Secure Chat Application Using End-To-End Encryption and Steganography

Dr. T. Sunil Kumar[1], Bagath Lokesh[2], Tarra Jogi Naidu[3], Shaik Sameer[4], Chikati Vamsi[5]
[1]*Professor, Dept of Computer Science and Engineering (CSE), Sanketika Institute of Technology and Management, Visakhapatnam, Andhra Pradesh, India*
[2,3,4,5]*Student, Dept of Computer Science and Engineering (CSE), Sanketika Institute of Technology and Management, Visakhapatnam, Andhra Pradesh, India*

***Abstract*—In the modern digital era, secure communication has become a critical requirement due to the increasing risk of cyber threats such as data interception, eavesdropping, and unauthorized access. Traditional messaging systems primarily rely on encryption to protect message content; however, they often fail to conceal the existence of communication, making them vulnerable to traffic analysis and targeted attacks. To address these challenges, this paper presents a secure chat application that integrates end-to-end encryption with image steganography to provide enhanced communication privacy and data protection. In the proposed system, messages are encrypted at the sender's end using a symmetric cryptographic algorithm, ensuring that only the intended receiver can decrypt and access the original content. The encrypted message is then embedded within a digital image using the Least Significant Bit (LSB) steganography technique, effectively concealing the presence of the message during transmission. At the receiver's end, the hidden data is extracted from the image and decrypted to reconstruct the original message. The implementation is carried out using Python and Flask for backend development, along with HTML, CSS, and JavaScript for the user interface. Experimental results demonstrate that the proposed system successfully ensures message confidentiality while simultaneously hiding communication, thereby providing a dual-layer security mechanism. The integration of cryptography and steganography significantly enhances the security of digital messaging systems and reduces the risk of detection and unauthorized access.**

***Index Terms*—Secure Communication, End-to-End Encryption (E2EE), Image Steganography, Cryptography, Data Hiding, Least Significant Bit (LSB), Secure Chat Application**

I. INTRODUCTION

The advancement of internet technologies and the widespread adoption of digital communication platforms have significantly changed the way individuals exchange information. Messaging applications are now an integral part of daily life, supporting communication in personal, academic, and professional environments. Despite their convenience, these platforms are increasingly exposed to security threats such as unauthorized access, data interception, and message tampering. As a result, ensuring secure and private communication has become a critical requirement in modern information systems.

Most existing messaging systems rely on encryption techniques to protect the content of transmitted messages. End-to-end encryption, in particular, ensures that only the sender and the intended receiver can access the message, preventing intermediaries from viewing the data. However, while encryption effectively protects the content, it does not conceal the existence of communication. Encrypted messages can still be identified during transmission, which may attract attention from attackers and make the system vulnerable to traffic analysis and targeted attacks. This highlights a significant limitation in traditional secure communication approaches.

To overcome this limitation, it is important to adopt additional techniques that not only secure the message content but also hide the presence of communication. Steganography offers a practical solution by embedding secret data within digital media such as images, making the communication appear normal

and less suspicious. When combined with encryption, steganography provides an additional layer of protection by concealing encrypted data within a cover medium.

The motivation for this work arises from the need to enhance communication security beyond conventional encryption-based methods. With the increasing volume of sensitive information being exchanged over digital platforms, there is a growing demand for systems that can ensure both confidentiality and invisibility of communication. Integrating cryptographic techniques with steganographic methods can significantly reduce the risk of detection and unauthorized access.

In this paper, a secure chat application is proposed that combines end-to-end encryption with image steganography. The system encrypts the user's message and embeds it into an image using the Least Significant Bit technique before transmission. At the receiver's end, the hidden data is extracted and decrypted to retrieve the original message. The main objective of this work is to develop a communication system that provides dual-layer security by protecting both the content and the existence of messages. The proposed approach aims to improve privacy, enhance data protection, and demonstrate the practical application of combined security techniques in modern communication systems.

