Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 15, Issue. 1, No.3 : 2024
ISSN : **1906-9685**

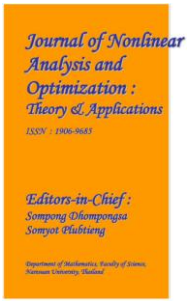

IMAGE STEGANOGRAPHY WITH MULTI-LAYER SECURITY AND HIGH CAPACITY

JAYA KUMAR, IV Year B.Tech CSE Students Dept of Computer Science and Engineering, DR MGR Educational And Research Institute, Maduravayol, Chennai, India
Jaikumar414446@gmail.com
JOESPH RAJ, IV Year B.Tech CSE Students Dept of Computer Science and Engineering, DR MGR Educational And Research Institute, Maduravayol, Chennai, India rajjoseph495@gmail.com
KAWRI SANKAR, IV Year B.Tech CSE Students Dept of Computer Science and Engineering, DR MGR Educational And Research Institute, Maduravayol, Chennai, India kawrisankar.tra@gamil.com
Dr. B. RAJA, Professor Dept of Computer Science and Engineering, DR MGR Educational And Research Institute, Maduravayol, Chennai, India
DR.V.SAI SHANMUGA RAJ Professor Dept of Computer Science and Engineering, DR MGR Educational And Research Institute, Maduravayol, Chennai, India
DR.G. GUNASEKARAN, Professor Dept of Computer Science and Engineering, DR MGR Educational And Research Institute, Maduravayol, Chennai, India

***Abstract*—**
Today's internet plays a vital role in communication. With the growing concerns about data security and privacy, the need for robust and efficient stenographic techniques have become imperative. Steganography, the art of concealing information within seemingly innocuous data, presents an avenue for secure communication. The paper presents a sophisticated desktop application aimed at enhancing image steganography by incorporating cutting-edge cryptographic algorithms, including Rivest-Shamir-Adleman (RSA) Advanced Encryption Standard (AES), and the F5 algorithm. This amalgamation aims to provide multi-level security and high-capacity data embedding, addressing the growing demand for robust and efficient stenographic techniques.

***Keywords*—**
Steganography, Cryptography, Multi-Level Security, aes, rsa, Data Concealment and data confidentiality.

I. INRODUCTION

Recently, the internet has become a convenient medium for exchanging digital data and multimedia, providing extensive accessibility and fast data transfer speeds. Despite its efficiency, a notable drawback of utilizing the Internet is the vulnerability of data security, as unauthorized individuals can monitor the transmitted information. This inherent risk underscores the importance of incorporating Steganography as a safeguarding measure to ensure secure communication over the Internet.

Image steganography, a technique within the broader realm of information hiding, serves as a means of covert communication by concealing secret messages within digital images. Unlike cryptography, which focuses on encrypting the content of messages, Steganography seeks to conceal the presence of communication entirely. This clandestine method has garnered significant interest in recent years, particularly with the rise of digital media and concerns surrounding information security. With its ability to embed large volumes of data within images, image steganography presents a versatile and powerful tool for secure communication and data protection. This introduction will provide an overview of image steganography, its applications, challenges, and implications in modern information security.

Traditional image steganography techniques have long been used to hide information within images, but as security threats have evolved, so too has the need for more robust and sophisticated methods. This has led to the development of multi-layer security and high-capacity image steganography, which represents a significant advancement In the domain of data concealment.

The image steganography application serves several crucial functions in modern contexts. Firstly, it facilitates discreet communication by hiding sensitive information within images, enabling confidential exchanges without arousing suspicion or risking interception. Moreover, steganography strengthens data protection by embedding data within images, providing an additional layer of security against unauthorized access or tampering. Additionally, steganographic techniques are commonly utilized for digital watermarking, allowing the embedding of ownership or copyright details within images to deter unauthorized use or distribution. In intelligence, law enforcement, and military operations, steganography enables covert communication and information exchange, vital for maintaining operational security and conducting undercover activities. Furthermore, steganography can aid in authentication and verification, assisting in verifying the authenticity of images or documents and detecting unauthorized alterations. Overall, the utilization of image steganography plays a crucial role in ensuring confidentiality, data protection, digital watermarking, covert operations, and authentication across various sectors and industries.

