iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** III **Month of publication:** March 2026

DOI: https://doi.org/10.22214/ijraset.2026.78275

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

Stegcrypt+ :A Hybrid Cryptographic and Adaptive Steganographic Secure Communication System

Nidhin Dev D[1], Pavin S Kumar[2], Rohith Sabu[3], Sayujya Nandabal[4], Sulthana S S[5], Radhika S M[6]
[1, 2, 3, 4, 5]*Department of Computer Science and Engineering, Rajadhani Institute of Engineering and Technology, Trivandrum, Kerala, India*
[6]*Assistant Professor, Department of Computer Science and Engineering, Rajadhani Institute of Engineering and Technology, Trivandrum, Kerala, India*

Abstract: ***The rapid growth of digital communication technologies has significantly transformed the way information is exchanged across the world. However, the increasing reliance on online communication platforms has also introduced serious concerns related to data privacy, unauthorized interception, and cyber espionage. Conventional cryptographic techniques are widely used to secure communication channels by transforming readable messages into encrypted ciphertext. Although encryption ensures that unauthorized entities cannot interpret the transmitted information, it does not conceal the presence of sensitive communication itself. The visibility of encrypted traffic may attract attention from attackers and surveillance systems, potentially exposing the communication to further analysis or targeted attacks. To address this challenge, this research proposes StegCrypt+, a hybrid secure communication framework that integrates cryptographic encryption with adaptive steganographic techniques to provide both confidentiality and concealment of information.***

The proposed system utilizes Advanced Encryption Standard in Galois/Counter Mode (AES-GCM) to perform secure symmetric encryption of messages. AES-GCM provides authenticated encryption, ensuring that the confidentiality, integrity, and authenticity of the transmitted message are preserved. To facilitate secure key exchange between communicating parties, RSA public key cryptography is used to encrypt the symmetric AES key. This ensures that only the intended recipient can decrypt and access the message content. Once the encryption process is completed, the encrypted ciphertext is embedded within digital images using an adaptive Least Significant Bit (LSB) steganography technique. Unlike conventional static embedding methods, the adaptive approach dynamically adjusts the embedding depth according to the complexity and texture characteristics of the cover image. This approach improves payload capacity while maintaining high visual quality and minimizing the possibility of detection through steganalysis.

The backend of the system is implemented using the Flask web framework, which performs cryptographic processing, steganographic embedding and extraction, and the calculation of image quality metrics such as Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), and Mean Squared Error (MSE). These metrics provide quantitative evaluation of the visual quality of stego-images and help ensure that the embedded data does not introduce noticeable distortion. The frontend of the application is developed using Flutter, providing a cross-platform graphical user interface that allows users to perform secure messaging operations including encryption, embedding, extraction, and decryption. Experimental evaluation demonstrates that the proposed system achieves strong security, high imperceptibility, and efficient communication performance. StegCrypt+ therefore offers a robust solution for covert communication in sensitive environments such as military communication systems, corporate information exchange, investigative journalism, and personal privacy protection.

Keywords: Steganography, Cryptography, AES-GCM, RSA, Secure Communication, Adaptive LSB, Information Security

I. INTRODUCTION

In the modern digital era, information exchange through online communication platforms has become an integral part of everyday life. Individuals, organizations, and governments rely heavily on digital networks to share sensitive information across geographical boundaries. While this rapid advancement in communication technologies has greatly improved connectivity and efficiency, it has also introduced new challenges related to data security and privacy. Cyber threats such as data interception, unauthorized access, digital surveillance, and cyber espionage have become increasingly common, highlighting the need for advanced security mechanisms to protect confidential information during transmission.

Traditional security mechanisms primarily rely on cryptographic techniques to ensure the confidentiality of transmitted data. Cryptography works by transforming plaintext messages into encrypted ciphertext using mathematical algorithms and secret keys.

Only authorized parties possessing the appropriate decryption key can convert the ciphertext back into its original readable form. While cryptographic methods such as AES and RSA provide strong protection against unauthorized data access, they do not hide the presence of encrypted communication. Encrypted messages can still be detected by network monitoring systems or attackers who may attempt cryptanalysis or traffic analysis to compromise the communication channel.