II. LITERATURE REVIEW

The problem of fraud detection in online financial systems has been widely explored due to the rapid growth of digital transactions and the increasing risk of cyber fraud. Early research in this field primarily focused on rule-based detection systems, where predefined rules and thresholds were used to identify suspicious transactions. These systems typically monitored parameters such as transaction amount, frequency, and unusual account activity. Although these approaches were simple and easy to implement, they lacked the ability to adapt to new and evolving fraud patterns.

With advancements in data analysis, researchers introduced machine learning techniques to improve fraud detection accuracy. Supervised learning algorithms such as Logistic Regression, Decision Trees, Random Forest, and Support Vector Machines have been widely used to classify transactions based on historical data. These models are capable of learning patterns from large datasets and can identify complex relationships between transaction features. In addition, deep learning methods, particularly Artificial Neural Networks, have been applied to capture non-linear patterns and enhance predictive performance.

Another important approach in existing research is anomaly detection, which focuses on identifying deviations from normal transaction behavior. These methods analyze user activity patterns and flag transactions that differ significantly from expected behavior. Techniques such as clustering, statistical analysis, and outlier detection have been used for this purpose. Furthermore, modern systems have started integrating real-time monitoring and alert mechanisms to notify users about suspicious activities immediately.

Despite these advancements, several limitations still exist in current fraud detection systems. Many machine learning models require large amounts of labeled data for training, which may not always be available. The issue of class imbalance, where fraudulent transactions are much fewer than legitimate ones, can also affect model performance. Additionally, existing systems may generate false positives, incorrectly identifying normal transactions as fraudulent, which can reduce user trust. Some systems focus on detecting fraud after the transaction has been completed rather than preventing it in real time. These limitations highlight the need for more efficient, adaptive, and real-time fraud detection approaches.vgvg

The need for secure communication has led to extensive research in the fields of cryptography and information hiding. Cryptography has long been considered a fundamental technique for protecting data confidentiality. Early principles such as Kerckhoffs' assumption emphasized that the security of a system should depend on the secrecy of the key rather than the algorithm itself [19]. Over time, modern cryptographic systems have evolved to include both symmetric and asymmetric techniques. Symmetric encryption methods provide efficient data

protection, while public key cryptography introduced by Diffie and Hellman [8] and later extended by Rivest, Shamir, and Adleman [9] addressed the challenges of secure key exchange and authentication. Comprehensive studies on cryptographic algorithms and protocols have further strengthened the foundation of secure communication systems [1], [7].

Despite the effectiveness of cryptography in protecting message content, it does not conceal the presence of communication. Encrypted data can still be detected during transmission, which may attract attention and lead to further analysis. This limitation has motivated the exploration of steganography as a complementary approach. Steganography focuses on hiding the existence of information by embedding it within digital media. Early work by Simmons introduced the concept of covert communication channels, highlighting the importance of hiding information in plain sight [17]. Subsequent research has provided a broader understanding of steganographic techniques and their applications in secure communication [2], [4].

Image steganography has gained particular importance due to the widespread use of digital images and their ability to carry hidden information without noticeable distortion. Techniques such as the Least Significant Bit method allow data to be embedded efficiently while maintaining visual quality [15]. More advanced approaches, including transform-based techniques, have been developed to improve robustness and resistance to detection [3], [10]. Detailed surveys and analyses have demonstrated the effectiveness of these methods while also identifying potential vulnerabilities in steganographic systems [16].

However, steganography alone does not provide sufficient protection for message content. If the hidden data is extracted, it can be easily interpreted unless it is encrypted. Researchers have therefore explored the integration of cryptography and steganography to achieve enhanced security. Hybrid approaches combine the strengths of both techniques by encrypting the message before embedding it within a cover medium, thereby ensuring both confidentiality and concealment [12], [18]. These methods significantly reduce the likelihood of detection and unauthorized access.

In addition to the development of secure embedding techniques, several studies have examined the limitations and potential attacks on steganographic systems. Research has shown that poorly designed steganographic methods can be vulnerable to statistical analysis and detection techniques [5], [6]. Information-theoretic models have also been proposed to evaluate the security and capacity of steganographic systems [11], providing a theoretical foundation for designing more robust solutions. Furthermore, specialized forms of steganography, such as linguistic steganography, have been explored to extend data hiding techniques beyond image-based methods [13].