As image steganography grows increasingly essential for secure communication, For guaranteeing the secrecy and effective hiding of sensitive data, our proposed system integrates advanced encryption and embedding methods. Employing the Advanced Encryption algorithms for text encryption, our approach establishes a robust cryptographic framework, thereby safeguarding the integrity of concealed data. Additionally, we employ the F5 algorithm for image embedding, offering an efficient and high-capacity method to seamlessly integrate data into images while balancing security and payload size. This comprehensive system caters to the evolving demands of secure communication systems, providing a versatile solution for applications requiring robust security measures and substantial data-hiding capabilities.

The concept of multi-layer security in image Steganography introduces a multifaceted approach to data concealment, incorporating multiple layers of protection to fortify the hidden information. This intricate stratagem ensures that even if one layer is compromised, the integrity and confidentiality of the concealed data remain uncompromised, presenting a formidable challenge to any unauthorized party seeking access. Simultaneously, high-capacity steganography aims to optimize the amount of data that can be covertly embedded within cover-image, all while minimizing any noticeable changes to its visual appearance. This critical capability becomes especially crucial when discreetly transmitting substantial volumes of sensitive data.

II. RELATED WORKS

[1] Here in this paper the author “Abdelmotalib, Ali Ahmed and Ahmed” explores a secure method for image steganography utilizing Least Significant Bit (LSB) substitution and Double XOR operations. The aim is to conceal information within images while enhancing security. LSB substitution involves embedding data into the least significant bits of pixel values, while Double XOR operations add an additional layer of encryption by performing successive XOR operations. This dual-layered approach enhances the security of the hidden information. The paper likely discusses the implementation of these techniques, their effectiveness in concealing data while preserving image quality, and possibly includes experimental results to validate the proposed method's security and performance.

[2] In this paper the author “M. Gupta, A. Gupta and H. Shukla ” delves into the realm of image steganography, emphasizing its significance in concealing various types of data within cover images while maintaining their original appearance. It investigates the integration of Discrete Cosine Transform (DCT), Least Significant Bit (LSB), and compression techniques tailored for green images to bolster the security of hidden uploads. Initially, the LSB method is utilized to embed predetermined data pieces onto the cover image, resulting in a stego image. Subsequently, DCT is employed to transform the stego image from a local domain to a standardized domain. The study then focuses on securely transmitting these images, evaluating metrics such as mean squared error (MSE) and low bit

error rate (BER) without necessitating a password, and conducts comparisons with previous methods to gauge efficacy.

[3] In this research paper " jagan raj jayapandiyan ,c. Kavitha, and k. sakthivel" have introduced an innovative approach, termed enhanced LSB (eLSB), aimed at improving the quality of cover images in steganography compared to conventional LSB embedding techniques. The method, operating in the spatial domain, comprises two phases for encoding the secret message. Initially, metadata and header information are embedded in the first few bytes of the cover image. Subsequently, the secret message is processed and embedded into the cover image using an optimized approach, which involves analyzing character sequences in the text. This optimized embedding results in a more efficient use of space within the cover image, thereby enhancing the quality of the resulting stego image. The algorithm facilitates a high-capacity embedding rate, enhances security through secret message preprocessing, and improves the overall quality of the cover image. Comparative analysis with traditional LSB embedding methods using metrics such as Root Mean Square Error (RMSE), Peak Signal-to-Noise Ratio (PSNR), and Mean Square Error (MSE) demonstrates the superior performance of the proposed eLSB algorithm in embedding secret text while preserving image quality.

[4] In this paper, "M. R. Islam, A. Siddiqa, T. R. Tanni, M. J. Sultana, and S. Parvin" introduce a novel approach to data encapsulation using LSB image steganography, with a focus on meticulously selecting image pixels for embedding confidential information. The method entails filtering the entire image based on pixel data to pinpoint appropriate candidate pixels. Security measures are bolstered by incorporating a user-defined password and employing AES encryption to cipher the secret message prior to steganography application. During the experimental phase, the quality of the resultant stego image is evaluated through Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) assessments. The stego image exhibits elevated PSNR and diminished MSE values compared to alternative methods examined, highlighting the versatility and effectiveness of this innovative approach.

