WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Designing Next Generation Cryptography for Secure and Private Communication

Eruguralla Satishbabu[1], Peddi Lahari[2], Samala Manoj[3], Boini Harshitha[4], Nune Akhil[5]

[1]Associate Professor, Department of CSE, Jyothishmathi institute of technology and science, Nustulapur, Karimnagar, T.S., India
[2,3,4,5]UG students, Department of CSE, Jyothishmathi institute of technology and science, Nustulapur, Karimnagar, T.S., India
Satishbabu09@gmail.com, laharipeddi15@gmail.com, manojsamala113@gmail.com, boiniharshitha4532@gmail.com, akhilnune1211@gmail.com

ABSTRACT:

The exponential growth in digital communication has significantly increased the demand for secure communication methods for data transmission. While traditional techniques lack confidentiality and security. This project addresses traditional challenges by proposing a hybrid secure data transmission system that combines symmetric cryptography with an advanced LSB steganography approach. The system encrypts the input data using a custom symmetric encryption algorithm where 128-bit blocks are divided into four 32-bit subblocks, each undergoing circular bitwise shifts and XOR operations with secret keys. The encrypted output is then embedded into a cover image using a dynamic steganographic method that alternates between LSB-1, LSB-2, and LSB3 embedding patterns. This variability not only improves security by making statistical detection more difficult but also increases data-hiding capacity while maintaining visual quality. he accuracy of data extraction and decryption confirms the integrity of the method. This hybrid model thus overcomes the drawbacks of using encryption or steganography in isolation and proves effective in secure, covert communication scenarios.

Key terms: Symmetric Encryption, Steganography, LSB, Secure Communication, Data Hiding, Information Security, Image-Based Security, Hybrid Security Model, stego image

I.INTRODUCTION

In the modern digital era, the security of sensitive data has become one of the most critical concerns. With the widespread use of internet-based insecure networks. Cyber threats such as unauthorized access, interception, and data tampering continue to evolve, making it essential to ensure both the confidentiality and integrity of data during transmission. Traditional cryptographic methods, such as symmetric encryption, are commonly employed to encode data and protect it from being understood by unauthorized parties. However, encryption alone does not conceal the existence of the data, which can still attract attention and become a target for malicious attacks.

To address this challenge, the concept of steganography has emerged as a complementary technique to encryption. While encryption transforms the content into an unreadable form, steganography goes a step further by hiding the very presence of the data. This is typically achieved by embedding the encrypted message into digital media such as images, audio, or video files using methods like Least Significant Bit (LSB) substitution. The combination of cryptography and steganography thus forms a two-layered security model: cryptography secures the content, while steganography conceals it from detection. This hybrid approach provides stronger protection than either method alone and is particularly valuable in scenarios where stealth and confidentiality are equally important.

This project implements a secure data transmission system by integrating symmetric key encryption with image-based steganography. The plaintext message is first encrypted using a symmetric algorithm, producing ciphertext. This ciphertext is then embedded into a cover image using an improved LSB technique, resulting in a stego image that can be transmitted or stored securely. On the receiving end, the process is reversed to retrieve and decrypt the hidden message. The system aims to provide a reliable and user-friendly solution for secure communication, ensuring that confidential information remains hidden and protected even when transmitted over vulnerable networks. With its dual-layered security model, this approach is well- suited for applications in military communication, secure messaging, digital rights management, and cloud data protection.

II. LITERATURE SURVEY

D. Artz emphasized that the Steganography enhances rather than replaces encryption. Messages are not secure simply by virtue of being hidden. Likewise, steganography is not about keeping your message from being known - it's about keeping its existence from being known.[1]

Marwa E. Saleh et al.

