Mr. Manohar Nelli V B.E.,M.Tech.
Assistant Professor,
Department of Computer Science,
JNNCE,
Shimoga, India

Chandan P
Student,
Department of Computer Science,
JNNCE,
Shimoga, India

Kantharaj B M
Student,
Department of Computer Science,
JNNCE,
Shimoga, India

Arya patil T
Student,
Department of Computer Science,
JNNCE,
Shimoga, India

Gowtham K
Student,
Department of Computer Science,
JNNCE,
Shimoga, India

***Abstract*— The increase of data communication globally requires secure exchange of private information. Steganography is a common form of information hiding from an unauthorized access. Secret messages can be in different ways and file formats such as: images, texts, audios, and videos. Transmitting secret messages is important for trading private information between different countries without hacking. Adaptive Steganography enables hiding data with variable numbers of bits based on the size of the secret message and the cover image. This paper proposes a new data hiding approach for image steganography based on the human visual properties using adaptive Least Significant Bits (LSB).**

I. INTRODUCTION

Steganography has a rich history that dates back to ancient times. One of the earliest known uses was by the Greeks, who would write messages on wooden tablets and cover them with wax. In the 15th century, Leonardo da Vinci used a similar technique by writing messages in invisible ink. The term "steganography" itself comes from the Greek words "steganos," meaning "covered," and "grapho," meaning "to write." Over the centuries, as communication methods evolved, so did the techniques for hiding information.

II. LITERATURE SURVEAY

"A new data hiding approach for image steganography based on visual color sensitivity" presents an innovative approach to image steganography that leverages human visual sensitivity for data embedding. The method employs a spiral embedding technique, starting from the edges of an image and moving toward the center, which optimizes the use of less perceptible areas for hiding data. Additionally, the study introduces an adaptive Least Significant Bit (LSB) technique that varies based on the color channels of the image, enhancing the robustness and imperceptibility of the hidden information. By aligning the data embedding process with human visual perception, the proposed method aims to improve the effectiveness of steganography in practical applications.

"Steganography in the Era of Deep Learning: A Survey" This survey paper explores the integration of deep learning techniques into modern steganography practices. The authors review various neural network architectures, including autoencoders and Generative Adversarial Networks (GANs), and their applications in enhancing the efficiency and security of steganographic methods. The paper discusses the advantages of using deep learning for both embedding and detecting hidden information, as well as the challenges faced in this evolving field, such as robustness against detection and the need for large datasets. The authors also outline future directions for research, emphasizing the potential of deep learning to revolutionize steganography.

"A Robust and Secure Image Steganography Method Using Neural Networks" This research introduces a robust image steganography method that utilizes deep neural networks (DNNs) for embedding hidden messages within images. The proposed approach focuses on ensuring that the embedded data remains secure against both distortion and detection attempts. By leveraging the capabilities of DNNs, the authors enhance the resilience of the steganographic method, making it difficult for adversaries to extract or alter the hidden information. The paper provides experimental results demonstrating the effectiveness of the method in various scenarios, highlighting its potential for secure communication in sensitive applications.

"Advances in Audio Steganography: Techniques, Applications, and Challenges" This paper reviews the latest advancements in audio steganography, focusing on innovative techniques for embedding information within sound files. The authors discuss various methods, including those that utilize machine learning to enhance the robustness of audio steganography against attacks. The paper also addresses the challenges faced in this domain, such as maintaining audio quality while ensuring the security of the hidden data. By analyzing current trends and future directions, the authors provide a comprehensive overview of the state of audio steganography, emphasizing its applications in secure communication and copyright protection.

"A Survey on Image Steganography and Steganalysis Techniques", This comprehensive survey paper reviews recent advancements in image steganography and steganalysis techniques. The authors provide an in-depth analysis of various image-based methods for hiding information, categorizing them based on their approaches and effectiveness. The paper discusses critical aspects of security, including vulnerabilities and countermeasures against detection. Additionally, the authors explore emerging techniques, particularly those leveraging deep learning for both embedding and detection processes. By synthesizing current research trends and identifying gaps in the literature, this survey serves as a valuable resource for researchers and practitioners seeking to understand the evolving landscape of image steganography and its associated challenges.

