*International Journal of Recent Research and Review, Vol. XVIII, Issue 1, March 2025*
ISSN 2277 – 8322

# Multi-Layered Secure Framework for Digital Data Protection Using Steganography, Embedding, and Cryptographic Techniques

Shailendra Kumar
M.Tech Scholar
Department of Computer Science and Engineering
Rajasthan Institute of Engineering & Technology, Jaipur

Ms. Pragya Bharti
Assistant Professor
Department of Computer Science and Engineering
Rajasthan Institute of Engineering & Technology, Jaipur

**Abstract:** The internet is a primary medium for data exchange, but digital content faces challenges such as copyright protection, authentication, and security. This work integrates embedding, hiding, and encryption to enhance data security with multiple protection layers. First, secret text is hidden in an image using DCT steganography, generating a Stego image. Then, LSB embedding is applied to conceal the Stego image within a cover image, forming an embedded image. MSE and PSNR values are calculated to ensure quality, followed by encryption using the RSA algorithm. This approach provides robust security, making unauthorized access extremely difficult.

**Keywords:** DCT, RSA, LSB, Cryptograph, Digital Data, Security

## 1. Introduction

In the era of digital innovation, the internet plays a crucial role in data exchange. With advancements in information technology, digital media has become one of the most widely used tools for transmitting data, including text, images, audio, and video over public networks [1-4]. A significant portion of this digital content consists of images, which are widely used in applications such as online communication, news platforms, e-commerce, emails, digital books, and more. However, digital content faces several challenges, including authentication, verification, and copyright protection. Various techniques such as encryption, embedding, and steganography can be employed to safeguard digital data [5-8].

Image encryption is a key area of research in cryptography and network security, especially for digital communication applications. This process converts original digital data into encrypted data, making it completely different from the original. Various encryption algorithms and techniques are used to ensure data security [9-12].

Images are a prevalent mode of communication across multiple fields, including medicine, research, industry, and military applications. Large-scale image transfers often occur over unsecure networks, making it essential to apply robust encryption mechanisms to prevent unauthorized access to sensitive data [13-14]. The advantage of images lies in their ability to carry extensive multimedia information, necessitating protection. Encryption serves as an effective security measure, ensuring the confidentiality, integrity, and accuracy of images during transmission and storage over the internet [15-16].

## 2. Proposed Methodology

In the proposed approach, a combination of embedding, hiding, and encryption techniques is utilized to enhance the security of digital data, ensuring multiple layers of protection that are highly resistant to unauthorized access.

Initially, the secret text is embedded within a secret image using the Discrete Cosine Transform (DCT) steganography technique, resulting in a stego image. This stego image visually resembles the original secret image but also contains the hidden text. Next, the Least Significant Bit (LSB) embedding technique is applied to the stego image and a cover image, producing an embedded image. While the embedded image appears identical to the cover image, it discreetly contains the stego image as well.

Following this, the Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) values are computed to assess the quality of hiding, where a low MSE and high PSNR indicate better concealment. Finally, cryptographic techniques are applied to the embedded image, generating an encrypted image that is entirely distinct from the original images and data. The encryption process employs the asymmetric RSA algorithm, further reinforcing security. By implementing this proposed technique, an exceptionally robust level of security is achieved for both the secret text and the secret image, making it highly challenging for unauthorized individuals to breach. The flowchart of the proposed work is illustrated in Figure 1.