The authors proposed a hybrid approach combining a modified AES algorithm with a steganographic technique. The encrypted message is first transformed securely using AES. Then, it is embedded into a cover medium using a steganographic method. This two-layer security ensures both confidentiality and concealment. The proposed model improves data integrity and privacy. It also demonstrates high embedding capacity and visual quality of stego images. The system is designed for applications requiring secure, covert communication. Experimental results validate its effectiveness in practical scenarios.[2]

"Secure Image Steganography using RSA and Hash- LSB". This work introduces a secure method that combines RSA encryption with a hash-based LSB embedding technique. The RSA algorithm ensures that the message is unreadable without the private key. Meanwhile, the hash-LSB approach hides the data invisibly within an image. Together, they offer both encryption and concealment. Even if the hidden data is detected, it cannot be deciphered without the RSA key. This dual-layer approach enhances protection from unauthorized access. The model supports robust data hiding with minimal image distortion. It is well-suited for secure multimedia communication.[3]

KP Bindu Madavi & P. Vijaya Karthick, proposed a hybrid encryption framework using AES, DES, and RC4 was proposed alongside LSB steganography. The paper emphasizes strong data security with perfect invisibility in image-based communication. User messages are first encrypted using layered symmetric ciphers. The ciphertext is then embedded into images using the LSB method. This increases resistance to cryptanalysis and steganalysis. It ensures that even if one layer is compromised, others provide protection. The study also aims for high visual quality in the stego image. It demonstrates effectiveness in secure digital communication environments.[4]

G. Diwakara Reddy et al. This paper presents an advanced LSB-based steganographic system integrated with XOR and ECC encryption. The ciphertext is transformed into image-compatible formats before embedding. The combined use of symmetric and asymmetric techniques enhances overall security. ECC offers lightweight and strong public-key encryption for data transmission. The approach is tailored for web-based confidential communication. It strengthens data confidentiality across networks. The study highlights growing demand for integrated encryption and steganography solutions. It proposes replacing traditional systems with more layered and adaptive models.[5]

Raiyan and Kabir (2025) introduced SCReedSolo, a system that leverages LSB-based image steganography with Fernet encryption and ReedSolomon coding, ensuring robust error correction in image-based secret communication.[6]

Habiba Sultana[1]|Deena Faria[2]|A.H.M. Kamal

Their study presents a method that combines Fernet symmetric encryption with an odd-even pixel modification technique for image steganography. This approach distributes encrypted data evenly across the image, enhancing security and imperceptibility.[7]

Maiti et al. (2024) proposed a layered framework that combines cryptography and steganography powered by deep learning, enabling the system to adaptively optimize hiding strategies to reduce detectability.[8]

Nor Fazlida Mohd Sani and Mohamad Adreen Nujjaid proposed a technique that combines AES symmetric encryption with RSA asymmetric encryption for secure text data hiding. The method enhances security by leveraging the strengths of both encryption types before embedding the data using LSB steganography.[9]

Upadhaya et al. (2024) enhanced traditional LSB methods by using pixel intensity-based adaptive bit positioning, improving payload capacity without compromising image quality.[10]

Tanwar et al. (2023) explored the use of digital watermarking alongside steganography, offering integrity verification in addition to secrecy through embedded hash signatures.[11]

Nair and Thomas (2023) designed a lightweight steganographic system for IoT environments, ensuring secure command transmission using fast symmetric ciphers and LSB embedding.[12] "A systematic literature review on combined framework of secure communication using steganography and cryptography" by j.suresh babu, g.Niranjana, kadiyala Ramana .The authors conduct a systematic review of frameworks that integrate steganography and cryptography for secure communication. The study identifies common approaches and evaluates their effectiveness in ensuring data security.[13]

III. METHODOLOGY

The proposed system secures data transmission by combining symmetric cryptography with Least Significant Bit (LSB) steganography. The methodology is divided into two core phases: encryption and embedding at the sender's end, followed by extraction and decryption at the receiver's end. Each phase involves a sequence of well-defined steps to ensure the confidentiality and imperceptibility of the transmitted data.

In the encryption phase, the user's original input (plain text) is first preprocessed and converted into binary format. The binary data is then divided into 128-bit blocks, which are further split into four 32- bit sub-blocks. Each sub-block undergoes bitwise circular shifts and XOR operations with dynamically generated keys, enhancing the diffusion and confusion properties of the encryption. This encrypted output becomes the cipher text used for the next phase.