III. METHADOLOGY

Image steganography, a technique of hiding secret information within an image, faces challenges in balancing the imperceptibility of the hidden data with the robustness of the steganographic method. The human visual system's varying sensitivity to different colors can be leveraged to develop a more effective data hiding approach. The problem lies in designing a steganographic method that exploits visual color sensitivity to achieve high-capacity data hiding while maintaining the integrity and quality of the cover image.

A. System architecture

Steganography is a technique for securely concealing secret data within cover data, ensuring discreet communication. The process begins with cover data, such as an image, audio file, or text document, which serves as the carrier for the hidden information. Secret data, which can be text, images, or any other type of confidential information, is embedded into the cover data through an embedding process. This process subtly modifies the cover data to incorporate the hidden message without noticeably altering its appearance or functionality, resulting in stego data that looks identical to the original cover data to an untrained observer. The stego data is then transmitted through a communication channel, such as the internet, email, or social media. At the receiving end, the hidden message is retrieved using a specific extracting algorithm. After extraction, the original cover data is typically discarded, as its purpose has been fulfilled.

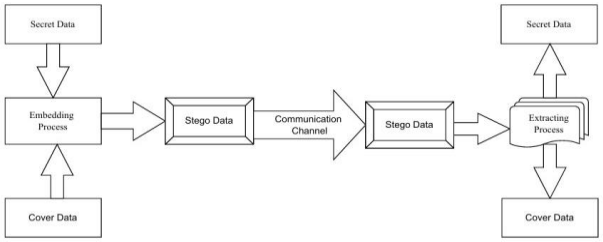

Fig 1: Architecture

B. Steganography Flow Chart

The process of steganography begins by selecting a suitable host image, which could be in formats like JPEG, PNG, or BMP. The choice of the host image is critical as it impacts the capacity to hide data and the visual quality of the resulting stego image.

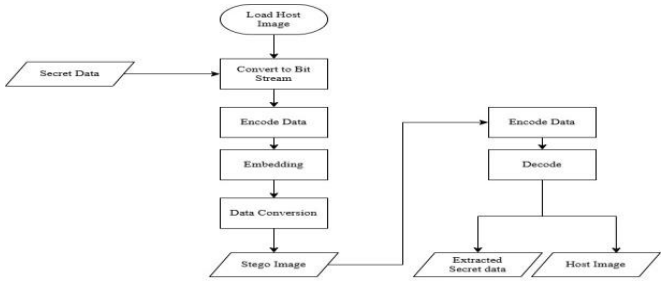

Fig 2: Flowchart

The secret data, whether text, audio, video, or another image, is converted into a bit stream (a sequence of 0s and 1s) as a standard digital data representation step. The data is then encoded using techniques such as Least Significant Bit (LSB) substitution, where the least significant bits of the host image's pixels are replaced with the secret data bits, spread spectrum techniques, which distribute the secret data across multiple pixels to enhance robustness and visual quality, or algorithm-based encoding, involving advanced methods like error-correcting codes or data compression. Following this, the encoded data is embedded into the host image based on the chosen encoding technique. The modified host image, now containing the hidden data, is then converted into a specific format (e.g., JPEG) for storage or transmission. To retrieve the secret data, the stego image is decoded using the same algorithm used for encoding, extracting the hidden bits from the image. These decoded bits are then converted back into the original format of the secret data. Depending on the embedding method and its reversibility, the original host image may or may not be recoverable.

IV. IMPLEMENTATION DETAILS

1. Advanced Encryption Standard (AES):

- A symmetric encryption algorithm operating on fixed 128-bit blocks.
- Supports key lengths of 128, 192, and 256 bits, offering varying levels of security.
- Employs substitution-permutation networks for strong cryptographic protection.
- Widely used in applications like secure communication and cloud storage.

2. Data Encryption Standard (DES):

- A symmetric block cipher with a 56-bit key length, now considered outdated due to susceptibility to brute-force attacks.
- Operates on 64-bit blocks using a 16-round Feistel network.
- Triple DES (3DES) was introduced to enhance DES security but is computationally intensive.

3. Image Adaptive Encryption:

- Encrypts images based on their specific characteristics like pixel intensity or regions of interest.
- Frequently uses chaos theory and selective encryption for efficiency and security.
- Suitable for applications like secure image sharing, medical imaging, and digital forensics.

4. Randomized Encryption:

- Uses randomness (e.g., initialization vectors or random padding) to produce unique ciphertexts for identical plaintexts.
- Reduces vulnerabilities to replay attacks and pattern recognition.
- Commonly used in secure messaging, database encryption, and file systems.

