IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 2, February 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 2, February 2024 ||

| DOI:10.15680/IJIRSET.2024.1302084 |

Secure Communication Framework with Cryptography and Stegnography Methods

Mrs.R.Arthi, Ms.Ponnaganti Malleswari, Ms.A Keerthana

Assistant Professor, Department of Cyber Security, Muthayammal Engineering College, Rasipuram, India

Student, Department of Cyber Security, Muthayammal Engineering College, Rasipuram, India

Student, Department of Cyber Security, Muthayammal Engineering College, Rasipuram, India

ABSTRACT: The process of data sharing come significant concerns about security and privacy.The need to ensure the confidentiality, integrity, and availability of sensitive information has never been more critical. Here propose a novel approach that combines steganography and cryptography techniques. The proposed system aims to enhance the security of data transmission by encrypting data using AES encryption and hiding it within an image using Modified Least Significant Bit (LSB) with and image encryption using Elliptic Curve Cryptography (ECC). In the contemporary digital era, ensuring the security and confidentiality of sensitive information during communication is of paramount importance.

This research proposes a comprehensive Secure Communication Framework (SCF) that combines advanced cryptographic and steganographic methods to enhance the confidentiality and integrity of transmitted data. The integration of cryptography and steganography aims to create a multi-layered security approach,mitigating the risks associated with various cyber threats. The cryptographic component of the framework involves the use of state-of-the-art encryption algorithms to protect the content of messages from unauthorized access. Robust encryption techniques, such as Advanced Encryption Standard (AES) and Rivest Cipher (RSA), are employed to secure data at the source and decrypt it at the destination, ensuring end-to-end confidentiality. The results of this research contribute to the development of a robust and flexible SecureCommunication Framework, offering an integrated solution that combines the strengths of cryptography and steganography. The proposed framework has the potential to safeguard sensitive information in various communication settings, playing a crucial role in the ongoing efforts to fortify digital security in an ever- evolving technological landscape.

I. INTRODUCTION

There has never been a more important requirement for safe communication in the increasingly linked digital world. Sensitive information is exchanged across multiple channels by individuals, businesses, and governments, increasing the danger of the threat of illegal access and data breaches is quite real. In order to overcome these obstacles, this study presents the Secure Communication Framework (SCF), which strengthens the integrity and secrecy of transmitted data by utilizing the synergies of sophisticated cryptography and steganography techniques. Digital security is based on the ancient science of information encoding, or cryptography. Modern cryptographic methods are used in our system to encrypt data, making it unintelligible to anybody without the necessary key for decryption. The use of robust algorithms such as Advanced Encryption Standard (AES) and Rivest Cipher (RSA) ensures that even in the face of sophisticated attacks, the confidentiality of the communicated information remains steadfast

Our architecture uses steganography, a clever technique for hiding information among seemingly innocent carriers, to strengthen the cryptographic protections. By incorporating encrypted data into multimedia files like Steganography adds an additional layer of obfuscation to images or audio, making it difficult for unauthorized parties to discern sensitive content. The integration of steganography with cryptography yields a multifaceted security strategy that improves the communication framework's overall resilience. Multimedia, text, and image broadcasts are among the many communication modes that the SCF is intended to accommodate. Because of its adaptability, the framework is not only sturdy but also useful in a range of situations, from personal exchanges of data at the enterprise level to communications. Understanding that cyber threats are dynamic, the SCF is prepared to change and adapt in order to remain ahead of any possible weaknesses.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 2, February 2024 ||

| DOI:10.15680/IJIRSET.2024.1302084 |

This study explores real-world applications in addition to offering a theoretical foundation. We assess the SCF's performance using extensive testing and simulations, taking into account important parameters as throughput, latency, and computational burden. These assessments seek to show the framework's effectiveness and viability in practical settings, guaranteeing that the suggested solution satisfies strict security standards and is both useful and effective when implemented. Steganography adds an additional layer of obfuscation by concealing encrypted data within seemingly innocent carriers, such multimedia files. By making it difficult for unauthorized parties to understand sensitivecontent, this strategy strengthens the communication framework's overall resilience. The SCF's versatility is emphasized, which makes it appropriate for a variety of scenarios, from private data exchanges to corporate interactions. The framework highlights its ability to adapt in order to remain ahead of potential vulnerabilities and recognizes the dynamic nature of cyber threats.

The Secure Communication Framework described in this research offers a thorough and creative solution in a time when information security is crucial. Combining steganography's and cryptography's advantages, We work hard to support continuous efforts to protect digital communication channels from a constantly changing array of cyberthreats.

II. SYSTEM ANALYSIS

Existing System:
Applications for reversible data hiding in ciphertext include privacy protection and the transferring of data in cloud settings. The original plain-text image can berecovered from the encrypted image formed after data embedding, and the embedded data can be extracted before or after decryption. The Paillier cryptosystem is provided with the random element substitution (RES) method asa lossless data hiding technique. It operates by changing the bits that will be buried for a cypher value's random component.