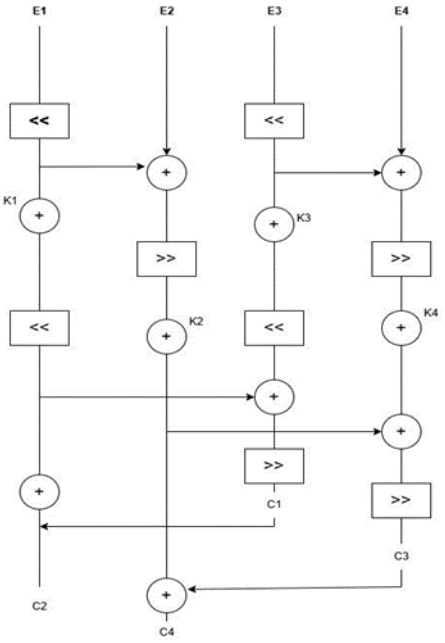
In the steganography phase, the cipher text is embedded into a cover image using a modified LSB technique. Unlike traditional LSB methods that only use the least significant bit of each pixel channel, this approach alternates between LSB-1, LSB-2, and LSB-3 positions. This variable embedding strategy

improves the imperceptibility and reduces the risk of statistical detection. The result is a stego-image that visually resembles the original image but secretly carries encrypted information.

At the receiver's end, the embedded cipher text is first extracted from the stego-image using the inverse of the LSB algorithm. The binary string is reassembled and passed into the decryption module, which uses the same key and transformation steps to recover the original plain text. The modular design allows for efficient integration, and test cases validate each unit and the complete flow to ensure the correctness and robustness of the system.

This hybrid approach provides a dual layer of security—concealing the existence of data and protecting its content—making it suitable for secure communications over untrusted channels.

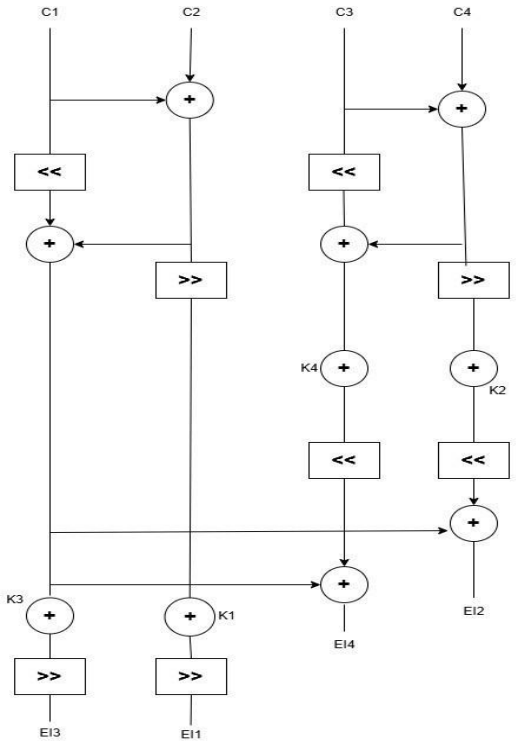
IV. PROPOSED ALGORITHM



Encryption

The proposed symmetric encryption algorithm is a custom-designed, block-based cryptographic approach that operates on 128-bit plaintext input. This input is divided into four equal parts—E1, E2, E3, and E4—each 32 bits in length. The encryption process utilizes four secret keys (K1, K2, K3, and K4), which are pre-shared between the sender and the receiver. To ensure both confusion and diffusion—fundamental principles of cryptography—the algorithm employs a combination of XOR operations and circular bit shifts (both left and right).

The encryption begins by applying a circular left shift to block E1, followed by an XOR operation with key K1. The output is again shifted, contributing to the final calculation of other blocks. Similarly, E2 is combined with the result from E1, shifted right, and XORed with K2. Parallelly, E3 is left-shifted and XORed with K3, while E4 is XORed with the transformed E3, then shifted and mixed with K4. These transformations ensure that every bit of the output ciphertext is dependent on multiple parts of the plaintext and keys, making the encryption process non-linear and highly secure. The final ciphertext consists of four blocks—C1, C2, C3, and C4—which are derived from a blend of the processed plaintext segments and secret keys. The algorithm's architecture ensures that any slight change in the plaintext or key produces a significantly different output, thereby enhancing security. This layered and interconnected transformation process increases resistance against brute force, differential, and linear cryptanalysis, making the encryption mechanism both robust and efficient for secure communication.