To overcome these limitations, researchers have explored the integration of cryptography with steganography. Steganography is the art of hiding information within seemingly harmless digital media such as images, audio files, or videos. Unlike cryptography, which focuses on protecting the content of the message, steganography aims to conceal the existence of the message itself. By combining these two techniques, it becomes possible to create a multi-layered security framework in which messages are both encrypted and hidden within ordinary media files. This significantly increases the difficulty for attackers to detect or compromise the communication.

StegCrypt+ is designed as an advanced hybrid secure communication system that integrates modern cryptographic techniques with adaptive steganographic embedding. In this system, messages are first encrypted using AES-GCM, which provides strong encryption along with authentication and integrity verification. The symmetric encryption key is then securely exchanged using RSA public-key cryptography, ensuring that only the intended recipient can decrypt the message. After encryption, the ciphertext is embedded into digital images using an adaptive Least Significant Bit steganography technique that intelligently adjusts the embedding depth according to the characteristics of the image.

The system follows a client–server architecture in which a Flask-based backend performs cryptographic processing, steganographic operations, and data management, while a Flutter-based frontend provides an intuitive user interface for secure communication. By combining encryption and steganography into a single integrated platform, StegCrypt+ provides a robust solution for secure and covert communication in modern digital environments.

II. RELATED WORK

Numerous research studies have explored the integration of cryptography and steganography to enhance data security. Traditional encryption methods such as DES, AES, and RSA have been widely used to secure digital communication. However, these methods only protect the content of messages and do not conceal the presence of encrypted communication.

Several steganographic techniques have been proposed to hide data within multimedia files. The Least Significant Bit (LSB) technique is one of the most widely used methods for image steganography due to its simplicity and high payload capacity. However, traditional LSB methods may introduce noticeable distortion or become vulnerable to statistical detection.

Advanced approaches have attempted to improve steganography using techniques such as Discrete Wavelet Transform (DWT), pixel disparity analysis, and alpha blending. These methods improve robustness but often increase computational complexity.

Hybrid security systems combining cryptography and steganography have shown promising results. By encrypting data before embedding it into media files, such systems provide both data confidentiality and communication concealment. However, many existing systems lack adaptability in embedding strategies or do not evaluate image quality metrics.

StegCrypt+ addresses these limitations by combining AES-GCM encryption, RSA key exchange, and adaptive LSB steganography, along with image quality evaluation metrics such as PSNR, SSIM, and MSE.

III. SYSTEM ARCHITECTURE

The StegCrypt+ system is designed using a client–server architecture that separates the user interface from the computational processes responsible for encryption, steganographic embedding, and secure message transmission. This architectural design improves modularity, scalability, and maintainability while ensuring that security-sensitive operations are handled within a controlled backend environment.

The frontend of the system is implemented using the Flutter framework, which provides a modern and responsive graphical user interface capable of running across multiple platforms including mobile devices and desktop systems. Through this interface, users are able to register accounts, generate cryptographic keys, send and receive secure messages, and perform steganographic operations such as embedding and extracting hidden messages from images. Flutter was chosen because of its cross-platform capabilities and ability to create interactive and visually appealing applications while maintaining high performance.

The backend is implemented using the Flask web framework in Python. Flask acts as the core processing engine of the system and manages all security-related operations. It handles user authentication, RSA key generation, AES encryption and decryption, steganographic embedding and extraction, and database management. The backend communicates with the frontend through RESTful APIs, ensuring secure and efficient data exchange between the two components.

Within the backend architecture, several modules work together to perform secure communication. The authentication module manages user registration and login operations and ensures that only authorized users can access the system. The cryptographic module performs RSA key generation, AES encryption, and decryption operations to secure message content. The steganography module is responsible for embedding encrypted messages into digital images using adaptive Least Significant Bit techniques and extracting hidden data from stego-images during message retrieval. Additionally, the image analysis module computes objective image quality metrics such as Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), and Mean Squared Error (MSE), which are used to evaluate the visual quality of stego-images and ensure minimal distortion.