5. **Comparative Security:**

- AES provides stronger security and efficiency compared to DES, which is largely deprecated.
- Image adaptive techniques are specialized but rely heavily on implementation specifics.
- Randomized encryption complements standard methods to improve security under active attacks.

6. **Performance Considerations:**

- AES is computationally efficient for large-scale applications, while DES is slower and less secure.
- Image adaptive encryption's performance varies with the complexity of image features.
- Randomized encryption introduces overhead due to randomness generation and management.

7. **Applications and Challenges:**

- AES and DES are general-purpose algorithms for secure communication and storage.
- Image adaptive encryption is tailored for multimedia security but can be computationally demanding.
- Randomized encryption enhances security but requires careful management of additional randomness parameters.

V. RESULTS

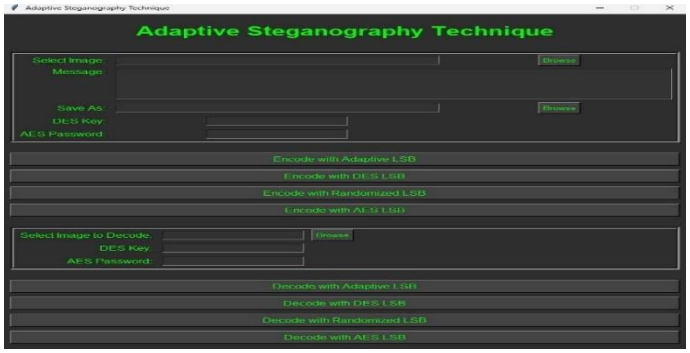

Fig 3: Graphical user interface

In Fig. 3, a GUI is specifically designed for implementing various adaptive steganography techniques. This user-friendly interface allows users to select a host image and input a secret message for embedding. It supports multiple embedding methods, such as adaptive LSB, DES LSB, AES LSB, and randomized LSB, providing versatility in the steganography process. The GUI also includes data encryption options using DES or AES, adding an additional layer of security. Once users configure the desired encoding parameters, they can seamlessly embed the secret message into the selected host image. Additionally, the decoding section enables users to select the stego image and the corresponding decoding method for extracting hidden messages. This comprehensive GUI simplifies the exploration and implementation of advanced steganography approaches, making them accessible to both novice and experienced users. It allows users to experiment with different techniques, enhancing their understanding of the security mechanisms involved in digital data hiding. The GUI's intuitive design ensures a smooth and efficient workflow, making it an ideal tool for applying.

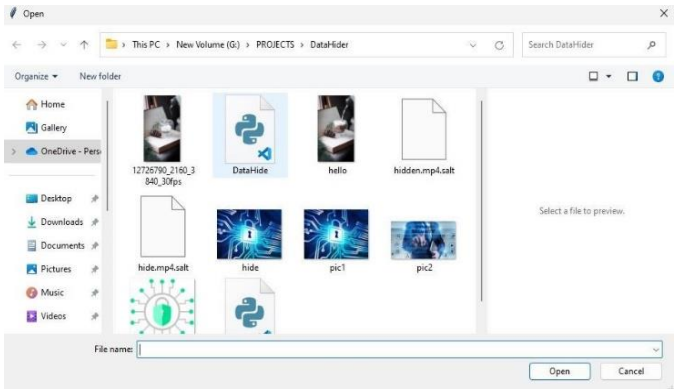

Fig 4: Image selection

In Fig 4 shows a file explorer window in Windows and image will be selected to perform steganography operation.

Fig 5: Entering Secret Message

In Fig 5 depicts that the user has selected an image file "pic1.jpg" as the host image and entered the secret message "Hello JNNCE". They have also specified the path and filename "hidden.png" for saving the resulting stego image. The interface likely provides options for encoding the message using various techniques and saving the output.