Decryption

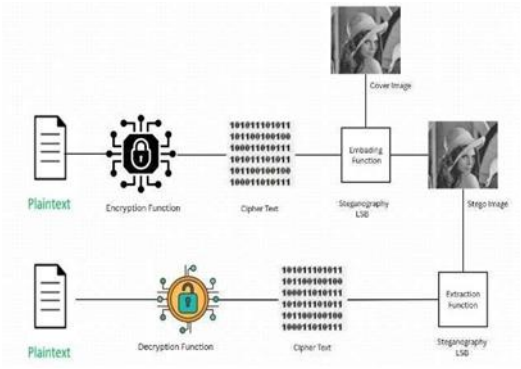
The decryption process in this system is designed to reverse the transformations applied during encryption, recovering the original 128-bit plaintext from the four encrypted 32-bit blocks: C1, C2, C3, and C4. The process uses the same symmetric keys (K1, K2, K3, and K4) that were used during encryption, ensuring that the operation is perfectly reversible. Each step in the decryption pipeline corresponds to the inverse of a specific transformation applied during the encryption phase, including bitwise XOR operations and circular shifts.

To begin the decryption, the left side of the diagram focuses on recovering the original blocks E1 and E3, denoted as EI1 and EI3. The process starts by applying a left circular shift to the ciphertext block C1. This reverses the final right shift that was applied to this block during encryption. The shifted result is then XORed with C2, reversing the final layer of mixing performed during the encryption process. A right circular shift is then applied to this XOR result to restore the original order of bits. The intermediate result is finally XORed with the corresponding secret keys K3 and K1, which effectively removes the encryption key influence and yields the original values for EI3 and EI1.

The right side of the diagram follows a similar pattern to recover the original blocks E2 and E4 (denoted as EI2 and EI4). The ciphertext block C3 undergoes a left circular shift, which is then XORed with C4, again undoing the mixing applied during encryption. The result of this XOR operation is passed through a right circular shift to realign the bit sequence. Afterward, the shifted result is XORed with keys K4 and K2, reversing the earlier encryption key application and recovering the original data blocks.

Through these systematic steps, the decryption function ensures complete and accurate reconstruction of the original 128-bit plaintext. The integrity of the message is preserved as long as the correct encryption keys are used. This design emphasizes the key principles of symmetric encryption: reversibility, key-dependence, and bitwise precision. If any single bit of the key or ciphertext is altered, the output will no longer match the original message, reinforcing the security of the system. Overall, the decryption module works efficiently and securely, maintaining data confidentiality and supporting seamless communication between sender and receiver.

