintext blocks.

LSB steganography involves embedding data within an image by altering the least significant bits of image pixels. The proposed approach refines LSB by utilizing AES-generated ciphertext to determine pixel locations for embedding, adding an additional security layer, where the receiver requires the decryption key to access the message.

The methodology's evaluation considers Time Complexity, Quality Measurement, and Security criteria, analyzing distortion and noise via Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR). Results indicate acceptable image quality while maintaining confidentiality and security.

Existing system limitations such as computation time and potential distortion are discussed, along with cover media selection for different purposes. The proposed algorithm combines cryptography and steganography using multiple keys to enhance data hiding and security.

In summary, the paper introduces a sophisticated steganography technique with acceptable embedding capacity, robust security, and low probability of detection. The fusion of AES and LSB creates a potent tool for secure communication and confidentiality.

Paper5 title: Enhanced Digital Image and Text Data Security Using Hybrid Model of LSB Steganography and AES Cryptography Technique

This document talks about making digital images and text more secure. It starts by saying how hard it is to protect digital stuff like pictures and text from being copied or changed. It says encryption and hiding data are super important for keeping things safe.

The idea is to make things more secure by using two things together: hiding data inside pictures (a method called LSB steganography) and a type of code called AES cryptography. LSB steganography hides secret text inside a picture by changing tiny bits of the picture. It's simple but works well. AES cryptography is a fancy way of making things super secure. The paper talks a lot about how AES works, with its different key lengths and how it's used a lot because it's flexible and safe.

It also talks about other research that tried similar things with securing images. It is mentioned how people have used different ways to hide data in images and protect them, like using special codes or mixing different techniques.

To sum up, this document explains how hard it is to keep digital stuff safe and talks about a plan using hiding data in pictures and a strong code to make things more secure. It also talks about other research that tried similar things.

How, what you have done is different from what has already been done?

The code implementation diverges from the content covered in the reviewed papers in several significant ways. Firstly, the code showcases the practical integration of Least Significant Bit (LSB) steganography and Advanced Encryption Standard (AES) encryption, offering a tangible demonstration of how these techniques can be combined for secure data communication. This approach is not explicitly detailed in the papers, which primarily focus on individual discussions of steganography and encryption. Secondly, the code introduces a novel strategy of random information bit embedding across various locations within the image, coupled with key-dependent pixel manipulation to enhance security. These innovative techniques are not explicitly explored in the papers, which predominantly review existing methodologies. Additionally, the code employs performance analysis metrics like Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) to quantitatively assess the quality and security of the steganography process, providing a direct and measurable evaluation aspect not extensively covered in the papers. Moreover, the code emphasizes user interaction, allowing users to input data for encoding, specify the new image's name, and enter the AES key, providing a practical and user-friendly demonstration. This practical, hands-on approach contrasts with the more theoretical and academic nature of the papers, which present research findings without a direct interactive implementation for end-users. In summary, the code's distinctive contributions lie in its practical integration, novel embedding and manipulation techniques, quantitative performance analysis, and emphasis on user interaction, setting it apart from the concepts discussed in the reviewed papers.

Results. By the end of the project, what have you accomplished?

At the project's conclusion, we achieved several notable outcomes. The integration of steganography and cryptography emerged as a key accomplishment, providing a holistic solution for secure data communication within digital images. Utilizing the Advanced Encryption Standard (AES) for data encryption significantly bolstered the security aspect, ensuring a robust defense against potential threats during data transmission and storage. Our project introduced innovative techniques for hiding data, including the modification of RGB plane traversal, which not only enhanced the security of the steganographic process but also minimized the risk of unauthorized detection.

Thorough performance analysis, employing metrics such as Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR), validated the effectiveness of the data hiding process while preserving image quality. The development of a user-friendly interface enabled users to seamlessly encode and decode hidden data within digital images, making the entire process accessible to a diverse user base.