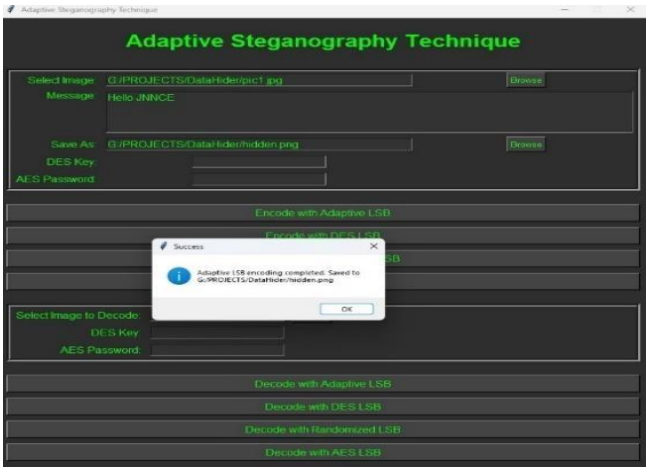

Fig 6: Encoding with adaptive LSB

In Fig 6 shows the GUI of an adaptive steganography tool. It displays a successful encoding message, indicating that the secret message "Hello JNNCE" has been embedded into the image "pic1.jpg" using the Adaptive LSB method. The stego image has been saved as "hidden.png" in the specified location. The interface also provides options for decoding the hidden message using various methods.

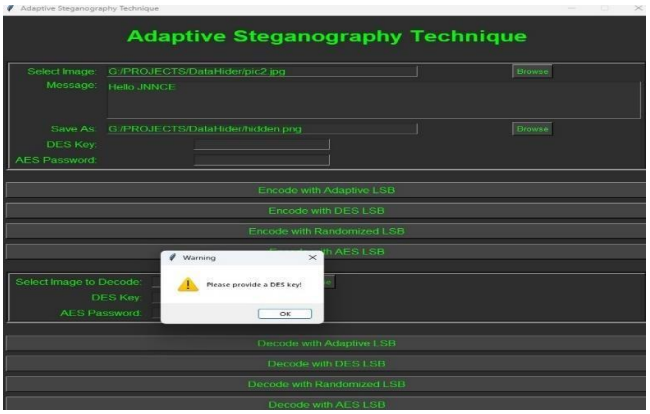

Fig 7: Warning raised

In Fig 7 shows the GUI of an adaptive steganography tool. It displays a warning message stating that a DES key is required for the selected encoding or decoding method. The user needs to provide the correct DES key to proceed with the operation. The interface also offers options for encoding and decoding using various methods, including Adaptive LSB, DES LSB, Randomized LSB, and AES LSB.

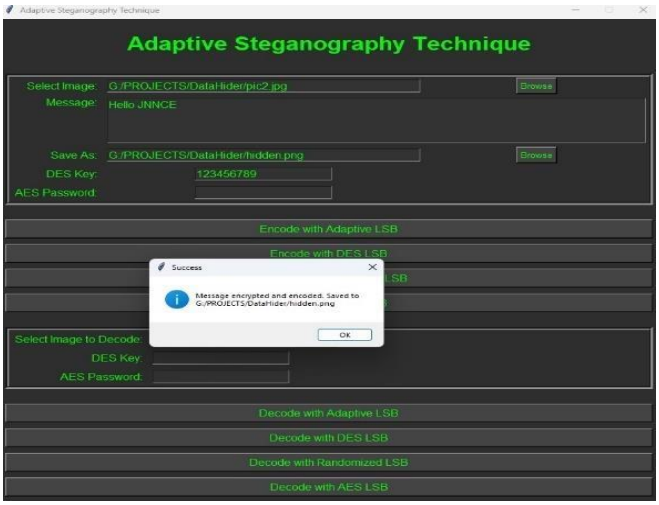

Fig 8: Encryption using DES

In Fig 8 displays a success message indicating that the message "Hello JNNCE" has been successfully encrypted using DES with the provided key (123456789) and then embedded into the image "pic2.jpg". The stego image has been saved as "hidden.png" in the specified location. The interface also offers options for decoding the hidden message using various methods.

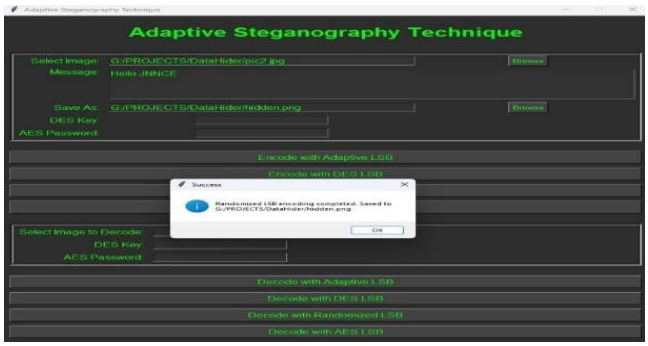

Fig 9: Encryption with Randomized LSB

In fig 9 shows the GUI of an adaptive steganography tool. A successful encoding message is displayed, indicating that the secret message "Hello JNNCE" has been embedded into the image "pic2.jpg" using the Randomized LSB method. The stego image has been saved as "hidden.png" in the specified location. The interface also provides options for decoding the hidden message using various methods.