Recent advancements have focused on improving the robustness, efficiency, and applicability of secure communication systems by integrating multiple security mechanisms. Techniques such as visual cryptography have also been introduced to enhance data protection through innovative encoding schemes [14]. Additionally, standardization efforts and terminology definitions have contributed to a more structured understanding of information hiding techniques [20].

From the analysis of existing literature, it is evident that both cryptography and steganography play crucial roles in secure communication. However, many existing systems rely primarily on a single technique, either protecting the message content or hiding its existence. There is a clear need for integrated solutions that combine these approaches within practical communication platforms. The proposed system addresses this gap by implementing a secure chat application that utilizes both end-to-end encryption and image steganography, thereby providing a comprehensive solution for secure and private communication.

III. PROPOSED SYSTEM

A.System Overview

The proposed system is designed to enhance communication security by integrating end-to-end encryption with image-based steganography. The

objective is to ensure that the message remains confidential while also concealing its existence during transmission. Unlike traditional messaging systems that rely only on encryption, the proposed approach introduces an additional security layer by embedding encrypted messages within digital images.

In this system, users interact through a web-based chat interface. When a message is entered by the sender, it is first encrypted using a symmetric encryption technique. The encrypted message is then embedded into a digital image using the Least Significant Bit (LSB) method. The generated image appears visually similar to the original image and does not reveal the presence of hidden data. At the receiver's end, the hidden message is extracted from the image and decrypted to obtain the original content.
This combination of encryption and steganography provides a dual-layer security mechanism, improving both confidentiality and communication privacy.

B.System Architecture
The architecture of the proposed system consists of multiple modules that work together to ensure secure message transmission. These modules include the user interface, authentication module, encryption module, steganography module, communication server, extraction module, and decryption module.

Initially, the user logs into the system through the authentication module, which verifies credentials and restricts access to authorized users. Once authenticated, the sender composes a message through the chat interface. The message is processed by the encryption module, where it is converted into ciphertext. This encrypted data is then passed to the steganography module, which embeds it into an image using the LSB technique.

The resulting stego image is transmitted through the communication server to the receiver. Upon receiving the image, the extraction module retrieves the hidden encrypted data, which is then decrypted using the appropriate key to recover the original message.
The overall system architecture is illustrated in Fig. 1.