The system also incorporates a database layer using SQLite to store user information, cryptographic public keys, contact lists, and encrypted messages. This database ensures efficient storage and retrieval of communication data while maintaining system integrity. Real-time communication features are supported through WebSocket connections, enabling instant message delivery and user status updates.

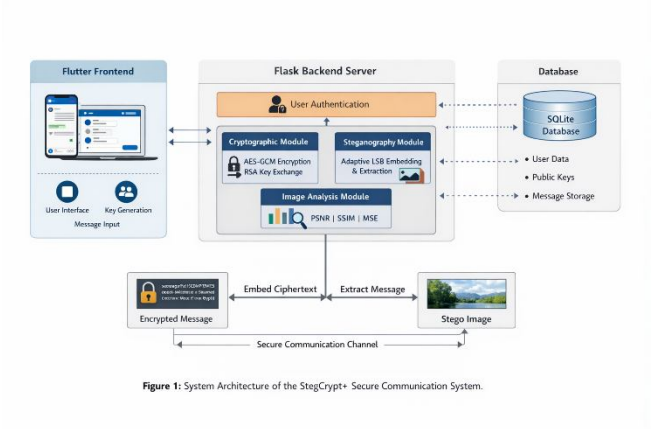


Figure 1: System Architecture of the StegCrypt+ Secure Communication System.

Figure 1 illustrates the overall architecture of the StegCrypt+ system, highlighting the interaction between the Flutter-based frontend, the Flask backend server, the cryptographic processing module, and the steganographic embedding system.

IV. ENCRYPTION AND STEGNOGRAPHY WORKFLOW

The StegCrypt+ communication framework operates through a multi-stage process that integrates cryptographic encryption with steganographic concealment. The workflow begins when a user composes a message within the application interface. This message is initially treated as plaintext and is transmitted to the backend server through a secure API request.

Upon receiving the message, the backend generates a random symmetric key used for encryption. The plaintext message is then encrypted using the Advanced Encryption Standard operating in Galois/Counter Mode (AES-GCM). AES-GCM was selected because it provides authenticated encryption, meaning that it guarantees both confidentiality and message integrity. In addition to producing ciphertext, the algorithm also generates an authentication tag that enables the receiver to verify that the message has not been altered during transmission. Once the message has been encrypted, the symmetric AES key must be securely shared with the recipient. To achieve this, the system uses RSA public-key cryptography. The AES key is encrypted using the recipient's public RSA key, ensuring that only the intended recipient possessing the corresponding private key can decrypt the symmetric key.

After the cryptographic stage is complete, the encrypted message is embedded within a digital image using adaptive Least Significant Bit steganography. In this technique, the least significant bits of selected image pixels are modified to store the encrypted data. The adaptive mechanism analyzes the complexity and texture of the image to determine how many bits can be modified without introducing noticeable visual distortion. Highly textured areas of the image allow deeper embedding, while smooth areas use minimal embedding to preserve visual quality.

The resulting stego-image contains the hidden encrypted message while appearing visually identical to the original image. This image can then be transmitted through standard communication channels without raising suspicion. When the recipient receives the image, the system extracts the embedded ciphertext using the reverse steganographic process. The encrypted AES key is decrypted using the recipient's RSA private key, and the recovered AES key is then used to decrypt the ciphertext and restore the original plaintext message.

This workflow ensures that even if an attacker intercepts the transmitted image, they will not only be unable to detect the presence of hidden data but will also be unable to decrypt the message without the appropriate cryptographic keys.

V. ALGORITHMS

The security of the StegCrypt+ system relies on the integration of two primary algorithms: the AES-GCM encryption algorithm and the adaptive LSB steganography algorithm.