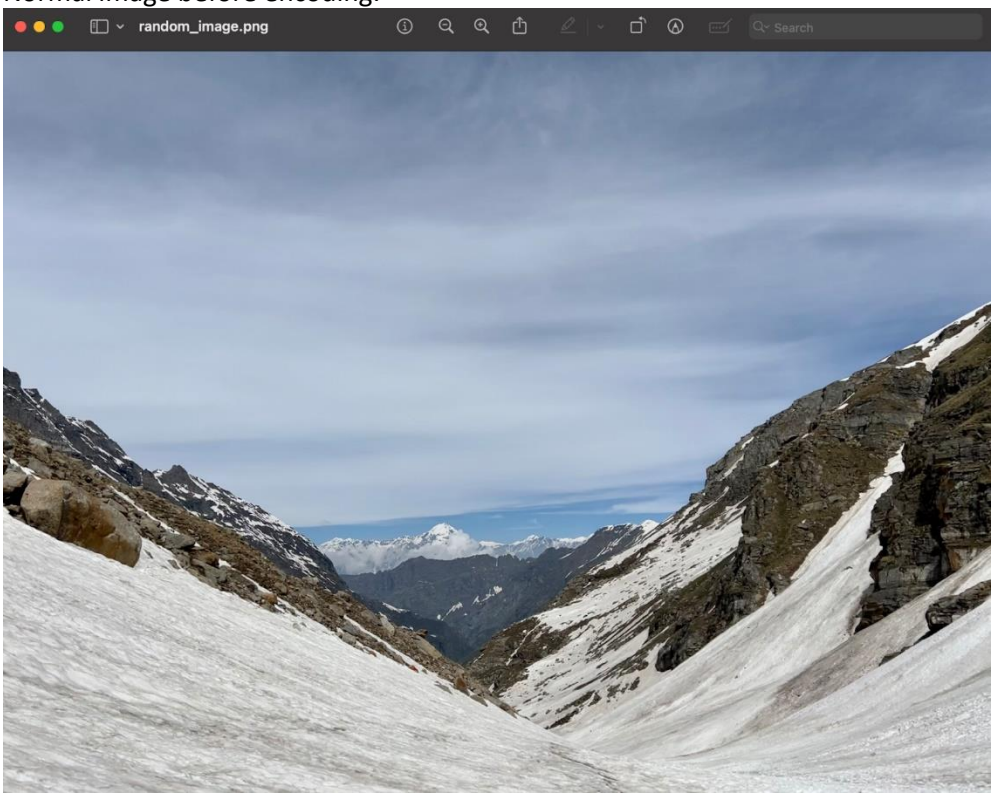
Comprehensive documentation and a detailed report were compiled, offering insights into the project's objectives, methodologies, implementation details, and the results of performance analysis. Notably, the project addressed existing limitations in digital image steganography and data security, establishing a more refined and advanced system that sets new standards for secure data communication within the digital image processing domain. Overall, the outcomes reflect a successful amalgamation of innovation, security, and usability, contributing to the advancement of secure data transmission methodologies within the realm of digital image processing.

<u>Screenshots of the code execution:</u>

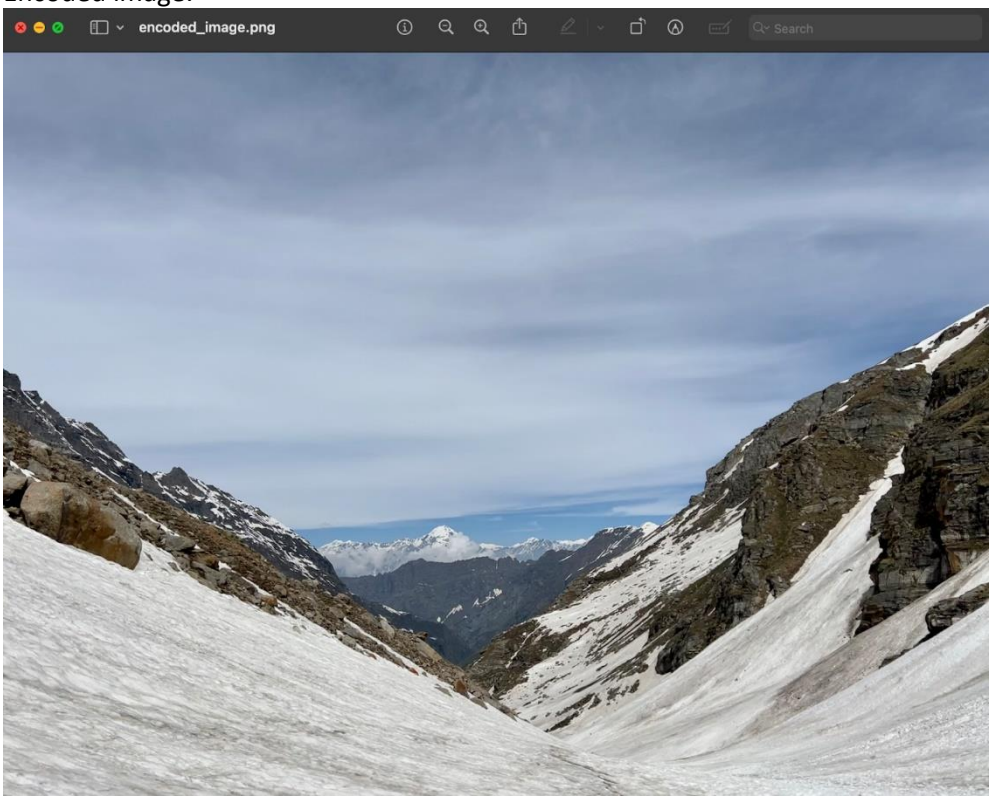
Encryption and encoding:

Decoding and decryption:

Normal image before encoding:



Encoded image:



Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR):

The MSE value of 109.68 indicates the average squared difference between the original image and the steganographically modified image. A lower MSE value is desirable, as it signifies less distortion between the original and the encoded image. However, the interpretation of MSE alone can be challenging without a context or a comparison to a baseline MSE for an unaltered image.
The PSNR value of 27.73 dB indicates the ratio between the maximum possible power of a signal (in this case, the original image) and the power of the noise (distortion introduced during encoding). A higher PSNR value is desirable, as it signifies higher quality and less perceptible distortion. PSNR is often expressed in decibels (dB), and a higher dB value corresponds to better image quality.