Limitations:
Homomorphic processing often involves complex algorithms and computations. This complexity may lead to increased computational overhead, affecting theoverall efficiency and speed of the system. It has a limited payload capacity dueto the constraints of maintaining lossless compression.

Proposed System:
In this system, the encrypted text data hidden within cover images can be securedusing Modified LSB Data hiding and ECC based image encryption. This technique ensures that the data is protected, and only authorized individuals can access it. This proposed data hiding with image encryption is a promising technique for securing sensitive information. Its use can enhance the effectiveness of secure communication systems while ensuring the privacy and security of the data.

Expected Merits:
Improve the embedding capacity. Make ease of key generation and key sharing process. Provide Reliable and Secure communication. Does not affect the image quality during data embedding process.

III. ALGORITHM

AES (Advanced Encryption Standard)

The first layer of security involves AES encryption, a widely recognized symmetric encryption algorithm known for its robustness and efficiency. This ensures that the plaintext message remains confidential, protected by a strong encryption key. Framework protects plaintext message confidentiality by using AES encryption. Because AES is symmetric, sensitive data can be efficiently and securely protected by using the same key for both encryption and decryption. Selecting a strong encryption algorithm such as AES strengthens the communication framework's overall security.

LSB (Least Significant Bit)

By embedding the AES-encrypted text within a cover image using a modified Least Significant Bit (LSB) algorithm. This covert embedding ensures that even if the transmission is intercepted, the presence of sensitive information remains hidden within the seemingly innocuous image. Your secure communication framework improves the

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 2, February 2024 ||

| DOI:10.15680/IJIRSET.2024.1302084 |

transmitted information's secrecy by using this stealthy embedding technique. Even if unwanted individuals manage to intercept the communication, it will be challenging for them to identify the presence of critical data because the encrypted text is so finely woven into the cover image.

ECC (Elliptic Curve Cryptography)

The second layer of security is introduced by ECC encryption, a powerful asymmetric encryption method that safeguards the integrity and authenticity of the cover image itself. ECC encryption leverages the mathematical properties of elliptic curves to create secure digital signatures for the image, making it tamper- evident and verifiable. ECC generates safe digital signatures that improve the cover image's overall security by utilizing the mathematical characteristics of elliptic curves. These digital signatures not only help ensure the integrity of the image but also provide a means of verifying its authenticity. In other words, ECC encryption makes the cover image tamper-evident, and the digital signature allows for verification that the image has not been altered or compromised during transmission.

SOFTWARE DESCRIPTION:

User Enrolment:
User enrolment is the process of registering with application to make communications. Both are registered in this application and get authentication factors for login process. For registering process, they should enter the details like name, father name, gender, age, mobile number, email id, username and password.

User Authentication:
Authentication is the process of verifying whether the user is valid or not. In this proposed work user should authenticated using username and password for login. Authenticated users are only allowed to access application. Otherwise the systemshows invalid access message.

Data Sharing:
Data hiding is the process of hiding secret message into cover file. Secret message is present in the form of text and cover file is selected in form of image. Uploaded message was hidden within the image to create stegno image. Generatekey for securely sharing the information to receiver.

Data Encryption using AES:
The sensitive data is first encrypted using the AES algorithm, a widely used symmetric encryption technique. The symmetric key by AES is the same key thatis used for encryption and decryption. The AES algorithm works on blocks of data that are typically 128 bits in size to produce ciphertext that is unreadable without the associated decryption key.

Data Hiding using LSB:
Using a modified Least Significant Bit (LSB) approach, the encrypted data is hidden within a cover image. In order to carry the secret information, LSB manipulation modifies the cover image's pixel values' least significant bits. Inthis strategy, only a few LSBs are changed in order to keep the modifications from being visible to the human eye.

Image Encryption using ECC:
To encrypt the stegnographic image for an additional degree of protection after the data has been placed within it using a modified LSB approach. Image encryption is the process of converting the image pixels into unpredictable form. To complete this process, elliptic curve cryptography (ECC) is used.