A. *AES-GCM Encryption Algorithm*

The AES-GCM encryption process begins with the generation of a random symmetric key. The plaintext message is then encrypted using this key along with a randomly generated nonce. The AES-GCM algorithm performs encryption and authentication simultaneously, producing ciphertext and an authentication tag. The authentication tag allows the receiver to verify that the message has not been modified or corrupted during transmission.

During decryption, the recipient uses the same symmetric key and nonce to decrypt the ciphertext. The authentication tag is verified before the message is accepted as valid. If the authentication check fails, the message is rejected, preventing tampered data from being processed.

B. *Adaptive LSB Steganography Algorithm*

The adaptive LSB steganography algorithm operates by embedding encrypted data within the least significant bits of selected pixels in the cover image. The process begins by analyzing the cover image to determine regions with varying levels of texture and complexity. Edge detection and pixel variation analysis are used to identify suitable embedding locations.

Once the analysis is complete, the encrypted message is converted into a binary data stream. This binary data is sequentially embedded into the least significant bits of selected pixels. In complex regions of the image, more bits can be modified without noticeable distortion, while in smooth regions fewer bits are altered to maintain visual fidelity.

During extraction, the same pixel selection strategy is applied to retrieve the embedded bits from the stego-image. The extracted binary data is then reconstructed into the encrypted ciphertext, which can subsequently be decrypted using the cryptographic keys.

VI. EXPERIMENTAL RESULTS

To evaluate the performance of the StegCrypt+ system, several experiments were conducted to analyze the visual quality of stego-images and the reliability of hidden message extraction. The evaluation focused on measuring the degree of distortion introduced during the embedding process and assessing the imperceptibility of the hidden data.

Three widely used image quality metrics were employed for this evaluation: Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), and Mean Squared Error (MSE). These metrics provide objective measurements of the difference between the original cover image and the resulting stego-image.

Peak Signal-to-Noise Ratio measures the ratio between the maximum possible pixel value and the noise introduced by the embedding process. Higher PSNR values indicate better image quality and less noticeable distortion. In the experiments conducted, the PSNR values consistently remained above 40 dB, which indicates that the stego-images maintain very high visual similarity to the original images. The Structural Similarity Index evaluates the similarity between two images based on structural information such as luminance, contrast, and texture. SSIM values range from 0 to 1, with values closer to 1 indicating higher similarity. The StegCrypt+ system achieved SSIM values close to 0.98, demonstrating that the structural characteristics of the images remain largely unchanged after embedding.

Mean Squared Error measures the average squared difference between corresponding pixels in the original and stego-images. Lower MSE values indicate smaller differences and better image quality. The experiments revealed very low MSE values, confirming that the adaptive embedding strategy introduces minimal distortion.

The experimental results demonstrate that the proposed system successfully hides encrypted messages within images while maintaining high visual fidelity. This makes it difficult for both human observers and automated steganalysis tools to detect the presence of hidden information.

VII. FLOWCHART OF SECURE COMMUNICATION PROCESS

The communication process in StegCrypt+ can be represented through a workflow diagram illustrating the sequential steps involved in secure message transmission. The process begins with user authentication and message input. The plaintext message is encrypted using AES-GCM, and the symmetric key is encrypted using RSA. The encrypted message is then embedded into an image using adaptive LSB steganography. The resulting stego-image is transmitted to the recipient, who extracts the hidden ciphertext, decrypts the AES key using RSA, and finally recovers the original message.

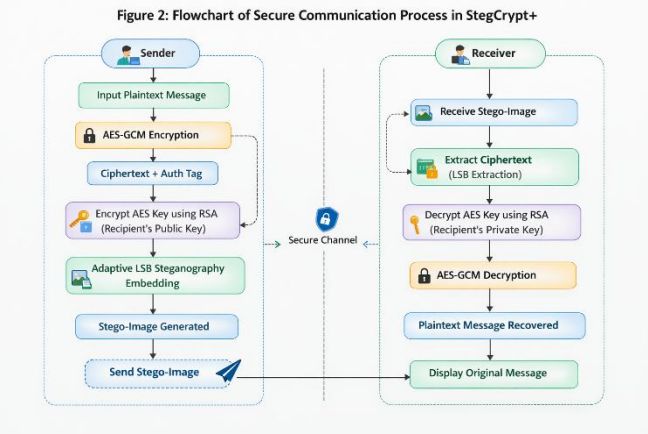


Figure 2 illustrates the flowchart of the StegCrypt+ secure communication process.