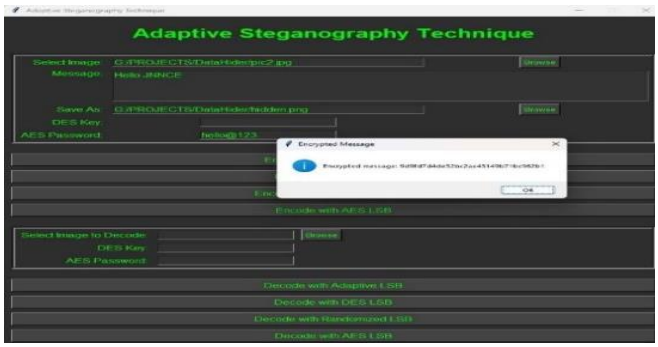

Fig 10: AES Encryption

In fig 10 displays a success message indicating that the message "Hello JNNCE" has been successfully encrypted using AES with the provided password "hello@123".

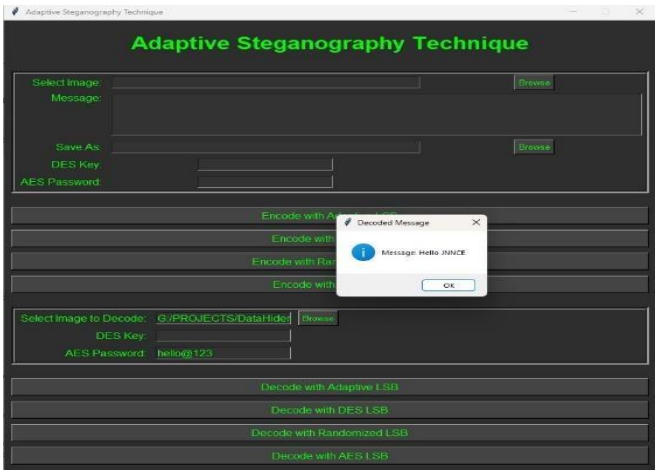

Fig 11: AES decryption

In fig 11 shows the GUI of an adaptive steganography tool. It displays a successful decoding message. The hidden message "Hello JNNCE" has been successfully extracted from the stego image using AES decryption with the provided password "hello@123".

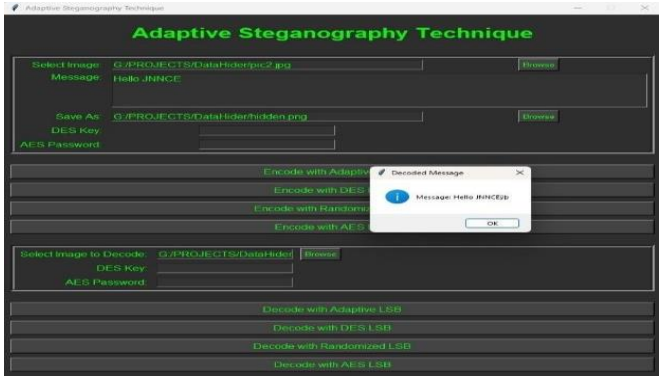

Fig 12: Decryption with adaptive LSB

In fig 12 displays a successful decoding message. The hidden message "Hello JNNCE" has been successfully

extracted from the stego image using the Adaptive LSB method. The interface also offers options for encoding and decoding using various methods, including DES LSB, Randomized LSB, and AES LSB.