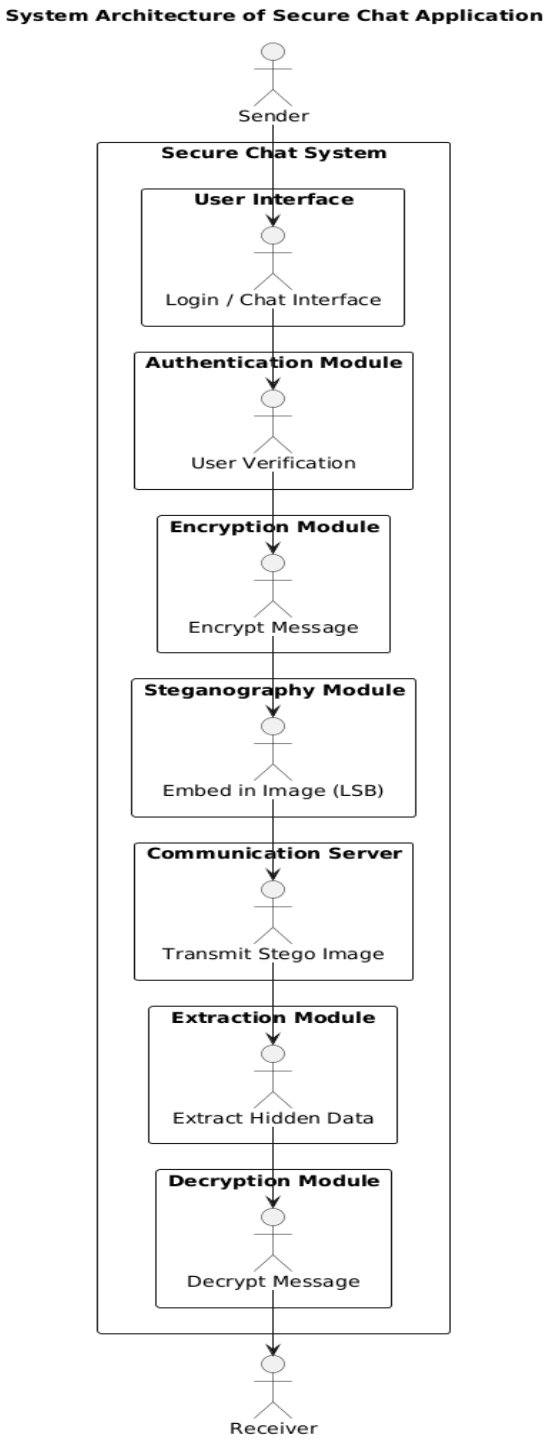

Fig. 1. System architecture of the proposed secure chat application

C. Workflow of the Proposed System
The operation of the proposed system follows a structured sequence of steps to ensure secure communication between users:

- The user logs into the system using valid credentials.
- The sender composes a message through the chat interface.
- The message is encrypted using a symmetric encryption algorithm.
- The encrypted message is converted into binary form.
- The steganography module embeds the encrypted data into an image using the LSB technique.
- The generated stego image is transmitted to the receiver.
- The receiver accesses the received image.
- The system extracts the hidden encrypted data from the image.
- The extracted data is decrypted using the appropriate key.
- The original message is displayed to the receiver.

This workflow ensures that the communication remains secure at every stage, protecting both the content and the presence of the message.

The workflow of the proposed system is shown in Fig. 2.

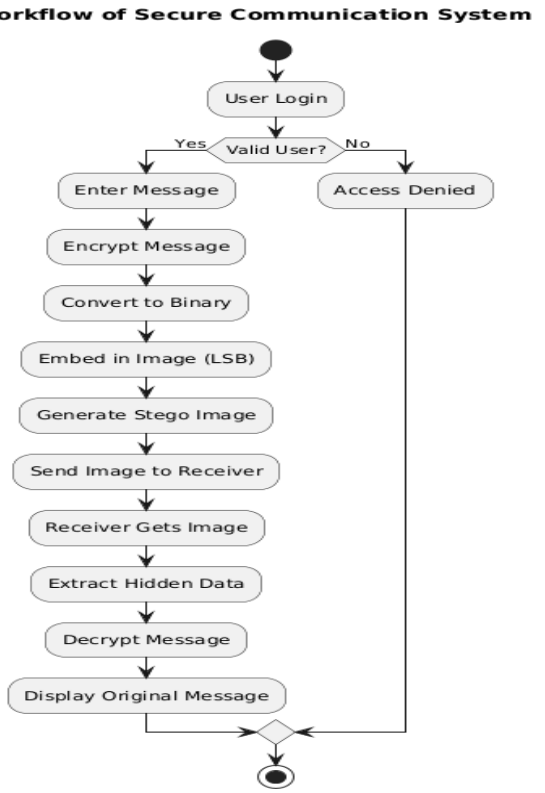

Fig. 2. Workflow of the proposed secure communication system

IV. METHODOLOGY

Encryption Algorithm

In the proposed system, message confidentiality is ensured using a symmetric encryption approach. The plaintext message entered by the sender is transformed into an unreadable format before transmission. A shared secret key is used for both encryption and decryption processes, ensuring that only authorized users can access the original content.

The encryption process begins by accepting the input message from the user. This message is then processed using an encryption function along with a secret key. The output of this process is ciphertext, which appears as random data and cannot be interpreted without the correct key. This ciphertext is then forwarded to the steganography module for embedding within an image.

Algorithm Steps:

1. Input the plaintext message P
2. Generate or obtain the secret key K
3. Apply encryption function to obtain ciphertext
4. Convert ciphertext into binary format
5. Pass encrypted data to the steganography module

This process ensures that even if the data is intercepted, it remains unreadable without the corresponding decryption key.