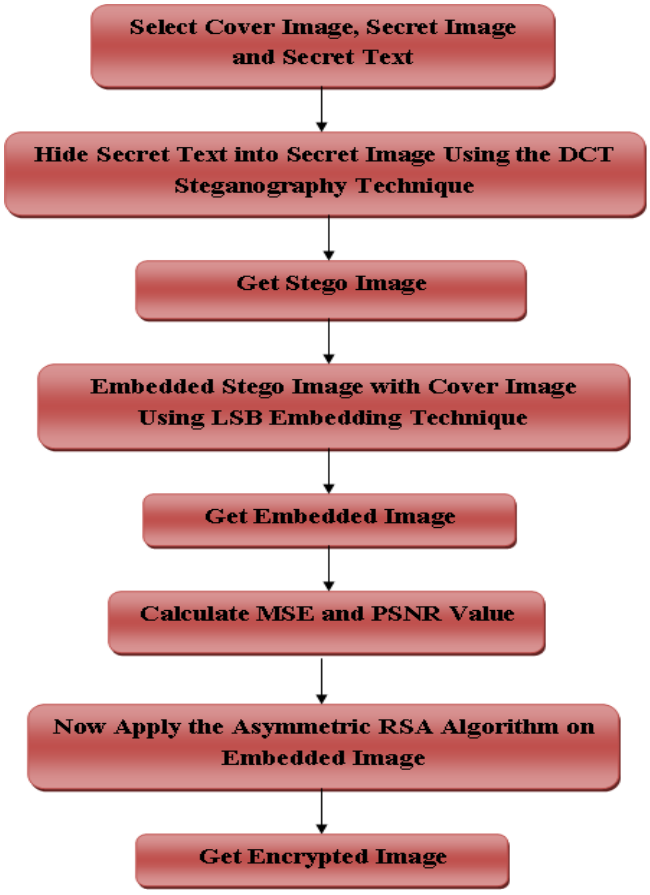



**Figure 3.1: Flowchart of the Proposed Work**

## 3. Results and Discussion

Take the cover image of nature view (shown in the Figure 2) and secret image of red flower (shown in the Figure 3). The taken secret text data is takenFlower is shown in the Figure4.

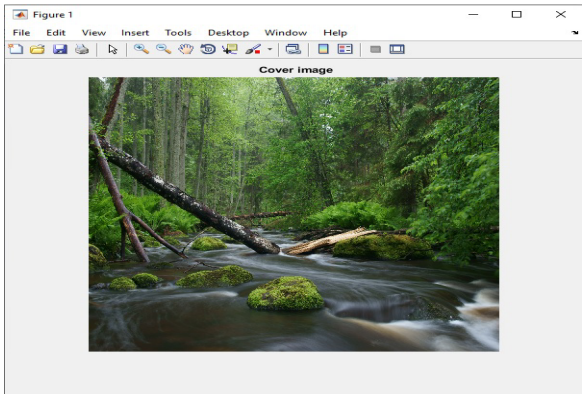



**Figure 2: Cover Image of Nature View**

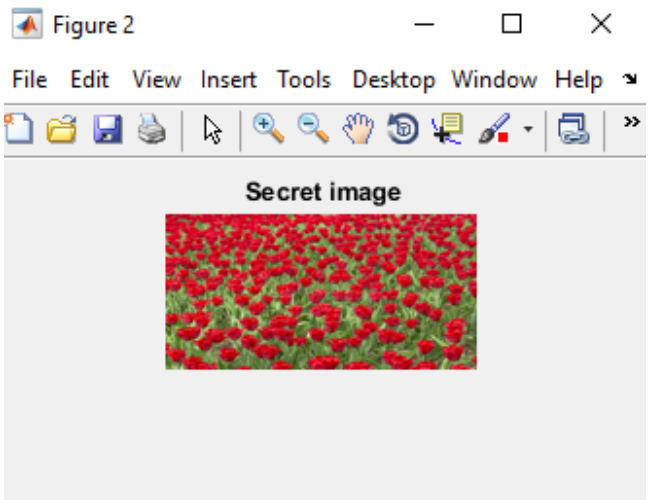



**Figure 3: Secret Image of Red Flower**

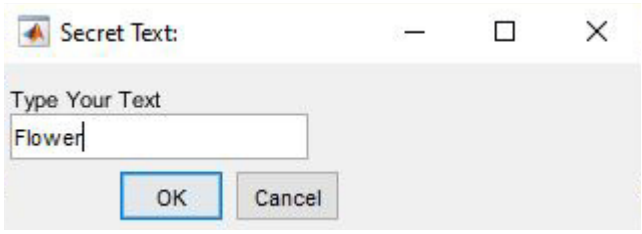



**Figure 4: Secret Text Flower**

Figure 5 displays the stego image, which appears identical to the secret image but contains hidden text using the DCT Steganography technique..

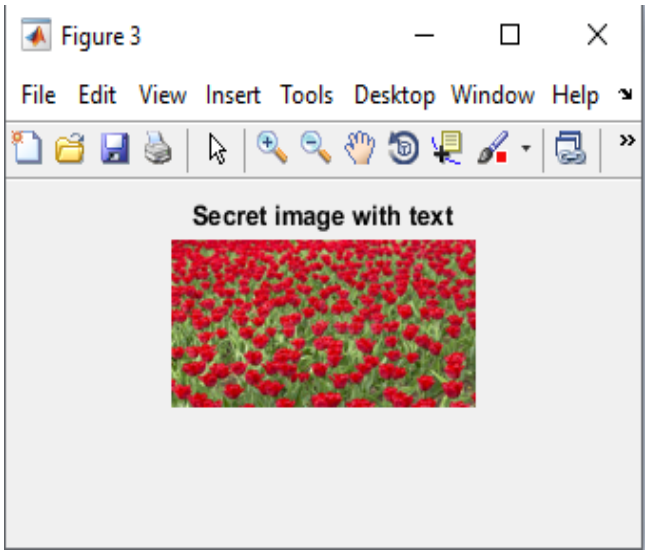


**Figure 5: Secret Image with Secret Text (Stego Image)**

Using the LSB embedding technique, the stego image was embedded into the cover image, resulting in the embedded image, as shown in Figure 6.

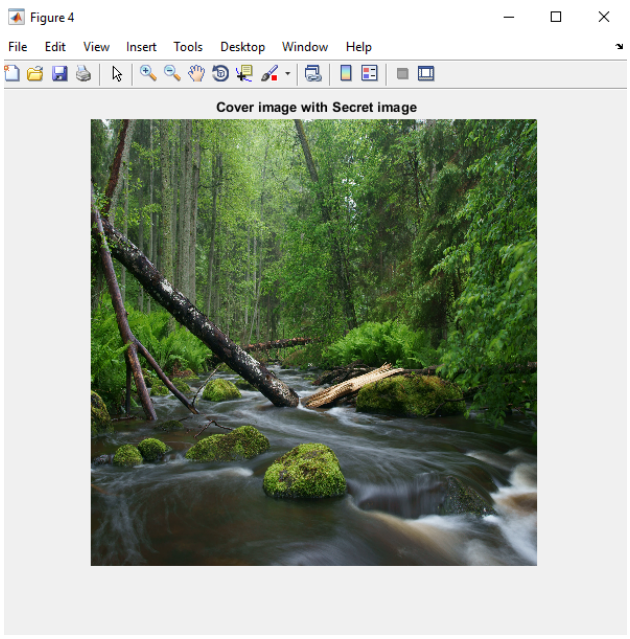
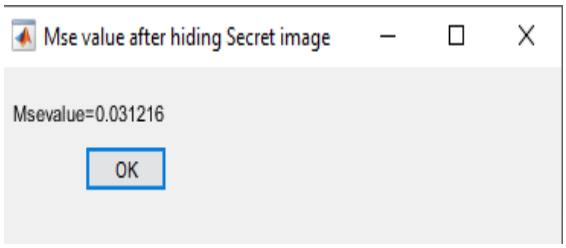



**Figure 6: Embedded Image**

After getting the embedded image calculate the MSE and PSNR value which is shown in Figure 7. Using proposed technique got the MSE value is 0.031216 and PSNR value is 63.187 .



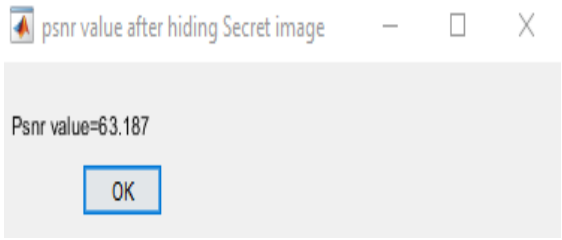




**Figure 7: MSE and PSNR Value**

Now apply the asymmetric RSA algorithm on the embedded image and get the encrypted image that is totally differ then the all the taken image and the encrypted image is displayed in the Figure8.

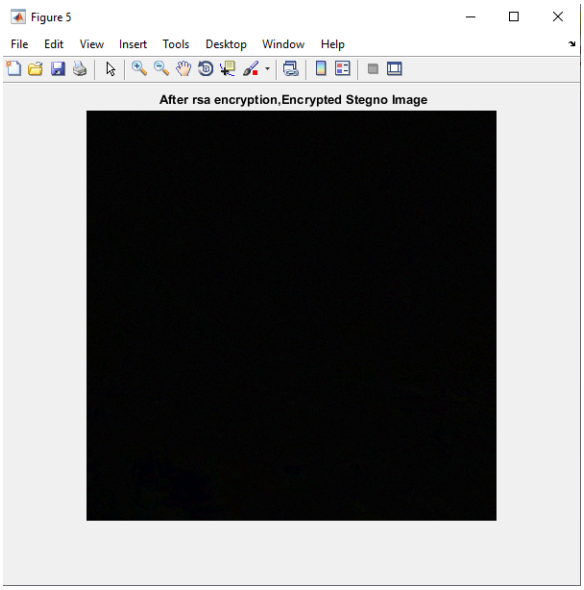



**Figure 8: Encrypted Image**

All these processes are performed at the sender's end to securely transmit the secret text data and secret image from one person to another. At the receiver's end, the reverse process is carried out to retrieve the decrypted cover image, the decoded secret image, and the extracted secret text data. Figure 9 displays the decrypted cover image, Figure 10 shows the decoded secret image of a red flower, and

Figure 11 presents the extracted secret text data ('Flower').

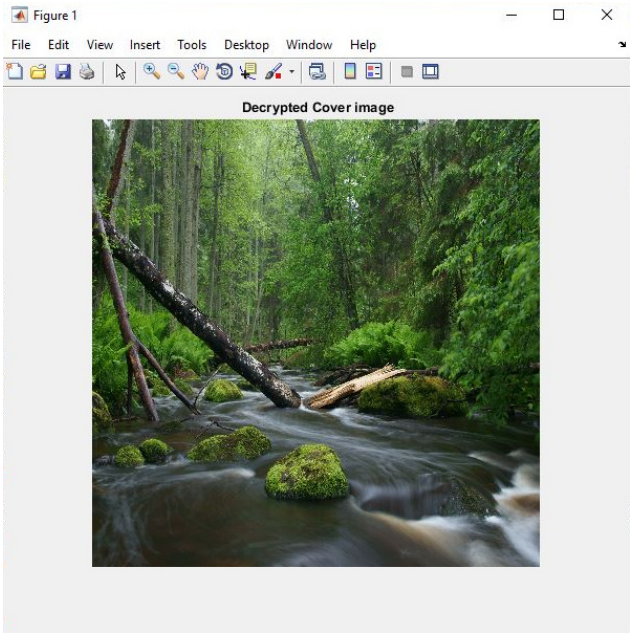



**Figure 9: Decrypted Cover Image**

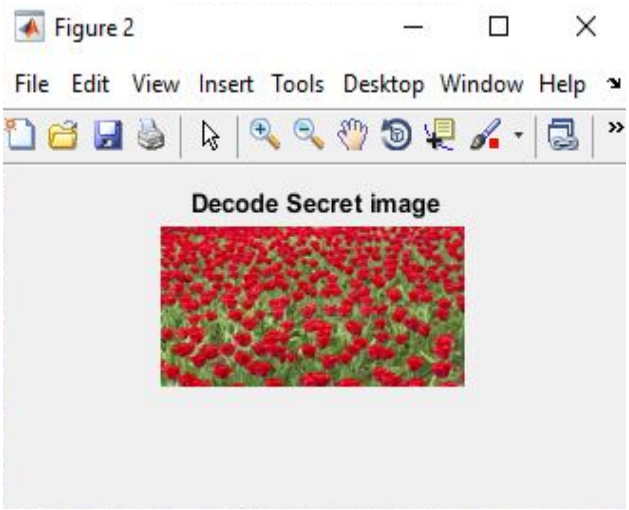



**Figure 10: Decoded Secret Image of Red Flowers**

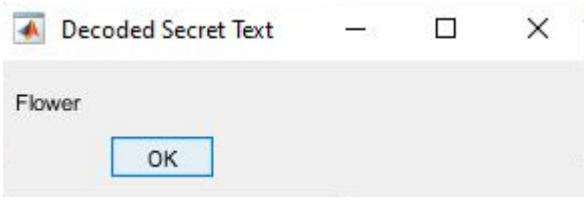



**Figure 11: Decoded Secret Text**

## 4. Conclusion

This research presents a multi-layered security approach integrating embedding, hiding, and encryption techniques to enhance the protection of digital data. The proposed method effectively conceals secret text within an image using DCT steganography, followed by LSB embedding to further hide the stego image within a cover image. The quality of hiding is evaluated using MSE and PSNR values, ensuring minimal distortion. Finally, the RSA encryption algorithm is applied, transforming the embedded image into an encrypted form that is highly secure and resistant to unauthorized access. The results demonstrate that the proposed technique achieves robust data security while maintaining image quality. The encrypted data can only be retrieved by authorized recipients using the reverse decryption process, ensuring safe and confidential transmission over unsecured networks. This approach is highly beneficial for applications requiring secure data exchange, such as military communication, medical imaging, and confidential digital transactions.

## References

[1]. Ramyashree, P. S. Venugopala, S. Raghavendra and V. S. Kubihal, "Enhancing Secure Medical Data Communication Through Integration of LSB and DCT for Robust Analysis in

Image Steganography," in IEEE Access, vol. 13, pp. 1566-1580, 2025.

[2]. S. N. Shilaskar, V. B. Mathapati, S. L. Mutekar, M. G. Nikam and S. Bhatlawande, "Comparative Analysis of Steganography Techniques Using ELSB, FFT and DCT," IEEE International Conference on Multi-Agent Systems for Collaborative Intelligence (ICMSCI), pp. 248-256, 2025.

[3]. Dr. Himanshu Arora, Gaurav Kumar Soni, Deepti Arora, "Analysis and Performance Overview of RSA Algorithm", International Journal of Emerging Technology and Advanced Engineering, Vol. 8, pp. 9-12, 2018.

[4]. G. K. Soni, H. Arora, B. Jain, "A Novel Image Encryption Technique Using Arnold Transform and Asymmetric RSA Algorithm", Springer International Conference on Artificial Intelligence: Advances and Applications 2019 Algorithm for Intelligence System, pp. 83-90, 2020.

[5]. H. Arora, R. Agarwal, P. Sharma, G. Shankar and D. Arora, "Image Security Utilizing Hybrid Model of Steganography and Asymmetric Cryptography Methods," 2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), pp. 277-280, 2023.

[6]. B. A. Dharani, B. Yashaswini, G. R. Shyashyankha Reddy and S. M. Rajagopal, "Multimodal Steganography: A Comparative Analysis of LSB and DCT Methods for Image and Audio Data Concealment," IEEE 9th International Conference for Convergence in Technology (I2CT), pp. 1-5, 2024.

[7]. H. Arora, G. K. Soni, R. K. Kushwaha and P. Prasoon, "Digital Image Security Based on the Hybrid Model of Image Hiding and Encryption," IEEE 2021 6th International Conference on Communication and Electronics Systems (ICCES), pp. 1153-1157, 2021.

[8]. Agarwal A, H. Arora, M. Mehra and D. Das, "Comparative Analysis of Image Security Using DCT, LSB and XOR Techniques," 2021 Second International Conference on Electronics and Sustainable Communication Systems (ICESC), pp. 1131-1136, 2021.

[9]. G. K. Soni, A. Rawat, S. Jain and S. K. Sharma, "A Pixel-Based Digital Medical Images Protection Using Genetic Algorithm with LSB Watermark Technique", Springer Smart Systems and IoT: Innovations in Computing. Smart Innovation, Systems and Technologies, Vol. 141, pp. 483-492, 2020.

[10]. V. Singh, M. Choubisa, G. K. Soni, "Enhanced Image Steganography Technique for Hiding Multiple Images in an Image Using LSB Technique", TEST Engineering Management, vol. 83, pp. 30561-30565, May-June 2020.

[11]. H. Sharma N. Seth, H. Kaushik, K. Sharma, "A comparitive analysis for Genetic Disease Detection Accuracy Through Machine Learning Models on Datasets", International Journal of Enhanced Research in Management & Computer Applications, Vol. 13, Issue. 8, 2024.

[12]. H. Arora, P. Kumar Sharma, K. Mitanshi and A. Choursia, "Enhanced Security of Digital Picture and Text Information with Hybride Model of Hiding and Encryption Techniques," 2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), pp. 1238-1241, 2022.

[13]. Himanshu Arora, Mr. Manish Kumar and Mr. Sanjay Tiwari, "Improve Image Security in Combination Method of LSB Stenography and RSA Encryption Algorithm", International Journal of Advanced Science and Technology, vol. 29, no. 8, pp. 6167-6177, 2020.

[14]. H. Kaushik, K. D. Gupta, "Machine learning based framework for semantic clone detection", Recent Advances in Sciences, Engineering, Information Technology & Management, pp. 52-58, 2025.

[15]. R. Misra, S. Vashistha, "A Review on Classification of Brain Tumor by Deep Learning Using Convolutional Neural Network", International Journal of Engineering Trends and Applications (IJETA), Vol. 11, Issue. 3, 2024.

[16]. H. Kaushik, K. D Gupta, "Code Clone Detection: An Empirical Study of Techniques for Software Engineering Practice", Lampyrid: The Journal of Bioluminescent Beetle Research, Vol. 13, pp. 61-72, 2023.

[17]. R. Misra, "A Novel Approach to Enhanced Digital Image Encryption Using the RSA Algorithm", International Conference on Engineering & Design (ICED), 2021.

[18]. A. Upadhyay, R. Misra, S. K. Henge, Y. Bhardwaj, "Protection of Digital Image and Text Information Security Using LSB and Crossover Techniques", Computational Vision and Bio-Inspired Computing. Advances in Intelligent Systems and Computing, Vol 1439, pp. 601-608, 2023.

[19]. Ran-Zan Wang, Chi-Fang Lin, Ja-Chen Lin, "Hiding data in images by optimal moderately significant-bit replacement" IEE Electron. Lett. 36 (25), 2000.