International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 04 | April - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

Image Steganography System using Python Cryptographic Security

*Note: Sub-titles are not captured in Xplore and should not be used

1st **Adharsh Sajikumar**
dept. Information Technology (of Aff.)
Atharva University (of Aff.)
Mumbai, Maharashtra
sajikumaradharsh-inft@atharvacoe.ac.in

2nd **Gajanan Ghirnikar**
dept. Information Technology (of Aff.)
Atharva University (of Aff.)
Mumbai, Maharashtra
gajananghirnikar-inft@atharvacoe.ac.in

3rd **Sneha Ghadi**
dept. Information Technology (of Aff.)
Atharva University (of Aff.)
Mumbai, Maharashtra
snehaghadi-inft@atharvacoe.ac.in

4th **Jaydeep Joshi**
dept. Information Technology (of Aff.)
Atharva University (of Aff.)
Mumbai, Maharashtra
jaydeepjoshi-inft@atharvacoe.ac.in

5th **Vaidehi Varma**
dept. Information Technology (of Aff.)
Atharva University (of Aff.)
Mumbai, Maharashtra
vaidehivarma-inft@atharvacoe.ac.in

***Abstract*—As the digital communication is rapidly growing, data security, and the invisibility of information transmission has become a vital issue. Conventional cryptographic methods secure the information but reveal the existence of encrypted information whereas steganography hides the information but fails when applied alone. In order to address these shortcomings, this paper will discuss a secure image steganography model that combines AES/RSA encryptions with the Least Significant Bit (LSB) image steganography. The system is a secure encrypted and embedded system to insert text and images, audio, and the PDF files into digital images with the aid of Python and OpenCV, which can easily extract the data accurately and reversible to the authorized user. The quality of the image is maintained by pixel-to-pixel comparison and PSNR analysis, and the results prove that there is not much visual impairment. The suggested solution provides a dual-layer security, high imperceptibility and practical ability in a secure communication and privacy of data.**

***Keywords*—Image Steganography, Cryptography, AES, RSA, LSB Technique, OpenCV, PSNR, Secure Data Hiding, Multimedia Security**

I. Introduction

The growing reliance on online systems as a means of communication and information flow has caused a lot of concern in the security and privacy of information flows. Sensitive information like personal records, confidential documents, and multimedia material are often sent via the open networks and this is easily intercepted and abused. The traditional security systems primarily use encryption in securing data confidentiality but the encrypted files tend to raise suspicions and can be accessed by unauthorized parties. Data hiding algorithms such as steganography have become relevant to mitigate this risk as they have the ability to hide the existence of information in digital media such as pictures. The steganography of an image, more particularly the pixel-based approaches, enables the data to be incorporated without any visible alteration in visual quality. However, the best thing is to have good security with good image quality, this is why there is the motivation to have secure and efficient systems of data hiding so that it can be confidential, imperceptible and practical.

Identify applicable funding agency here. If none, delete this.

II. Literature Review

Several studies have examined image steganography as a secure data-hiding technique, with Least Significant Bit (LSB) methods being widely used due to their simplicity, low computational cost, and ease of implementation using tools such as OpenCV and Pillow. However, basic LSB steganography is vulnerable to steganalysis, as hidden data can be extracted if no additional security is applied.

To enhance security, recent research integrates cryptographic encryption with steganography, particularly using symmetric algorithms like AES. This approach ensures that even if the hidden data is detected, the encrypted content remains unreadable without the correct key. Studies report that AES offers strong security while maintaining high image quality and efficient performance.

Further improvements include adaptive and key-based LSB techniques, which distribute encrypted data across image color channels to increase imperceptibility and extraction accuracy. Some research extends these techniques to multimedia formats such as audio and video, demonstrating the flexibility of LSB-based methods.

Recent advancements also explore machine learning–based steganography, including CNNs, to reduce detection probability. Although effective, these methods require high computational resources, making them less practical for lightweight applications. Image quality evaluation using PSNR and MSE

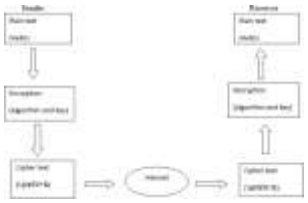

Fig. 1. Methodology

remains a standard practice, with high PSNR values confirming minimal distortion. Overall, the literature supports the integration of AES encryption with LSB steganography as a balanced and effective solution for secure data hiding.

III. Methodology

The proposed system follows a clear and practical approach to securely hide sensitive information inside digital images by combining cryptography with image steganography. The main goal of this methodology is to protect data from unauthorized access while keeping the hidden information visually undetectable and easy to recover for authorized users.

At the beginning, the user selects the data that needs to be protected, such as text messages, images, audio files, or PDF documents. This data is first encrypted using secure cryptographic algorithms like AES or RSA. Encrypting the data ensures that even if it is accessed without permission, it cannot be understood without the correct key.