IV. SYSTEM ARCHITECTURE

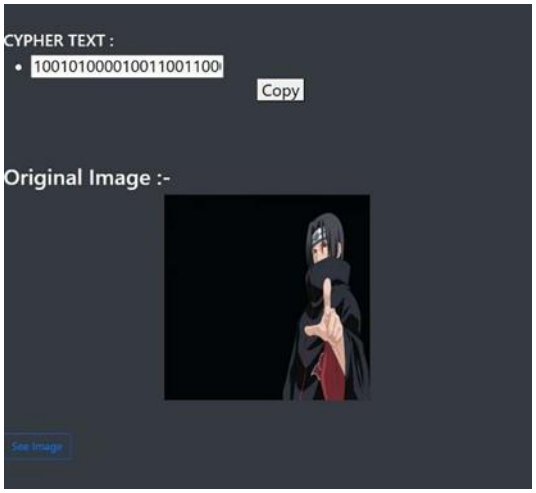


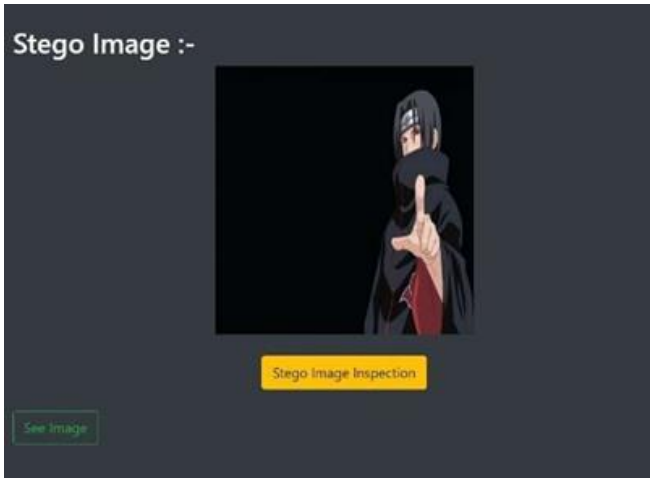
The architecture illustrated in the diagram represents a hybrid model for secure data transmission that combines symmetric encryption with image-based steganography. This layered approach is designed to protect sensitive information by not only encrypting the content but also hiding its existence. The process begins with the user supplying plaintext data, which is passed to the encryption function. This function applies a symmetric encryption algorithm— commonly Advanced Encryption Standard (AES) or other custom block ciphers—to convert the readable message into an unreadable binary format called ciphertext. Symmetric encryption is chosen for its speed and efficiency in real-time communication, as it requires the same secret key for both encryption and decryption.

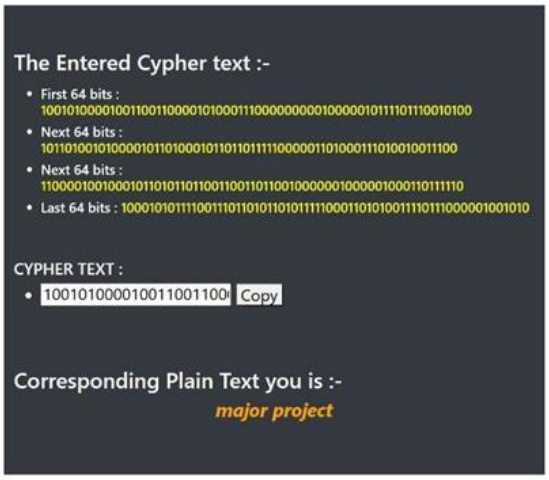
Once the message is encrypted, the ciphertext undergoes a steganographic embedding process. Here, the system takes a cover image—a regular, unaltered digital image—and uses a technique known as Least Significant Bit (LSB) substitution to embed the binary ciphertext into the image's pixel data. This process does not cause visible distortion to the image, ensuring that the presence of the hidden message goes unnoticed to a casual observer or even image analysis tools. The result is a stego image, which visually appears identical to the original cover image but secretly carries the encrypted data. This dual-layer security (encryption + hiding) ensures that even if the image is intercepted, the message within remains both unseen and unreadable without the proper key and extraction process.

On the receiving side, the extraction function is responsible for reversing the steganographic process. It scans the stego image, extracts the embedded binary data from the least significant bits, and reconstructs the ciphertext. This ciphertext is then sent to the decryption function, where the original symmetric key is used to decrypt it, restoring the original plaintext message. The combination of these two techniques ensures a high degree of security: even if one layer is breached (e.g., the stego image is detected), the encryption remains intact. This architecture is highly applicable in environments where data confidentiality, integrity, and stealth are critical, such as military communication, digital watermarking, secure file transfer, and cloud storage.

V. RESULTS







VI. CONCLUSION

The proposed system effectively combines symmetric encryption and image-based steganography demonstrates a robust, efficient, and practical approach to safeguarding sensitive digital communication, to ensure both the confidentiality and invisibility of sensitive information during transmission. While encryption techniques alone secure the content of a message, they do not conceal its existence. By integrating steganography, particularly using a modified LSB technique (LSB1,LSB-2,LSB-3) this system hides the presence of encrypted data within a cover image, offering a dual-layered security model that greatly enhances protection against unauthorized access or interception.This system supports multiple image formats including PNG, JPG, JPEG, and GIF for steganographic operations. It was tested across major web browsers (Chrome, Firefox, Edge) and operating systems (Windows, Linux, macOS), confirming its cross-platform compatibility. This makes it flexible and portable solution suitable for deployment in diverse technical environments.