There is an inverse relationship between MSE and PSNR. As MSE decreases, indicating less error, PSNR increases, indicating higher quality. While minimizing MSE is important, it's crucial to strike a balance with other factors, such as the nature and sensitivity of the hidden data, as well as the level of distortion that can be tolerated

Challenges you have faced and how you addressed those challenges.

(You may address technical challenges.)

During the course of the project, integrating AES encryption into the steganography process posed some challenges. Incorporating encryption while ensuring seamless data hiding within digital images required careful consideration of various technical aspects.

Challenges Faced:

Integration Complexity: Combining steganography, particularly the LSB method, with AES encryption introduced complexity. Both processes involve manipulating pixel values, and ensuring a harmonious integration demanded meticulous coding.

Key Management: Managing encryption keys, specifically ensuring compatibility with AES while preserving the security of the steganographic process, was a multifaceted challenge. Key size, encoding, and alignment were critical aspects that required careful attention.

Performance Impact: The introduction of AES encryption could potentially impact the performance of the steganographic process. Balancing the need for robust encryption with efficient data hiding without compromising performance was a delicate balancing act.

Addressing Challenges:

Detailed Planning: A comprehensive planning phase was undertaken to outline the integration process. This involved breaking down the tasks into manageable components and designing a systematic approach to address each aspect of the integration.

Key Size Standardization: To manage key-related challenges, a standardization approach was implemented. The system was designed to handle AES keys of a specific size, and input keys were automatically adjusted to meet this requirement.

Optimization: Performance impact was mitigated through optimization techniques. Code was refined to streamline the encryption and steganography processes, ensuring efficient execution without sacrificing security.

Thorough Testing: Rigorous testing was conducted at each stage of integration. This involved using sample images and data with known characteristics to validate the effectiveness of both encryption and steganography. Testing played a crucial role in identifying and resolving integration issues.

By systematically addressing these challenges, we successfully integrated AES encryption into the steganography process, resulting in a cohesive and secure system for data communication within digital images. The challenges encountered during the project served as valuable learning experiences, contributing to the refinement and enhancement of the overall system.

Conclusion

In summary, this project addresses the critical need for secure data transmission within digital images by combining steganography and cryptography. The integration of the least significant bit (LSB) replacement method with the Advanced Encryption Standard (AES) offers a robust defense against data privacy threats. Through random data embedding in RGB images, the project introduces an innovative approach to enhance security.

The significance of this work lies in its comprehensive and efficient solution, providing a practical demonstration of combining steganography and cryptography. The novel techniques introduced contribute to improving the security of the steganographic process. The execution of the project, evidenced by code execution screenshots and performance metrics such as Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR), showcases successful innovation, security, and usability.

This project sets new standards for secure data communication within the digital image processing domain. Despite facing technical challenges, the systematic approach to integration, key management, and optimization ensured successful project execution. In conclusion, the outcomes represent a valuable contribution to advancing methodologies for secure digital image communication.

References:

1. S. Sravani and R. Raniith, "Image Steganography for Confidential Data Communication," 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kharagpur, India, 2021, pp. 01-05, doi: 10.1109/ICCCNT51525.2021.9579814.
https://ieeexplore.ieee.org/document/9579814

2. R. Dumre and A. Dave, "Exploring LSB Steganography Possibilities in RGB Images," 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kharagpur, India, 2021, pp. 1-7, doi: 10.1109/ICCCNT51525.2021.9579588.
https://ieeexplore.ieee.org/document/9579588

3. Z. Abbas and K. T. Chong, "A Novel Approach Towards Fusion of Steganography and Cryptography for Enhanced Data Security using RGB Image," 2023 IEEE International Conference on Electro Information Technology (eIT), Romeoville, IL, USA, 2023, pp. 309-313, doi: 10.1109/eIT57321.2023.10187231.
https://ieeexplore.ieee.org/document/10187231

4. A. Pabbi, R. Malhotra and K. Manikandan, "Implementation of Least Significant Bit Image Steganography with Advanced Encryption Standard," 2021 International Conference on Emerging Smart Computing and Informatics (ESCI), Pune, India, 2021, pp. 363-366, doi: 10.1109/ESCI50559.2021.9396884.
https://ieeexplore.ieee.org/document/9396884

5. M. Kumar, A. Soni, A. R. S. Shekhawat and A. Rawat, "Enhanced Digital Image and Text Data Security Using Hybrid Model of LSB Steganography and AES Cryptography Technique," 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS), Coimbatore, India, 2022, pp. 1453-1457, doi: 10.1109/ICAIS53314.2022.9742942.
https://ieeexplore.ieee.org/document/9742942