Steganography Algorithm

The encrypted message is concealed within an image using the Least Significant Bit (LSB) steganography technique. This method modifies the least significant bits of pixel values to store hidden data without causing noticeable changes to the image.

The process begins by selecting a cover image that will carry the hidden message. The encrypted message is converted into a binary sequence, which is then embedded into the pixel values of the image. Since only the least significant bits are altered, the visual quality of the image remains nearly unchanged.

Algorithm Steps:

1. Select a cover image I
2. Receive encrypted binary data M
3. Extract pixel values from the image
4. Replace least significant bits of pixels with message bits
5. Generate stego image I'

6. Transmit stego image to the receiver

At the receiver's side, the reverse process is performed to extract the hidden data and recover the encrypted message.

Mathematical Model

The proposed system combines cryptographic transformation and data hiding techniques, which can be represented mathematically.

Encryption Model:

$C = E(K, P)$

$P = D(K, C)$

where:

- P= Plaintext message
- C= Ciphertext
- K= Secret key
- E= Encryption function
- D= Decryption function

This model ensures that only users possessing the correct key can retrieve the original message.

Steganography Model (LSB):

$I' = (I \ \& \sim 1) \mid M$

where:

- $I = Original\ pixel\ value$
- $M = Message\ bit\ (0\ or\ 1)$
- I' = Modified pixel value (stego pixel)

This operation replaces the least significant bit of the pixel with the message bit, allowing data to be hidden within the image.

Combined Security Model:

$I' = S\big(E(K, P)\big)$

$P = D(K, S^{-1}(I'))$

where:

- $S = Steganography\ embedding\ function$
- S^{-1}= Extraction function

This combined model represents the dual-layer security mechanism of the system, where encryption protects the message content and steganography conceals its presence.

V. RESULTS AND DISCUSSION

The results obtained from the implementation of the proposed secure chat application demonstrate its effectiveness in providing both message confidentiality and communication concealment. The system was evaluated under different scenarios to verify its functionality, reliability, and security. The integration of encryption and steganography techniques was tested to ensure that messages are securely processed, transmitted, and retrieved without loss or exposure of sensitive information.

To validate the correctness of the system, a series of test cases were executed covering all major modules, including user authentication, message encryption, steganographic embedding, message transmission, data extraction, and message decryption. The system successfully allowed authorized users to log in and prevented unauthorized access attempts. Messages entered by the sender were correctly encrypted and converted into an unreadable format before embedding. The steganography module effectively embedded the encrypted data into the selected image without producing visible distortion. The generated stego image was transmitted successfully to the receiver, where the system accurately extracted the hidden data and decrypted it to reproduce the original message. These observations confirm that all components of the system operate correctly and are well integrated.

The graphical outputs generated during system execution further illustrate the functionality of the application. The login and registration interfaces provide secure access to the system, ensuring that only valid users can participate in communication. The chat interface allows users to input messages and select images for embedding, offering a simple and user-friendly experience. The encryption output demonstrates the transformation of plaintext into ciphertext, while the steganography output shows the generation of the stego image containing the hidden message. At the receiver's end, the extraction process retrieves the embedded data, and the decryption module reconstructs the original message accurately. These output screens provide visual confirmation of the secure communication process.

The output screens of the implemented system are shown in Fig. 3, Fig. 4, Fig. 5, and Fig. 6.