[5] In this paper, the authors"Srilekha Mukherjeea, Goutam Sanyala, Subhajit Roya" propose a novel method for image steganography called the Mid Position Value (MPV) technique. This technique involves concealing secret data within a cover image to enable secure communication. At first, a transformation by Arnold is employed on the cover image, which jumbles the data bits and disturbs the pixel alignment. Then, the MPV technique is employed to embed data bits from the secret image into the scrambled cover image. This process is followed by an inverse Arnold transformation to restore the original orientation of the modified image, generating the stego image. The authors conduct comprehensive experimental evaluations to assess the effectiveness of their method, including both quantitative and qualitative analyses. The results demonstrate that the imperceptibility of the embedded data is well-preserved, ensuring its non-detectability, while also maintaining a substantial payload with minimal distortion in image quality. Overall, the paper presents a novel approach to image steganography that enhances secure communication by effectively concealing confidential data within cover images using the MPV technique.

III. EXISTING SYSTEM

Existing systems in image Steganography often face notable challenges, particularly in achieving a harmonious balance between security and capacity. Many conventional stenographic methods, such as LBS-based approaches, while simple and widely used, exhibit vulnerability to sophisticated attacks and can result in perceptible visual distortions in the carrier image. Furthermore, the trade-off between embedding capacity and detection resistance remains a persistent issue. Some existing systems focus on enhancing security but sacrifice capacity, limiting their practical utility for scenarios requiring the covert transmission of larger volumes of information. On the other hand, systems prioritizing higher capacity may compromise security, as increased payload size can make the hidden data more susceptible to detection through advanced steganalysis techniques. Striking an optimal balance between these competing demands is a formidable challenge faced by current image Steganography systems Maintaining the Integrity of the Specifications.

3.1 Problem with current scenario :

- The hacker would easily break the security of the text message.
- Some Steganography methods cause noticeable visual artifacts in the stego images, making it easier to detect the hidden data.
- Steganalysis techniques have become increasingly sophisticated, making it more challenging to create stenographic systems that can evade detection.
- Many Steganography tools lack user-friendly interfaces, hindering their widespread adoption and usability by non-experts.

IV. PROPOSED SYSTEM

Our proposed image Steganography system introduces a sophisticated approach to meet the escalating demands for multi-layered security and high capacity in covert communication. The system strategically integrates the strengths of two powerful encryption algorithms, Rivest–Shamir–Adleman (RSA), Advanced Encryption Standard (AES) and for securing textual information. In the encryption phase, the confidential text undergoes a dual-layer encryption process, leveraging AES for symmetric key encryption, ensuring efficient encoding, and RSA for secure asymmetric key encryption, facilitating a robust key exchange mechanism. This combination establishes a resilient foundation for the protection of sensitive information.

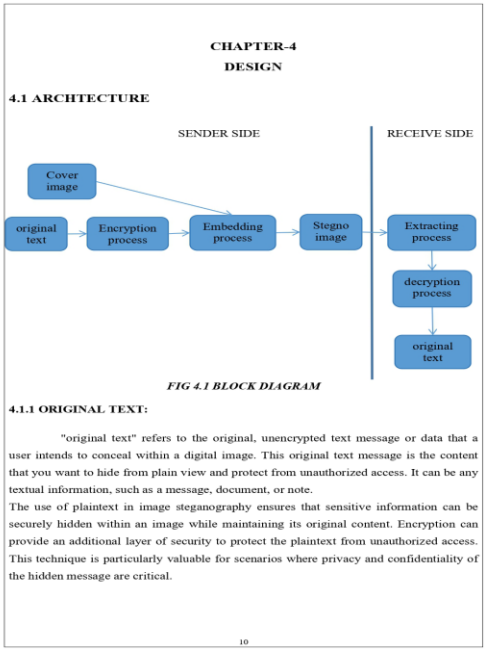

Fig1. Block diagram

Following the encryption phase, the system employs the F5 algorithm for key embedding into the cover image. The F5 algorithm is renowned for its capacity to hide substantial amounts of data within digital images while maintaining their visual integrity. This embedding phase ensures not only a high capacity for concealed information but also introduces an additional layer of security through the strategic integration of encryption and Steganography. The F5 algorithm operates seamlessly, preserving the aesthetic quality of the cover image and making the hidden information resistant to detection through visual inspection or steganalysis techniques.

4.1 Solution for existing system :

- Our proposed solution tackles the challenges present in current systems by combining AES and RSA for text encryption, along with the F5 algorithm for embedding keys into images.
- This solution offers a multi-layered approach to enhance both security and capacity. By leveraging AES and RSA, the system ensures a robust dual-layer encryption strategy. AES, known for its efficiency, symmetrically encrypts the text, while RSA provides secure asymmetric key encryption for key exchange.