The results demonstrate that this hybrid approach maintains high visual quality in the stego images while securely embedding encrypted content. The system also supports reliable decryption and data recovery at the receiver's end, proving its robustness and effectiveness. This makes it suitable for use in sensitive applications such as military communication, online document sharing, digital forensics, and personal data protection. Future enhancements may include the use of biometric authentication, dynamic key generation, or AIassisted embedding strategies to further improve security and performance. Overall, the project provides a practical and secure framework for transmitting confidential data over untrusted networks.

VII. REFERENCES

1. Digital steganography: hiding data within data, D.Artz, publisher-IEEE ,Internet Computing ,volume 5
2. Marwa E. Saleh , Abdelmgeid A. Aly,Fatma A. Omara, "Data Security Using Cryptography and steganography Technique", (IJACSA) International Journal of Advanced , Computer Science and Applications, Vol. 7, No. 6, 2016
3. Rituparna Halder, Susmit Sengupta, Sudipta Ghosh, Debashish Kundu, A Secure Image Steganography Based on RSA Algorithm and HashLSB Technique , IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, pISSN: 2278-8727, Volume 18, Issue 1, Ver. IV (Jan – Feb. 2016), PP 39-43
4. KP Bindu Madavi & P. Vijaya Karthick "Enhanced Cloud Security using Cryptography and Steganography Techniques", Publisher: IEEE,2021 International Conference.
5. G Diwakara reddy,Yaddanapudi VSSRR Udai Karan,Pradhdeep singh,shubhranshu Vikram singh, sachita shaw, Jitendra singh, "A Proficient and secure way of Transmission using Cryptography and Steganography", Publisher: IEEE, 2022 International Conference.
6. Raiyan, S. R., & Kabir, M. H. (2025). SCReedSolo: A Secure and Robust LSB Image Steganography Framework. arXiv:2503.12368.
7. Ali, T., & Hussain, N. (2018). "Securing cloud data using stego-crypto model". International Journal of Computer Applications, 179(14),1-5
8. Maiti, A., Laha, S., Upadhaya, R., Biswas, S., Kar, B., & Sen, J. (2024). Boosting Digital Safeguards with AI-Based Cryptography and Steganography. arXiv:2404.05985.
9. Upadhaya, R., & Thomas, P. (2024). Pixel Intensity-Based Adaptive Steganography Using AES. Journal of Multimedia Security, 19(1), 33–41.
10. Tanwar, A., Reddy, S. K., & Nair, K. (2023). Watermarking Plus Steganography for Integrity and Privacy. Applied Information Security Journal, 5(4), 54–63.
11. Nair, K., & Thomas, D. (2023). Lightweight Cryptographic Steganography for IoT Nodes. Internet of Things Security Journal, 12(3), 45–52.
12. J suresh babu, g.Niranjana, kadiyala Ramana(2023),"A systematic literature review on combined framework of secure communication using steganography and cryptography" , AIP Conference Proceedings
13. Shrivastava, R., & Thakur, D. (2020). Comparative study of DES, AES, and Blowfish in secure image steganography. International Journal of Advanced Trends in Computer Science and Engineering, 9(3), 2342–2348.
14. Singh, R., & Gupta, R. (2019). A secure image steganography based on RSA algorithm and hashLSB technique. Procedia Computer Science, 152, 404–412.
15. Roy, S., & Dey, S. (2018). Steganographybased secure image transmission using DWT and AES. Journal of Computer Engineering, 20(4), 31–37.
16. Tanwar, A., Reddy, S. K., & Nair, K. (2023). Watermarking Plus Steganography for Integrity and Privacy. Applied Information Security Journal,5(4),54-63.
17. Bindu, K. P., & Karthick, P. V. (2020). Hybrid encryption and LSB-based steganography for secure communication. International Journal of Advanced Research in Computer Science,11(2),88- 94.
18. Saini, N., & Sharma, S. C. (2017). A novel approach for secure data communication using cryptography and steganography. Procedia Computer Science, 132, 1194– 1201.
19. Rathi, A., & Singh, P. (2020). Image steganography using LSB with AES and RSA encryption. International Journal of Engineering Research and Applications, 10(4), 29–34.