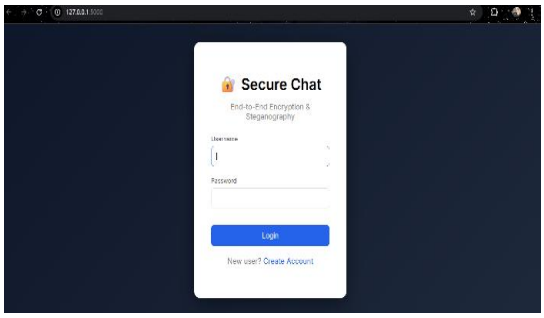

Fig. 3. User authentication interface

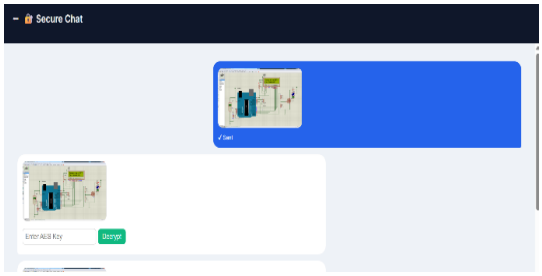

Fig. 4. Chat interface for message input and transmission

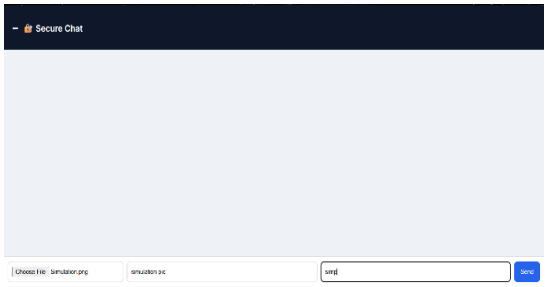

Fig. 5. Stego image containing hidden encrypted message

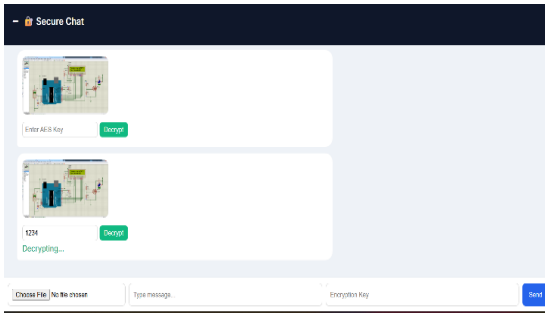

Fig. 6. Retrieved message after extraction and decryption

The performance of the system was analyzed in terms of processing efficiency, security strength, and usability. The encryption process was executed with minimal delay, ensuring that the system remains responsive during communication. The LSB-based steganography technique required low computational overhead and did not significantly affect the quality of the image, making it suitable for practical implementation. The extraction and decryption processes were also performed efficiently, allowing the receiver to obtain the original message without noticeable delay. From a security perspective, the dual-layer approach enhances protection by ensuring that even if the image is intercepted, the hidden message remains difficult to detect and cannot be understood without the decryption key.

Overall, the results indicate that the proposed system successfully achieves its objective of providing secure communication. The combination of encryption and steganography improves both data confidentiality and communication privacy, making the system more robust compared to traditional messaging approaches that rely solely on encryption.

VI. CONCLUSION

In this paper, a secure chat application integrating end-to-end encryption and image steganography has been presented to enhance the privacy and security of digital communication. The proposed system addresses the limitations of conventional messaging approaches by not only protecting the content of the message through encryption but also concealing its existence using steganographic techniques. This dual-layer security mechanism reduces the risk of interception, detection, and unauthorized access during message transmission.

The implementation of the system demonstrates that encrypted messages can be effectively embedded within digital images without causing noticeable changes to image quality. The use of the Least Significant Bit technique enables efficient data hiding, while the encryption process ensures that the message remains unintelligible without the appropriate key. At the receiver's end, the system successfully extracts and decrypts the hidden data, confirming the reliability and correctness of the communication process.

The experimental results indicate that the proposed approach provides a practical and secure solution for modern communication systems. The integration of cryptography and steganography enhances both confidentiality and communication privacy, making

the system more robust compared to traditional methods that rely solely on encryption. Overall, the developed application demonstrates the effectiveness of combining multiple security techniques to build a reliable and secure messaging platform suitable for real-world applications.

VII. FUTURE WORK

Although the proposed secure chat application demonstrates effective integration of encryption and steganography for enhancing communication security, several improvements can be considered to further extend its capabilities. One potential direction is the adoption of more advanced steganographic techniques such as transform domain methods, including Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). These approaches can provide improved robustness against image processing operations and steganalysis attacks, thereby strengthening the security of hidden data.