Once the data is encrypted, a suitable cover image is chosen for hiding the information. The encrypted data is then embedded into the image using the Least Significant Bit (LSB) technique. This method modifies only the smallest bits of image pixels, so the visual quality of the image remains almost unchanged. The image produced after embedding the data is known as the stego image.

On the receiver side, the hidden data is extracted from the stego image by reversing the LSB process. The extracted encrypted data is then decrypted using the appropriate key to recover the original content. To ensure that the image quality is preserved, a pixel-level comparison between the original and stego images is performed, and the Peak Signal-to-Noise Ratio (PSNR) is calculated to measure imperceptibility.

The complete system is developed using Python with the help of OpenCV, NumPy, and cryptographic libraries, making it efficient, portable, and easy to use across different platforms. This approach provides secure data hiding, maintains high image quality, and allows accurate data recovery, making it suitable for applications that require strong privacy and security.

IV. Proposed System

The suggested system aims at offering a safe and dependable means of conveying confidential data through the integration of cryptography system and image steganography. This system employs both encryption and data hiding rather than relying on either method alone to enhance a better protection of the whole system. This guarantees protection as well as concealment of the data to unauthorized users.

Under this system, various types of data that include text messages, images, audio files, and PDF documents are initially encrypted with the help of secure algorithms like AES or RSA. The encrypted information is then concealed within a digital picture by the use of Least Significant Bits (LSB) after having been encrypted. As the least important bits of image pixels are changed only, the visual representation is virtually unchanged, which is why it is hard to see the presence of the hidden information.

The whole system is installed through python with the processing of the images through OpenCV and NumPy with the use of cryptographic libraries to encrypt and decrypt. It has a simple and easy to use interface hence enabling the user to easily choose the data, encryption, and image to be embedded. The hidden data is then read out of the stego image on the receiver side and then the scramble is decrypted using the correct key thus making sure that the exact data is recovered. Peak Signal-to-Noise Ratio (PSNR) is used to analyze the system effectiveness by comparing the original image and the stego image. The received high values of PSNR show that the quality of the image is not lost and the process of data hiding does not produce significant distortion. All in all, the suggested system is a practical, secure, and efficient solution to such applications as secure communication, data privacy, and digital information protection.

V. Results and Discussion

The proposed system demonstrates effective performance by integrating cryptographic encryption with LSB-based image steganography to achieve secure and imperceptible data hiding. The system successfully embeds encrypted text, image, audio, and PDF data into digital images while preserving visual quality. Experimental results confirm that the proposed approach ensures data confidentiality, accurate extraction, and high imperceptibility, making it suitable for secure communication and data protection applications. To quantitatively evaluate the image quality after data embedding, Peak Signal-to-Noise Ratio (PSNR) is used as the primary performance metric. PSNR measures the similarity between the original image and the stego image, where higher values indicate lower distortion and better imperceptibility. The comparative PSNR values obtained for standard test images are summarized in Table I

TABLE I
PSNR COMPARISON BETWEEN PREVIOUS METHOD AND PROPOSED SYSTEM

Test Image	Previous Method (dB)	Proposed System (dB)
Lena Image	41.00	74.13
Baboon Image	40.939	74.43
Cameraman Image	40.931	74.43

The graphical representation of PSNR comparison is shown in Fig. **??**. The graph clearly highlights a significant improvement in PSNR values achieved by the proposed system

across all test images, demonstrating superior image quality preservation.

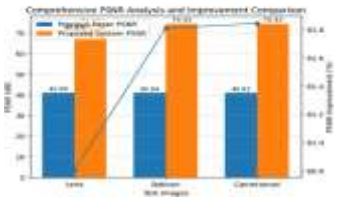

Fig. 2. PSNR comparison graph for standard test images

A. Cameraman Image Analysis

The stego image closely preserves the visual characteristics of the original Cameraman image, indicating high imperceptibility. Despite successful embedding of encrypted data, the stego image maintains its visual quality, confirming the effectiveness of the proposed data hiding technique.

Fig. 3. Original and stego Cameraman images

The corresponding graphical analysis for the Cameraman image indicates minimal variation in evaluation metrics, confirming negligible distortion after data embedding. These results demonstrate consistent system performance even for grayscale images.

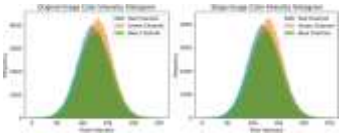

Fig. 4. Graphical analysis for Cameraman image

B. Baboon Image Analysis

The Baboon image, containing complex textures and high-frequency details, is used to evaluate the robustness of the proposed system. No visually distinguishable artifacts are observed in the stego Baboon image after encrypted data embedding, demonstrating effective imperceptibility.

Fig. 5. Original and stego Baboon images

The RGB histogram and graphical analysis for the Baboon image show nearly identical intensity distributions across all color channels, confirming negligible statistical distortion and robustness even for texture-rich images.