VIII.FUTURE WORK

Although the StegCrypt+ system provides strong security and effective concealment of messages, several improvements can be explored in future research. One possible direction is the integration of artificial intelligence techniques to optimize the steganographic embedding process. Machine learning models could be used to identify optimal embedding locations within images, further improving imperceptibility and resistance to steganalysis.

Another potential enhancement involves extending the system to support additional media formats such as audio and video steganography. This would increase the versatility of the system and allow secure communication across multiple types of digital media. Future work may also explore the implementation of post-quantum cryptographic algorithms to ensure long-term security in the presence of emerging quantum computing technologies.

Additionally, cloud deployment and distributed architectures could be incorporated to improve scalability and performance, enabling the system to support large numbers of users in real-time communication environments.

IX. CONCLUSION

This paper presented StegCrypt+, a hybrid secure communication system that combines advanced cryptographic techniques with adaptive steganography to achieve both confidentiality and concealment of sensitive information. The integration of AES-GCM encryption, RSA key exchange, and adaptive Least Significant Bit embedding provides a multi-layered security framework capable of protecting digital communication against interception and analysis.

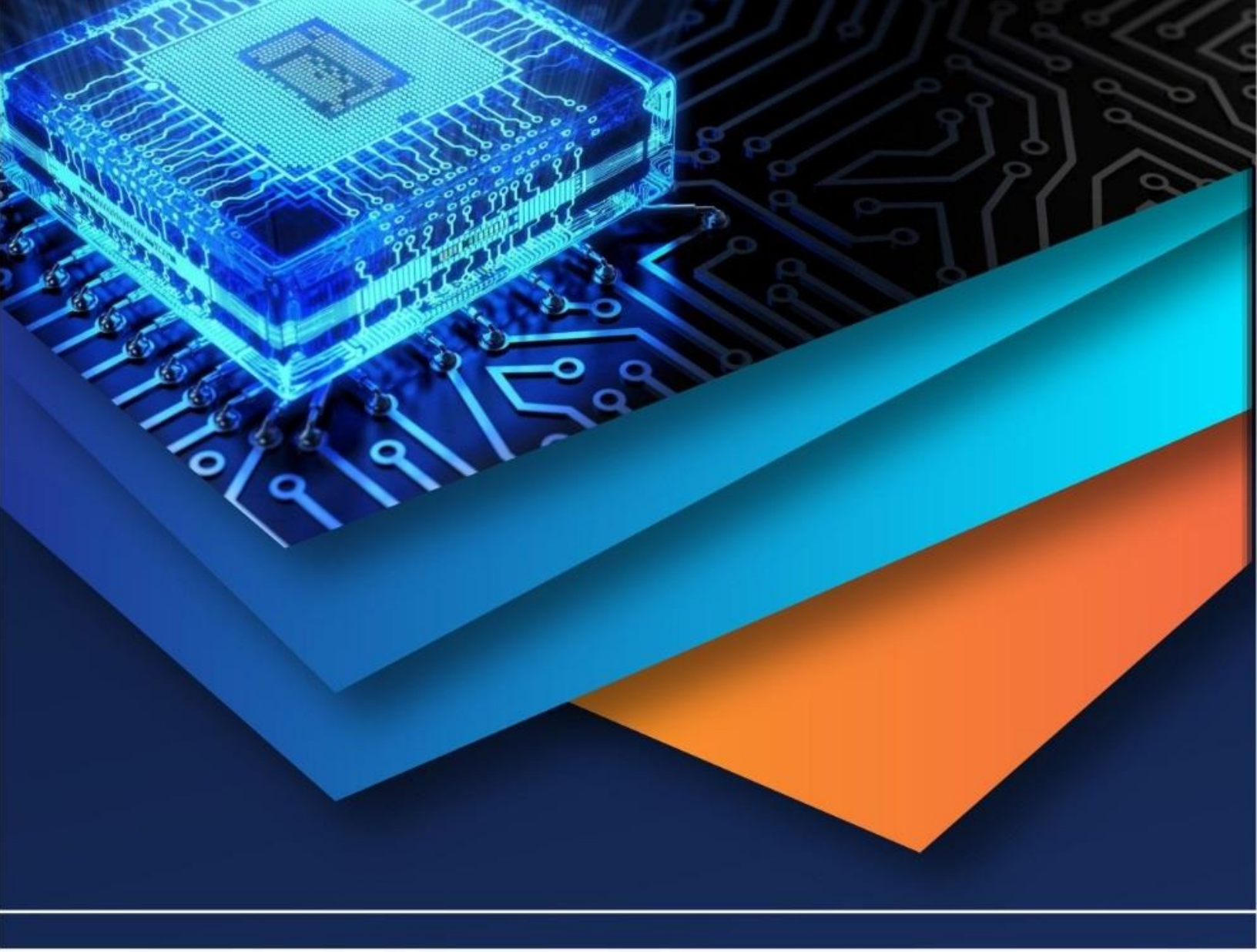
The system architecture, implemented using a Flutter frontend and Flask backend, provides a flexible and user-friendly platform for secure messaging applications. Experimental evaluation demonstrates that the proposed approach maintains high image quality while successfully embedding encrypted data, making it highly resistant to detection.