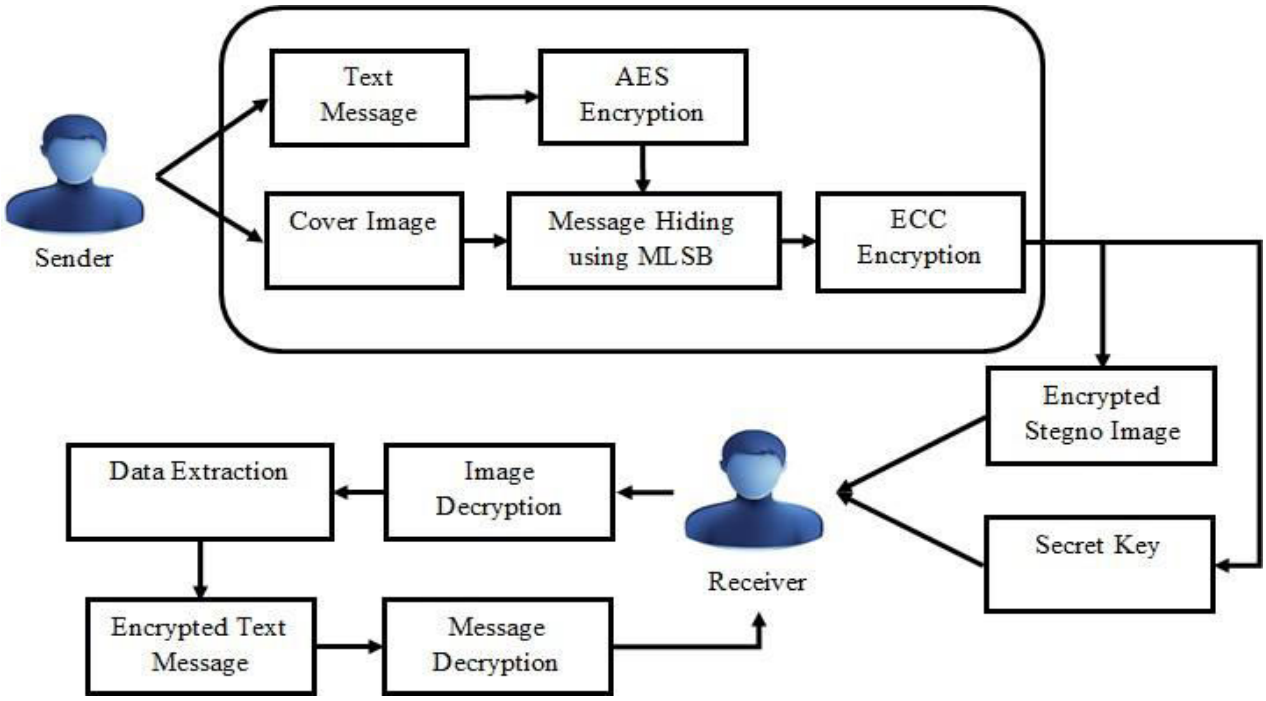
Data Retrieval:
Data extraction is the process of extracting the original data. Receiver gets the secret message with cover image. Specific key is generated and shared to the receiver during the process of message sending. Receiver can decrypt the image using shared secret key. Then the original message is shown to the receiver.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 2, February 2024 ||

| DOI:10.15680/IJIRSET.2024.1302084 |

System Architecture:



IV. CONCLUSION

To sum up, the Secure Communication Framework (SCF) introduced in this study offers a strong and novel solution to the urgent requirement for increased security in digital communications. A multilayered protection against potential attacks is provided by the framework's integration of advanced encryption and steganography techniques, which place an emphasis on confidentiality, integrity, and adaptability. The security of transmitted data is strengthened by the use of cutting-edge cryptographic methods, such as Rivest Cipher (RSA) and Advanced Encryption Standard (AES). These algorithms' power is foundin their resilience to sophisticated attacks as well as in their capacity to secure information, guaranteeing that private information is safe as it travels across various communication routes. An extra layer of security is introduced when steganography is used as a supplementary component to cryptography.

The SCF makes it harder for unauthorized parties to decode the message by hiding encrypted information inside harmless cover items like photos or audio files. This clever fusion of cryptography and steganographic techniques build astrong defense, enabling the framework to securely protect data on multiple platforms. One important aspect of the SCF is its adaptability, which recognizes the ever-changing nature of cyber threats. Its architecture enables flexible deployment across many situations and communication channels, making it suitable for a wide range of use cases, from enterprise-level data transfers to personal chats. This flexibility is further demonstrated by theframework's ability to change in reaction to new security issues, maintainingits applicability in the face of constantly evolving threat.

REFERENCES

1. Xiao, Di, Fei Li, Mengdi Wang, and Hongying Zheng. "A novel high- capacity data hiding in encrypted images based on compressive sensing progressive recovery." IEEESignal Processing Letters 27 (2020): 296-300.
2. Chen, Fan, Yuan Yuan, Hongjie He, Miao Tian, and Heng-Ming Tai. "Multi MSB compression based reversible data hiding scheme in encrypted images." IEEE Transactions on Circuits and Systems for Video Technology 31, no. 3 (2020): 905- 916.
3. Chen, Bing, Wei Lu, Jiwu Huang, Jian Weng, and Yicong Zhou. "Secret sharing basedreversible data hiding in encrypted images with multiple data hiders." IEEETransactions on Dependable and Secure Computing19, no. 2 (2020): 978-991.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 2, February 2024 ||

| DOI:10.15680/IJIRSET.2024.1302084 |

4. Du, Yang, Zhaoxia Yin, and Xinpeng Zhang. "High capacity lossless data hiding in JPEG bitstream based on general VLC mapping." IEEE Transactions on Dependable and Secure Computing 19, no. 2 (2020): 1420-1433.
5. Hua, Zhongyun, Yanxiang Wang, Shuang Yi, Yicong Zhou, and Xiaohua Jia. "Reversible data hiding in encrypted images using cipher-feedback secret sharing." IEEE Transactions on Circuits and Systems for Video Technology 32, no. 8 (2022): 4968-4982

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details