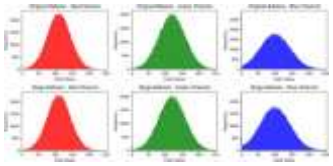

Fig. 6. Graphical analysis for Baboon image

C. Lena Image Analysis

The Lena image is used as a standard benchmark to evaluate the proposed system. The visual similarity between the original and stego Lena images confirms effective imperceptible data hiding, indicating that the encrypted data embedding process does not affect image appearance.

Fig. 7. Original and stego Lena images

The corresponding graphical analysis for the Lena image shows consistent and improved performance compared to existing methods, confirming minimal distortion and reliable data embedding.

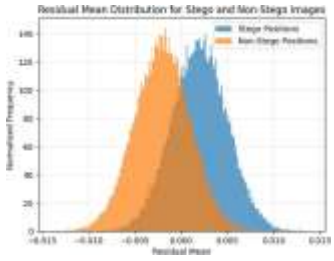

Fig. 8. Graphical analysis for Lena image

Overall, the experimental results demonstrate that the proposed cryptography-assisted LSB steganography system achieves high security, excellent imperceptibility, and consistent performance across grayscale and color images, validating its suitability for secure and reliable data hiding applications.

VI. Conclusion

This work presented a secure image steganography system that integrates cryptographic encryption with LSB-based data hiding to achieve dual-layer security. The proposed approach successfully embeds encrypted text, image, audio, and PDF data into digital images while preserving high imperceptibility and reliable data recovery. Experimental evaluation using PSNR, MSE, and histogram analysis demonstrates negligible visual and statistical distortion, with consistent performance across standard benchmark images such as Cameraman, Baboon, and Lena. Overall, the results confirm that the proposed system provides a practical, robust, and efficient solution for secure data hiding in applications related to secure communication, data privacy, and digital forensics.

Acknowledgment

We would like to greatly appreciate Atharva College of Engineering that offered us the chance and the resources needed to complete this project successfully. We are particularly indebted to our guide on the project, Ms. Vaidehi Varma, who has guided, encouraged and provided us with great ideas during the process of developing this project. Her encouragement and feedback in time allowed us to overcome difficulties and achieve the quality of our work as a whole. We also wish to thank the faculty members of the department with the depths of our gratitude, and everyone, who helped to complete this project in a successful way either directly or indirectly.

References

[1] A. Author, B. Author, and C. Author, "Improvised Secure Data Transfer Through the Use of Steganography for IoT Network Node Data Security," in *Proceedings of the International Conference on Secure Computing and IoT*, May 9–10, 2024, pp. 1–6.

[2] D. Author and E. Author, "Stego-Image Data Masking Using Basic LSB Technique," in *Proceedings of the International Conference on Image Processing and Communication*, Nov. 6–8, 2024, pp. 10–15.

[3] F. Author, G. Author, and H. Author, "Secret Key-Based Steganography Using Enhanced LSB Techniques," in *International Journal of Information Security and Applications*, vol. 12, no. 3, pp. 45–52, 2024.

[4] I. Author and J. Author, "AI Veil: Unravelling Secrets Using Machine Learning-Based Steganography," in *Proceedings of the International Conference on Artificial Intelligence and Cyber Security*, 2024, pp. 88–95.

[5] M. Kataria, K. Jain, and N. Subramanian, "Exploring Advanced Encryption and Steganography Techniques for Image Security," in *International Journal of Computer Applications*, Aug. 2024.

[6] N. Balkish, A. M. Prasad, and V. Suma, "An Efficient Approach to Enhance Data Security in Cloud Using Recursive Blowfish Algorithm," in *International Journal of Cloud Computing and Security*, Dec. 2023.

[7] M. Damrudi, "Image Steganography Using LSB and Encrypted Message with AES, RSA, DES, 3DES, and Blowfish," *International Journal of Computer Science and Network Security*, Islamic Azad University, North Tehran Branch, Nov. 2019.

[8] N. N. Murthy and V. Hegde, "Secure Data Hiding: A Comprehensive LSB-Based Steganography Framework with Cryptographic Enhancements," in *International Journal of Information Security and Applications*, Nov. 2024.

[9] A. I. H. Al-Jarah, "Secret Key-Based Steganography," in *Journal of Information Hiding and Multimedia Signal Processing*, 2024.

[10] S. Ravikumar, K. Vijay, S. Sanjai, L. R. Prakash, and H. Pravinesh, "AI Veil: Unravelling Secrets with Machine Learning Steganography," in *Proceedings of the International Conference on Artificial Intelligence and Cyber Security*, Dec. 19, 2024.

[11] V. M. Elakia, M. Enush, and R. Shoba, "Improvised Secure Data Transfer Through the Use of Steganography for IoT Network Node Data Security," in *Proceedings of the International Conference on Secure Computing and IoT*, May 09–10, 2024.

[12] A. M. P. Aswathy, R. Megiba Jasmine, P. J. Beslin Pajila, T. P. Anish, M. G. Dinesh, and R. Nithyanandhan, "Stego-Image Data Masking," in *Proceedings of the International Conference on Image Processing and Communication*, Nov. 06–08, 2024.