- The integration of the F5 algorithm facilitates high- capacity Steganography, enabling the embedding of encrypted keys into images without compromising visual quality.
- The F5 algorithm's effectiveness in concealing substantial amounts of data within digital images addresses the capacity limitations faced by existing systems.

V. METHODOLOGY

The methodology outlined in this paper is divided into four phases as depicted in Fig 2.

Phase 1: Text Encryption (AES): (i) Input: Take a plain text text message M as input. (ii) Binary Conversion: Convert the text message M into its binary representation $B_{M.}$ (iii) AES Encryption: Generate a random secret key K_{AES}. Apply AES encryption to the binary message B_M using the secret key K_{AES} to obtain the encrypted binary message C_{AES} (B_M, K_{AES}).

Phase 2: Key Generation and Encryption (RSA): (i) RSA Key Pair Generation: Generate an RSA key pair ($K_{RSA\ public}$, $K_{RSA\ private}$). (ii) AES Key Encryption: Encrypt AES secret key K_{AES} using RSA public key $K_{RSApublic}$ to obtain the encrypted AES key C_{RSA}(K_{AES}, $K_{RSApublic}$).

Phase 3: Steganography Module: (i) Integration of AES-Encrypted Text and RSA-Encrypted Key: Combine the AES-Encrypted binary message C_{AES} (B_M, K_{AES}) and the F5-embedded RSA-Encrypted AES key into a unified steganographic payload.(ii) Stego-Image Generation: Generate the stego-image Istego by combining the modified frequency coefficients with the original image Icover in the frequency domain. Apply the inverse FFT to convert Istego back to the spatial domain.

Phase 4: Output: The final output is the stego-image I_{stego} containing both the encrypted text message and the encrypted AES key.

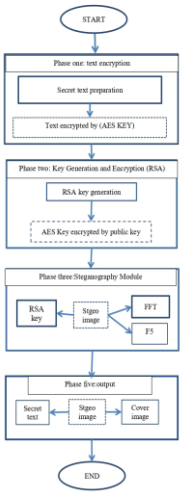

Fig2. The General Flowchart of the Proposed Methodology

VI. RESULT AND DISCUSSION

The study on image Steganography employing multi-layer and high-capacity techniques, along with AES and RSA encryption for text confidentiality, alongside the F5 algorithm for embedding, reveal a successful integration of advanced methods to enhance data hiding capabilities within digital images.

Advanced Encryption Standard (AES) was employed for data encryption. Developed by two Belgian cryptographers,Vincent Rijmen, Joan Daemen. AES, derived from the Rijndael cipher, is a symmetric block cipher. It was designed to replace DES as the recommended standard for various applications.

There are three different key lengths: The size of the key used in an AES cipher dictates the number of transformation rounds required to convert the plaintext into ciphertext.

The number of rounds varies according to the key length:

- For a 128-bit key, there are 10 rounds.
- For a 192-bit key, there are 12 rounds.

- For a 256-bit key, there are 14 rounds.

Although AES efficiently encrypts substantial data volumes, securely transmitting the AES key itself presents a challenge, particularly across insecure channels such as the internet. To address this, RSA, an asymmetric encryption algorithm, is utilized. RSA employs two keys: One key is used for encryption, known as the public key, and another for decryption, know as private key. Using the recipient's public key, the sender encrypts the AES key, ensuring that only the recipient, who possesses the corresponding private key, can decrypt it. This integration of AES and RSA establishes a resilient and secure method for encrypting and transmitting data over insecure channels.

The integration of AES and RSA algorithms for text encryption, alongside the F5 algorithm for embedding, constitutes the backbone of our multi-layer, high-capacity image steganography approach. The F5 algorithm orchestrates a sophisticated embedding process, meticulously concealing encrypted text within the image while preserving imperceptibility and maximizing payload capacity. Beginning with the selection of embedding locations based on a secret key, F5 encodes the encrypted message into binary format before dynamically adjusting embedding strength to optimize capacity. These results underscore the robustness of our image steganography technique, demonstrating its ability to securely conceal substantial amounts of data within images while maintaining visual fidelity.

The following Fig. 3 and Fig. 4, illustrate the cover image and the image with the secret text, respectively. The original image had a size of 776,355 bytes, while the image containing the hidden ciphertext grew to a size of 1,682,318 bytes.

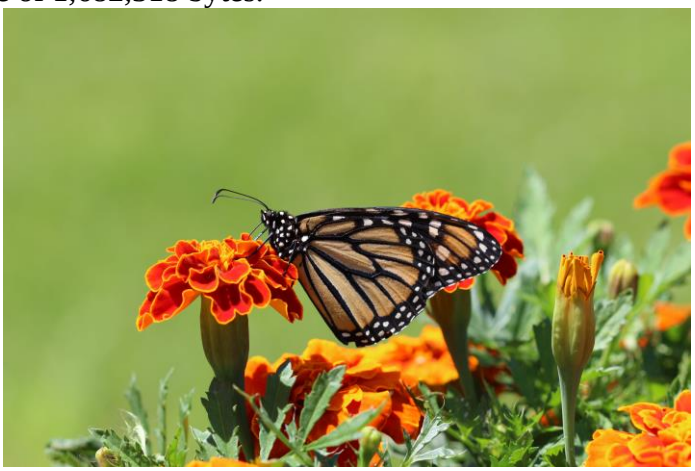

Fig3. Cover Image

Fig4. Stego-image

VII.CONCLUSION

we proposed a comprehensive image Steganography system designed for multi-level security and high capacity. The system integrates robust text encryption through the AES and the RSA algorithm, ensuring a secure foundation for data confidentiality. For efficient and high-capacity data embedding, we employed the F5 algorithm, allowing for optimal concealment of information within the image.

Our experimental results underscore the efficacy of the proposed method. Through rigorous testing and analysis, we observed consistently high levels of security, as evidenced by the resilience of the encryption algorithms against various attacks. Simultaneously, the F5 algorithm demonstrated remarkable efficiency in maximizing payload capacity while minimizing perceptual impact on the stego image.

VIII. REFERENCES

[1] Ali Ahmed and Abdelmotalib Ahmed, "A Secure Image Steganography using LSB and Double XOR Operations, " IJCSNS International Journal of Computer Science and Network Security, vol.20 No.5, May 2020

[2] A. Gupta, H. Shukla, and M. Gupta, "A Secure Image Steganography using X86 Assembly LSB," NEU Journal for Artificial Intelligence and Internet of Things, vol. 1, no. 1, pp. 38-47, 2022.

[3] jagan raj jayapandiyan ,c. Kavitha, and k. sakthivel, "Enhanced Least Significant Bit Replacement," *IEEE Access,* vol.8*, July 14, 2020.*

[4] M. R. Islam , T. R. Tanni , S. Parvin , M. J. Sultana & A. Siddiqa, " A modified LSB image Steganography method using filtering algorithm and stream of password." Information Security Journal: A Global Perspective, 29 Nov 2020.

[5] Srilekha Mukherjeea,* , Subhajit Roya , Goutam Sanyala , "Image Steganography Using Mid Position Value Technique." International Conference on Computational Intelligence and Data Science , Procedia Computer Science 132 (2018) 461–468.

[6] Fatmah abdularhman boathman and budoor salem edhah, " towards agent-based LSB image Steganography system.", journal of intelligent systems, may 14, 2021.

[7] Jiufen Liu1, Chunfang Yang1,2* , Junchao Wang1 and Yanan Shi, "Stego key recovery method for F5 Steganography with matrix encoding." EURASIP Journal on Image and Video Processing" , (2020).

[8] Sonali K. Powar1, H.T. Dinde2, Radhika.M. Patil3. "A Study and Literature Review on Various Image Steganography Techniques," International Research Journal of Engineering and Technology (IRJET), Volume: 07 Issue: 08 | Aug 2020.

[9] R SHANTHAKUMARI1,* and S MALLIGA2."Dual-layer security of image Steganography based on IDEA and LSBG algorithm in the cloud environment," Indian Academy of Sciences, 20 April 2019.

[10] Hemant R. Deshmukh, Mahip M. Bartere, "Enhancement of Image Steganography Technique for Improvement of Security," International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume-8 Issue-4, February 2019.

[11] Pooja Rawat, Amit Kumar Pandey, Rajendra Singh Kushwah, "Enhancement in Time Efficiency and Expected Capacity of F5 Algorithm," International Conference on Computational Intelligence and Communication Networks, 2015.

[12] Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav, "Steganography Using Least Significant Bit Algorithm" International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 3, May-Jun 2012.