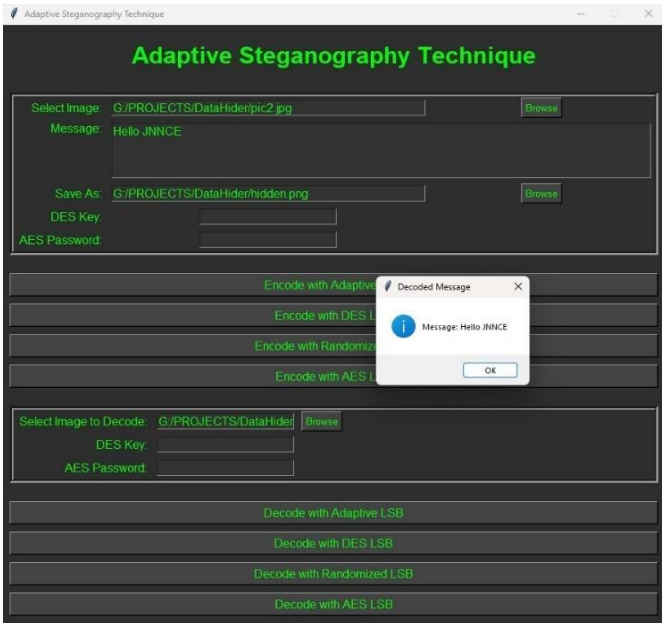

Fig 13: Decryption with Randomized LSB

Figure 13 shows the GUI of an adaptive steganography tool. A successful encoding message is displayed, indicating that the secret message "Hello JNNCE" has been embedded into the image "pic2.jpg" using the Randomized LSB method. The stego image has been saved as "hidden.png" in the specified location. The interface also provides options for decoding the hidden message using various methods.

VI. CONCLUSION

Our steganography project effectively combines image processing, encryption, and data embedding techniques to securely hide and retrieve messages within images. By utilizing various encoding methods, such as Adaptive Least Significant Bit (LSB) encoding, Randomized LSB encoding, and cryptographic techniques using DES and AES encryption, the system ensures both data concealment and message security. The LSB method hides messages in the least significant bits of image pixels, while the randomized LSB adds an extra layer of security by selecting random pixel positions for embedding. The use of DES and AES encryption further secures the message, making it unreadable without the correct decryption key or password. The project provides a user-friendly graphical user interface (GUI) built using Tkinter, allowing users to easily load images, input messages, and select from various encoding and encryption methods. This makes it accessible to users without requiring in-depth technical knowledge. The system is designed to handle both encoding and decoding tasks, making it a versatile tool for secure communication. Users can encode messages in images and then decode them with the appropriate keys, ensuring confidentiality and privacy. While the project offers a range of encoding techniques, there are areas for improvement. For instance, the system may encounter limitations when dealing with larger messages due to the pixel constraints of the images. Additionally, more advanced error handling mechanisms could be implemented to address edge cases and improve the user experience. Future enhancements could also include message compression before embedding to optimize space usage and allow larger payloads. Overall, this steganography project provides a solid foundation for secure communication using images, highlighting the importance of combining encryption and data embedding for protecting sensitive information in digital form. It is a practical tool for those interested in secure messaging, digital watermarking, and data protection.

REFERENCES

[1] "A new data hiding approach for image steganography based on visual color sensitivity" by Ashraf AbdelRaouf.

[2] "Information Hiding: Steganography and Watermarking Attacks and Countermeasures" by Neil F. Johnson, Sushil Jajodia.

[3] "A Survey of Steganographic Techniques" by M. S. E. R. K. Reddy et al. (2012) – A detailed survey of various steganographic methods and the challenges in the field.

[4] "An Overview of Image Steganography Techniques" by Vijay Kumar, and Ram Rattan Yadav (2019) – Reviews image-based steganographic techniques, comparing their effectiveness and vulnerabilities.

[5] "Steganography: A Survey of the Art of Information Hiding" by Jessica Fridrich, Miroslav Goljan, and David Hogrefe – A seminal paper that provides insights into different steganographic methods, especially in the context of digital media.

[6] "Deep Learning-Based Steganography and Anti-Detection" by authors such as X. Xu, L. Zhang, and others – Explores the role of machine learning and neural networks in creating advanced steganographic techniques.

[7] "A New Approach for Digital Image Steganography using Pixel-Value Differencing" by M. B. Khargharia and S. K. Sood – Introduces novel methods based on pixel differences for embedding secret messages in images "Books on Cryptography and Information"

[8] "Security Cryptography and Network Security" by William Stallings – Provides foundational knowledge in cryptography, often used in conjunction with steganography in secure communications.

[9] "Applied Cryptography" by Bruce Schneier – Offers a comprehensive understanding of cryptographic protocols, which is often relevant when discussing steganography in secure systems.