By integrating encryption and steganography into a unified communication framework, StegCrypt+ offers a powerful solution for covert communication in sensitive domains where both secrecy and privacy are essential.

REFERENCES

[1] W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed. Boston, MA, USA: Pearson Education, 2017.
[2] J. Daemen and V. Rijmen, The Design of Rijndael: AES – The Advanced Encryption Standard. Berlin, Germany: Springer-Verlag, 2002.
[3] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120–126, Feb. 1978.
[4] N. Provos and P. Honeyman, "Hide and Seek: An Introduction to Steganography," IEEE Security & Privacy Magazine, vol. 1, no. 3, pp. 32–44, 2003.
[5] N. F. Johnson, Z. Duric, and S. Jajodia, Information Hiding: Steganography and Watermarking – Attacks and Countermeasures. Boston, MA, USA: Springer, 2001.
[6] J. Fridrich, Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge, UK: Cambridge University Press, 2009.
[7] C. Cachin, "An Information-Theoretic Model for Steganography," in Proceedings of the Second International Workshop on Information Hiding, Portland, OR, USA, 1998, pp. 306–318.
[8] A. Westfeld and A. Pfitzmann, "Attacks on Steganographic Systems," in Proceedings of the Third International Workshop on Information Hiding, Dresden, Germany, 1999, pp. 61–76.
[9] R. C. Gonzalez and R. E. Woods, Digital Image Processing, 4th ed. Upper Saddle River, NJ, USA: Pearson, 2018.

[10] Z. Wang, A. Bovik, H. Sheikh, and E. Simoncelli, "Image Quality Assessment: From Error Visibility to Structural Similarity," IEEE Transactions on Image Processing, vol. 13, no. 4, pp. 600–612, Apr. 2004.
[11] D. Boneh and V. Shoup, A Graduate Course in Applied Cryptography. Stanford University, 2020.
[12] M. Kaur and S. Behal, "A Survey on Steganography Techniques," International Journal of Computer Applications, vol. 60, no. 2, pp. 34–38, Dec. 2012.
[13] M. Grinberg, Flask Web Development: Developing Web Applications with Python, 2nd ed. Sebastopol, CA, USA: O'Reilly Media, 2018.
[14] E. Windmill, Flutter in Action. Shelter Island, NY, USA: Manning Publications, 2019.
[15] NIST, "Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC," National Institute of Standards and Technology, NIST Special Publication 800-38D, 2007.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY