ISSN: 2582 - 6379
IJISEA Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed, Open Access Journal
2025, Volume 6 Issue 3
www.ijisea.org

Article Info
Date Received: 08/06/2025;
Date Revised: 19/07/2025;
Available Online: 22/08/2025;

A Robust Image Steganography Model with Three-Tier Encryption and Region-Based Embedding

1.Bandela Kalyani **2.Padala Srinivasa Reddy ***

Author Affiliations

1.Department Master of Computer Application(MCA), SVKP & Dr KS Raju Arts & Science College(A), Penugonda, W.G.Dt., A.P India, Kalyani.bandela18@gmail.com

2. Associate Professor , Department of Computer Science, SVKP & Dr KS Raju Arts &Science College(A), Penugonda, W.G.Dt,A.P India, psreddy1036@gmail.com

ABSTRACT

With the rapid evolution of Internet infrastructure, especially in e-healthcare, ensuring the security of sensitive medical records has become a paramount concern. Traditional cryptography protects the content of data, but not its presence. To address both, this project proposes a robust image steganography system integrating a novel Image Region Decomposition (IRD) technique with three-tier encryption (AES, RSA, and XOR/Base64). The method enhances imperceptibility and embedding capacity, particularly for grayscale MRI images. Each image is decomposed into low-, medium-, and high-intensity regions, with varying LSB embedding strategies per region to optimize data concealment. Testing on four MRI classes using PSNR, MSE, and SSIM demonstrates high fidelity and robustness against attacks. The combined use of steganography and encryption ensures both confidentiality and stealth, addressing limitations found in conventional approaches [1], [3], [6].

1. INTRODUCTION

In the digital age, images dominate online communication, making them ideal for steganographic applications [1], [2]. Image steganography allows hidden communication by embedding secret data in cover images without raising suspicion [3]. Unlike cryptography, which conceals the meaning of data, steganography hides its existence, offering a more covert channel for secure communication [4]. As computing environments become more interconnected, vulnerabilities to data breaches have grown, emphasizing the need for stronger security measures.

To address this, our project integrates encryption with image steganography using a three-tier security mechanism—combining AES for symmetric encryption, RSA for secure key sharing, and XOR/Base64 for lightweight obfuscation. These layers are followed by an LSB-based embedding

ISSN: 2582 - 6379
IJISEA Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed, Open Access Journal
2025, Volume 6 Issue 3
www.ijisea.org

technique that exploits region-based segmentation of grayscale MRI images, allowing greater control over embedding based on pixel intensity levels [3], [4], [6].
This hybrid approach strengthens the overall system by making it resilient to statistical and visual attacks while preserving image quality. By embedding encrypted data in medical images, our solution ensures that patient records remain secure and imperceptible during transmission across open networks—particularly crucial in the healthcare sector where data sensitivity is high [1].

2. LITERATURE SURVEY

Comprehensive survey of image steganography: Techniques, evaluations, and trends in future research[1]

Author: I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran:

Storing and communicating secret and/or private information has become part of our daily life whether it is for our employment or personal well-being. Therefore, secure storage and transmission of the secret information have received the undivided attention of many researchers. The techniques for hiding confidential data in inconspicuous digital media such as video, audio, and image are collectively termed as Steganography. Among various media types used, the popularity and availability of digital images are high and in this research work and hence, our focus is on implementing digital image steganography. The main challenge in designing a steganographic system is to maintain a fair trade-off between robustness, security, imperceptibility and higher bit embedding rate. This research article provides a thorough review of existing types of image steganography and the recent contributions in each category in multiple modalities. The article also provides a complete overview of image steganography including general operation, requirements, different aspects, different types and their performance evaluations. Different performance analysis measures for evaluating steganographic system are also discussed here. Moreover, we also discuss the strategy to select different cover media for different applications and a few state-of-the-art steganalysis systems.

3. PROPOSED SYSTEM

In this project we are using AES, Triple Des & LSB to encode messages inside images. Sender can share images with receiver and after login receiver can see all images shared by sender and then by clicking in image can decode and view images.

Advantages Of Proposed System : 1) High accuracy 2)High efficiency

System Architecture:

Architecture flow:

The word Steganography is derived from two Greek words- 'stegos' meaning 'to cover' and 'grayfia', meaning 'writing', thus translating to 'covered writing', or 'hidden writing'. Steganography is a method of hiding secret data, by embedding it into an audio, video, image, or text file. It is one of the methods employed to protect secret or sensitive data from malicious attacks.

How is it different from cryptography?

ISSN: 2582 - 6379
IJISEA Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed, Open Access Journal
2025, Volume 6 Issue 3
www.ijisea.org

Cryptography and steganography are both methods used to hide or protect secret data. However, they differ in the respect that cryptography makes the data unreadable, or hides the meaning of the data, while steganography hides the existence of the data. In layman's terms, cryptography is similar to writing a letter in a secret language: people can read it, but won't understand what it means. However, the existence of a (probably secret) message would be obvious to anyone who sees the letter, and if someone either knows or figures out your secret language, then your message can easily be read.

If you were to use steganography in the same situation, you would hide the letter inside a pair of socks that you would be gifting the intended recipient of the letter. To those who don't know about the message, it would look like there was nothing more to your gift than the socks. But the intended recipient knows what to look for, and finds the message hidden in them.

Similarly, if two users exchanged media files over the internet, it would be more difficult to determine whether these files contain hidden messages than if they were communicating using cryptography.

Cryptography is often used to supplement the security offered by steganography. Cryptography algorithms are used to encrypt secret data before embedding it into cover files.

Image Steganography

As the name suggests, Image Steganography refers to the process of hiding data within an image file. The image selected for this purpose is called the cover image and the image obtained after steganography is called the stegoimage.

How is it done?

An image is represented as an N*M (in case of grayscale images) or N*M*3 (in case of color images) matrix in memory, with each entry representing the intensity value of a pixel. In image steganography, a message is embedded into an image by altering the values of some pixels, which are chosen by an encryption algorithm. The recipient of the image must be aware of the same algorithm in order to know which pixels he or she must select to extract the message.

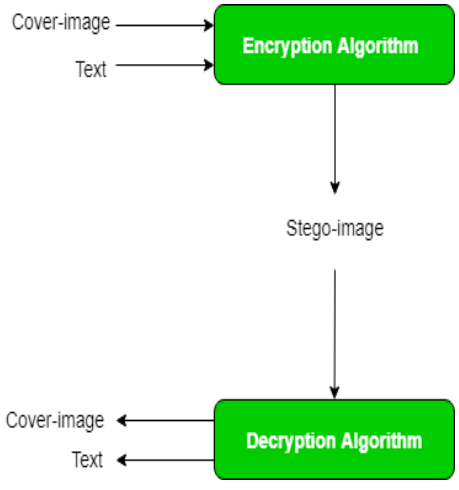

Figure 1: Shows the Encryption and Decryption flow

ISSN: 2582 - 6379
IJISEA Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed, Open Access Journal
2025, Volume 6 Issue 3
www.ijisea.org

4. METHODOLOGY

The project begins with preprocessing the input data, which includes a secret message or file that the user wants to hide within an image. The data is first passed through a three-layer encryption process to enhance its security before embedding. The three encryption techniques typically used are: AES (Advanced Encryption Standard) for symmetric encryption, RSA (Rivest–Shamir–Adleman) for public-key encryption, and a custom or lightweight obfuscation algorithm like XOR or Base64 encoding. This multi-layered encryption ensures that even if the hidden data is extracted, it remains unreadable without the proper keys.[3],[6].

Once encrypted, the binary output is converted into a bitstream and prepared for embedding into an image using steganography. The most common approach used is LSB (Least Significant Bit) technique, where each bit of the encrypted data is embedded into the least significant bits of the image's pixel values—typically in the RGB channels. This process is carefully performed to preserve the image's visual quality and make the alterations imperceptible to the human eye. Error checking and capacity verification steps ensure that the image can carry the full message without data loss or overflow.

On the receiver's end, the stego image is processed to extract the hidden bitstream, which is then decrypted in reverse order: first using the custom encoding (like Base64), then with the private key for RSA, and finally with the symmetric key for AES. The original message is restored after all decryption steps. The system is implemented using JAVA libraries such as PyCryptodome for AES/RSA, cv2 or PIL for image processing, and NumPy for pixel-level data manipulation. This methodology ensures data confidentiality, integrity, and stealth, combining encryption and steganography to form a robust secure communication channel.[3],[4],[6].

Algorithms

1. AES (Advanced Encryption Standard)

- **Type:** Symmetric Encryption
- **Purpose:** Encrypts the message using a shared secret key.
- **Key Sizes Supported:** 128 / 192 / 256 bits

Java Implementation:

```
import javax.crypto.Cipher;
import javax.crypto.KeyGenerator;
import javax.crypto.SecretKey;

SecretKey key = KeyGenerator.getInstance("AES").generateKey();
Cipher cipher = Cipher.getInstance("AES");
cipher.init(Cipher.ENCRYPT_MODE, key);
byte[] encrypted = cipher.doFinal(message.getBytes());
```

ISSN: 2582 - 6379
IJISEA Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed, Open Access Journal
2025, Volume 6 Issue 3
www.ijisea.org

2. RSA (Rivest–Shamir–Adleman)

- **Type:** Asymmetric Encryption
- **Purpose:** Secures the AES key using public/private key pair.

Java Implementation:

```
import javax.crypto.Cipher;
import java.security.KeyPair;
import java.security.KeyPairGenerator;

KeyPairGenerator keyGen = KeyPairGenerator.getInstance("RSA");
keyGen.initialize(2048);
KeyPair pair = keyGen.generateKeyPair();

Cipher cipher = Cipher.getInstance("RSA");
cipher.init(Cipher.ENCRYPT_MODE, pair.getPublic());
byte[] encryptedKey = cipher.doFinal(aesKey.getEncoded());
```

3. Base64 or XOR Obfuscation

- **Purpose:** Adds a simple obfuscation layer to confuse intruders.

Base64 (Encoding):

```
import java.util.Base64;

String encoded = Base64.getEncoder().encodeToString(encryptedData);
```

XOR Encryption:

```
public static String xorEncrypt(String data, char key) {
   char[] chars = data.toCharArray();
   for (int i = 0; i < chars.length; i++) {
      chars[i] ^= key;
   }
   return new String(chars);
}
```

4. LSB Steganography (Least Significant Bit)

- **Purpose:** Hides encrypted data within the pixel values of an image.
- **Approach:** Modify the **LSB (Least Significant Bit)** of RGB color components in an image.

Java Implementation:

```
import javax.imageio.ImageIO;
```

ISSN: 2582 - 6379
IJISEA Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed, Open Access Journal
2025, Volume 6 Issue 3
www.ijisea.org

```
import java.awt.image.BufferedImage;
import java.io.File;

BufferedImage image = ImageIO.read(new File("input.png"));
int bitIndex = 0;

for (int y = 0; y < image.getHeight(); y++) {
   for (int x = 0; x < image.getWidth(); x++) {
      int rgb = image.getRGB(x, y);

      int red = (rgb >> 16) & 0xFF;
      // Modify LSB of red component
      red = (red & 0xFE) | (bitstream.charAt(bitIndex++) - '0');

      int newRGB = (red << 16) | (rgb & 0x00FFFF);
      image.setRGB(x, y, newRGB);

      if (bitIndex >= bitstream.length()) break;
   }
}

ImageIO.write(image, "png", new File("stego.png"));
```

5. RESULTS

Embed message:

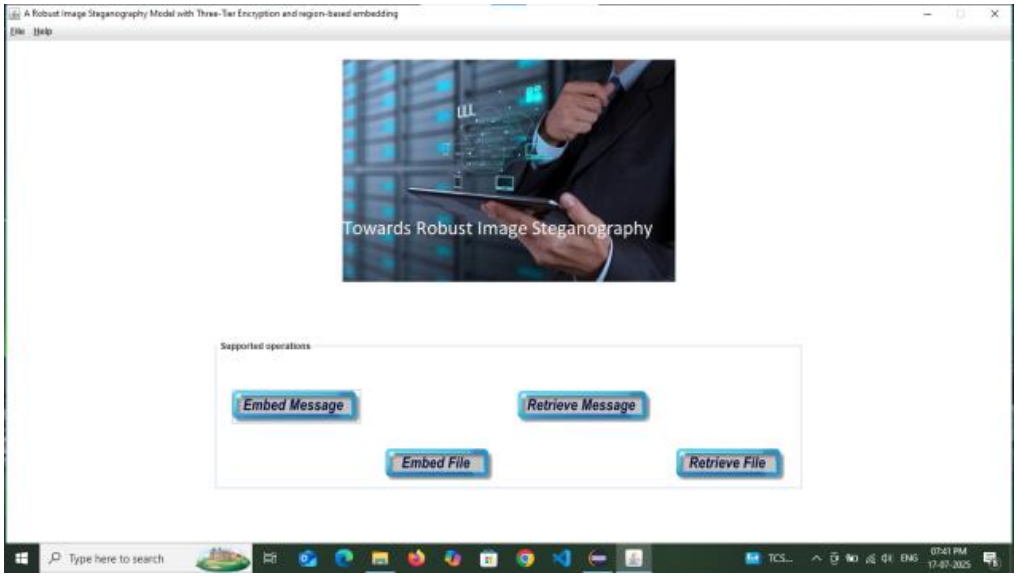

Figure 1 : Shows the Screenshot of the Proposed method visual

Allow the user to type a secret message and embeb itInto an image file after encrypting it using three different encryption methods.

ISSN: 2582 - 6379
IJISEA Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed, Open Access Journal
2025, Volume 6 Issue 3
www.ijisea.org

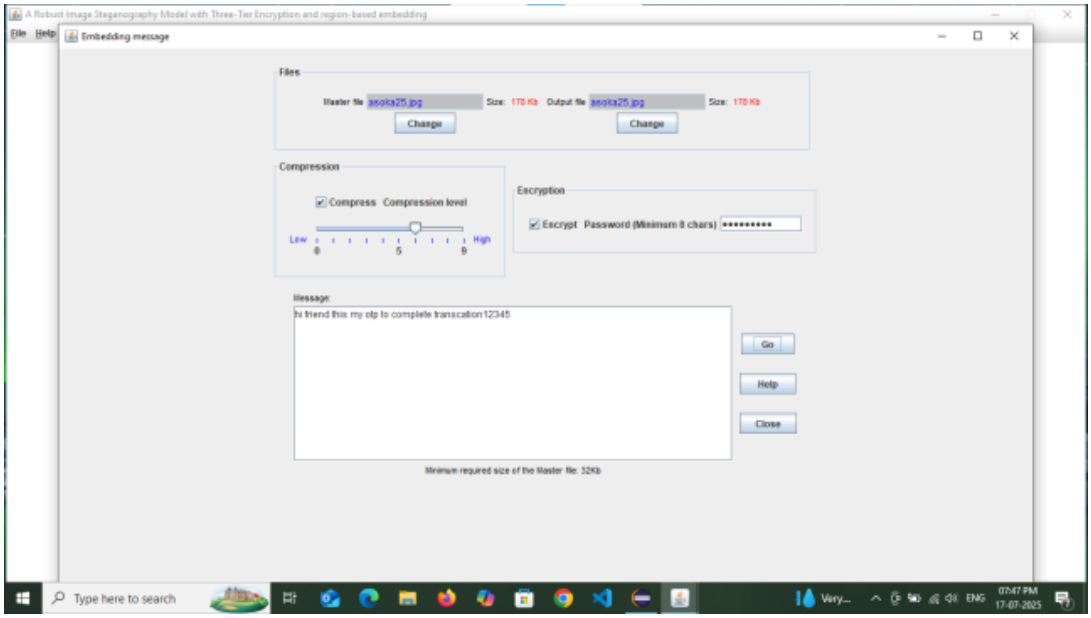

Figure 2: Shows the compression and password-based encryption

This window allows the user to securely hide a secret message inside an image using compression and password-based encryption. The message will be embedded into the selected image file after clicking the "Go" button.

Message embedding successful:

A text message ("hi friend") is encrypted with a password and embedded into the image file asoka25.jpg successfully.

Retrieve message:

Figure 3: Shows the hidden encrypted message

ISSN: 2582 - 6379
IJISEA Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed, Open Access Journal
2025, Volume 6 Issue 3
www.ijisea.org

7. CONCLUSION

the image spatial domain to embed variable-sized patient secret data into MRI host images. The algorithm first segments the image into three intensity-based regions. Three least significant bits are operated in low, medium, and high-intensity regions. In the low-intensity area, the sub- stitution of secret data bits is done on 3rd LSB with the enhancement of 2nd and 1st LSB. In the medium intensity region two LSBs are operated, the substitution of secret data bits is done on 2nd LSB, with the adjustment of 1st LSB. In the high-intensity region, only 1st LSB is operated and substituted with secret data bits. The algorithm is tested over a set of MRI images for both positive and negative cases. The results of the proposed IRD methods are significant in terms of imperceptibility and payload capacity. The proposed IRD method is also evaluated over a standard set of images (lena. baboon, peppers, cameraman, barbara) of 512 × 512 dimen- sion. The quality and structural similarity parameters MSE, PSNR, and SSIM verify the image degradation.

FUTURE WORK

Support for Audio/Video Steganography

While the current system focuses on hiding encrypted messages in images, future development could extend this technique to audio and video files. This would allow larger payloads to be hidden and increase security by embedding messages across multiple media frames, making detection far more difficult for attackers using steganalysis tools.

Adaptive LSB & Edge-Based Embedding

To improve stealth, future versions can implement adaptive steganography, where the encrypted bits are embedded in noisy or edge-rich regions of the image using edge-detection algorithms like Sobel or Canny. This makes the modifications less noticeable and more resistant to statistical analysis, enhancing security and imperceptibility.

Integration with Blockchain for Traceability

For highly sensitive communications, the system could be integrated with blockchain technology to maintain immutable logs of hidden message creation and access. Each transaction (like encoding, decoding, or transmission) can be recorded on-chain for audit and traceability without revealing the content itself.

Cloud-Based or Web Deployment

In future work, the system can be packaged as a web-based or cloud service allowing users to upload an image, encrypt a message, and download the stego file securely from anywhere. This would make the tool more accessible for journalists, whistleblowers, or organizations needing confidential file transfers.

AI-Powered Steganalysis Resistance

To future-proof the solution, it could incorporate machine learning techniques to simulate attacks by AI-based steganalysis models, and adapt the embedding strategy accordingly. This “adversarial training” would help the system evolve and stay secure even as detection tools improve.

ISSN: 2582 - 6379
IJISEA Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed, Open Access Journal
2025, Volume 6 Issue 3
www.ijisea.org

REFERENCE:

[1] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran.(2019).Comprehensive survey of image steganography: Techniques, evaluations, and trends in future research,'' Neurocomputing, vol. 335, pp. 299–326.

[2]D.Artz.(2001).Digital steganography: Hiding data within data, IEEE Internet Comput., vol. 5, no. 3, pp. 75–80.

[3]A.K.Sahu and G. Swain.(2019).High fidelity based reversible data hiding using modified LSB matching and pixel difference, J. King Saud Univ.-Comput. Inf.Sci.,doi: 10.1016/j.jksuci.2019.07.004.

[4] H. Noda, M. Niimi, and E. Kawaguchi.(2006).High-performance JPEG steganography using quantization index modulation in DCT domain, Pattern Recognit. Lett., vol. 27, no. 5, pp. 455–461.

[5]R.Chandramouli.(2003).A mathematical framework for active steganalysis, Multimedia Syst., vol. 9, no. 3, pp. 303–311.

[6] A. Sahu and G. Swain.(2019).Dual stego-imaging based reversible data hiding using improved LSB matching, Int. J. Intell. Eng. Syst., vol. 12, no. 5, pp. 63–73.

[7]H.Sajedi&M. Jamzad.(2010).BSS:Boosted steganography scheme with cover image preprocessing, Expert Syst. Appl., vol. 37, no. 12, pp. 7703–7710.

[8] W.-J. Chen, C.-C. Chang, and T. H. N. Le.(2010).High payload steganography mechanism using hybrid edge detector, Expert Syst. Appl., vol. 37, no. 4, pp. 3292–3301.

[9] A. Ioannidou, S. T. Halkidis, and G. Stephanides.(2012).A novel technique for image steganography based on a high payload method and edge detection, Expert Syst. Appl., vol. 39, no. 14, pp. 11517–11524.

ISSN: 2582 - 6379
IJISEA Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed, Open Access Journal
2025, Volume 6 Issue 3
www.ijisea.org

ABOUT AUTHORS

1.Bandela Kalyani is Currently pursuing MCA in SVKP & Dr K S Raju Arts &Science College Affiliated to Adikavi Nannaya University,Rajamahendravaram.Her research interests include Data science, Data Security,Cryptography ,Image Steganography, Cybersecurity.

2.Padala Srinivasa Reddy is working as Associate Professor in SVKP &Dr K S Raju Arts & Science College(A),Penugonda, West Godavari District,A.P.Hereceived Master's Degree in Computer Application from Andhra University.His research interests include Cryptography , Data mining and Data science, Cybersecurity, Datasecurity.