Another area for enhancement is the implementation of more sophisticated key management mechanisms. The current system uses a symmetric encryption approach, which may be extended by incorporating secure key exchange protocols such as public key cryptography or Diffie–Hellman key exchange. This would improve the overall security of the system, particularly in scenarios involving multiple users or distributed communication environments.

The system can also be expanded to support additional media formats for data hiding, such as audio and video files. This would increase flexibility and allow users to choose different communication channels based on their requirements. Furthermore, developing a mobile application version of the system would improve accessibility and usability, enabling secure communication on portable devices.

Future work may also include the integration of advanced authentication mechanisms, such as multi-factor authentication or biometric verification, to enhance user security. In addition, deploying the system on a cloud-based infrastructure could improve scalability and enable the application to handle a larger number of users efficiently.

Overall, these enhancements would strengthen the robustness, scalability, and practicality of the proposed system, making it more suitable for real-world secure communication applications.

REFERENCES

[1] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed. Harlow, U.K.: Pearson Education, 2017.

[2] N. Provos and P. Honeyman, “Hide and seek: An introduction to steganography,” *IEEE Secur. Privacy*, vol. 1, no. 3, pp. 32–44, May–Jun. 2003.

[3] J. Fridrich, *Steganography in Digital Media: Principles, Algorithms, and Applications*. Cambridge, U.K.: Cambridge Univ. Press, 2009.

[4] M. Johnson and S. Jajodia, “Exploring steganography: Seeing the unseen,” *Computer*, vol. 31, no. 2, pp. 26–34, 1998.

[5] A. Westfeld and A. Pfitzmann, “Attacks on steganographic systems,” in *Proc. 3rd Int. Workshop Information Hiding*, 1999, pp. 61–76.

[6] R. Anderson and F. A. P. Petitcolas, “On the limits of steganography,” *IEEE J. Sel. Areas Commun.*, vol. 16, no. 4, pp. 474–481, May 1998.

[7] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd ed. New York, NY, USA: Wiley, 1996.

[8] W. Diffie and M. Hellman, “New directions in cryptography,” *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, Nov. 1976.

[9] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[10] S. Katzenbeisser and F. A. P. Petitcolas, *Information Hiding Techniques for Steganography and Digital Watermarking*. Norwood, MA, USA: Artech House, 2000.

[11] C. Cachin, “An information-theoretic model for steganography,” in *Proc. 2nd Int. Workshop Information Hiding*, 1998, pp. 306–318.

[12] J. Kahn, “Secure communication through encryption and data hiding techniques,” *IEEE Commun. Mag.*, vol. 40, no. 10, pp. 102–107, Oct. 2002.

[13] K. Bennett, “Linguistic steganography: Survey, analysis, and robustness concerns for hiding information in text,” Purdue Univ., West Lafayette, IN, USA, Tech. Rep., 2004.

[14] M. Naor and A. Shamir, “Visual cryptography,” in *Advances in Cryptology—EUROCRYPT*, Berlin, Germany: Springer, 1994, pp. 1–12.

[15] T. Morkel, J. H. P. Eloff, and M. S. Olivier, "An overview of image steganography," in *Proc. Inf. Secur. South Africa Conf.*, 2005.

[16] A. Cheddad, J. Condell, K. Curran, and P. McKevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Process.*, vol. 90, no. 3, pp. 727–752, 2010.

[17] G. J. Simmons, "The prisoners' problem and the subliminal channel," in *Advances in Cryptology*, Berlin, Germany: Springer, 1984, pp. 51–67.

[18] P. Wayner, *Disappearing Cryptography: Information Hiding—Steganography and Watermarking*. San Francisco, CA, USA: Morgan Kaufmann, 2002.

[19] A. Kerckhoffs, "La cryptographie militaire," *J. Sci. Militaires*, vol. 9, pp. 5–38, 1883.

[20] B. Pfitzmann, "Information hiding terminology: Results of an international workshop," *Lecture Notes Comput. Sci.*, Berlin, Germany: Springer, 1996.