International Journal of Scientific Research in Engineering & Technology
Volume5, Issue3 (May-June 2025), PP: 86-92.
www.ijsreat.com ISSN No: 2583-1240

Enhanced Text-In-Image Steganography Using LSB Substitution with Transposition Cipher

Satish[1], Sumiran Dahiya[2]
[1] *P.G. Student, Department of ECE, Sat Kabir Institute of Technology and Management, Bahadurgarh, Haryana, India.*
[2] *Assistant Professor, Department of ECE, Sat Kabir Institute of Technology and Management. Bahadurgarh, Haryana, India.*

To Cite this Article: *Satish[1], Sumiran Dahiya[2], "Enhanced Text-In-Image Steganography Using LSB Substitution with Transposition Cipher", International Journal of Scientific Research in Engineering & Technology, Volume 05, Issue 03, May-June 2025, PP: 86-92.*

Abstract: *In order to assure secret communication, steganography is the art of hiding information within multimedia materials. This study offers a productive method for embedding text into photos by combining pre-processing, encryption, and embedding strategies. The suggested approach starts with the careful choice of a suitable cover image and text input. The cover image is transformed from RGB to grayscale to maximize embedding efficiency and reduce distortion, and then noise is removed to improve image quality. An extra degree of security is added by encrypting the secret text using the Transpose Cipher. The embedding and retrieval procedures are managed by a Stego Key, which guarantees that the secret message may only be recovered by authorized persons. The encrypted text is embedded into the cover image using the Least Significant Bit (LSB) approach, which benefits from its basic nature and low visual perceptibility. The stego key makes it easier for the recipient to precisely retrieve the embedded data that is subsequently decoded to recreate the initial text. According to outcomes from experiments, the suggested approach offers strong and secure text hiding abilities while preserving the stego image's excellent visual fidelity. For critical applications, this method provides a workable solution for protected text-based communication.*

Keywords: *Steganography, Text Hiding, Transpose Cipher, Cover Image.*

1. INTRODUCTION

Nowadays, since individuals commonly send digital photographs via email or share them via other online communication apps, steganography systems use multimedia components like voice, video, images, etc. as cover media. It is not the same as keeping a message's actual words intact. To put it another way, it is similar to concealing any message within other information. Steganography often refers to a technique that conceals the secret message within the cover object without altering its contours. According to the cover media employed to incorporate hidden data, steganography can be divided into image, text, audio, and video steganography. Anything from altering an existing text's formatting to modifying words within a text to creating random letter sequences or employing context-free grammars to produce understandable messages can be considered text steganography [1]. Because text steganography lacks unnecessary data found in image, audio, or video files, it is thought to be the most difficult. Whereas the layout of other document kinds, like pictures, differs from what we see, the structure of text documents is the same as what we see. Thus, by altering the document's structure without significantly altering the relevant output, we can conceal information in these kinds of files [2].

These days, communication is essential for precisely and swiftly sending information from one party to another. In the meantime, the internet in this day and age makes it quite easy to move large volumes of data across borders.

Every person needs to communicate data securely and confidentially [3]. We share and transfer information in our daily lives over a variety of safe channels, including the internet and the phone. But regrettably, these routes are still unsafe at a certain degree [4]. As a result, there are two popular methods that are frequently employed to conceal information before safely transmitting it. These methods include steganography (figure 1) and cryptography [5].

The text or message is altered in an encrypted format using the cryptography process, and just the sender and the recipient know the encryption key. Still, using such a mechanism to transmit an encrypted message could easily raise suspicions among the attacker, which means the message will be intercepted, attacked, and decrypted. Consequently, to address the shortcomings of the cryptographic methods, steganography strategies have been devised and developed. The science of communicating in a way that conceals and conceals the communication's existence is called steganography [6]. Since the steganography approach conceals the presence of a message, no one can identify its existence. To put it another way, the steganography approach embeds the message with one of the multimedia contents—such as music, video, or image files—while concealing the message within the material [7].

Images are thought to be the most often utilized cover objects for steganography techniques [8]. The widespread use of digital photos on the Internet and the abundance of extraneous bits in them are the reasons behind this. Picture steganography is regarded as a technique for ambiguous and secret correspondence that aims to transmit a lot of unknown data. Generally speaking, between relaying parties, to the extent shown in the cover photo. Additionally, it seeks to allay suspicions about non-conveying assemblages in communications of this kind.

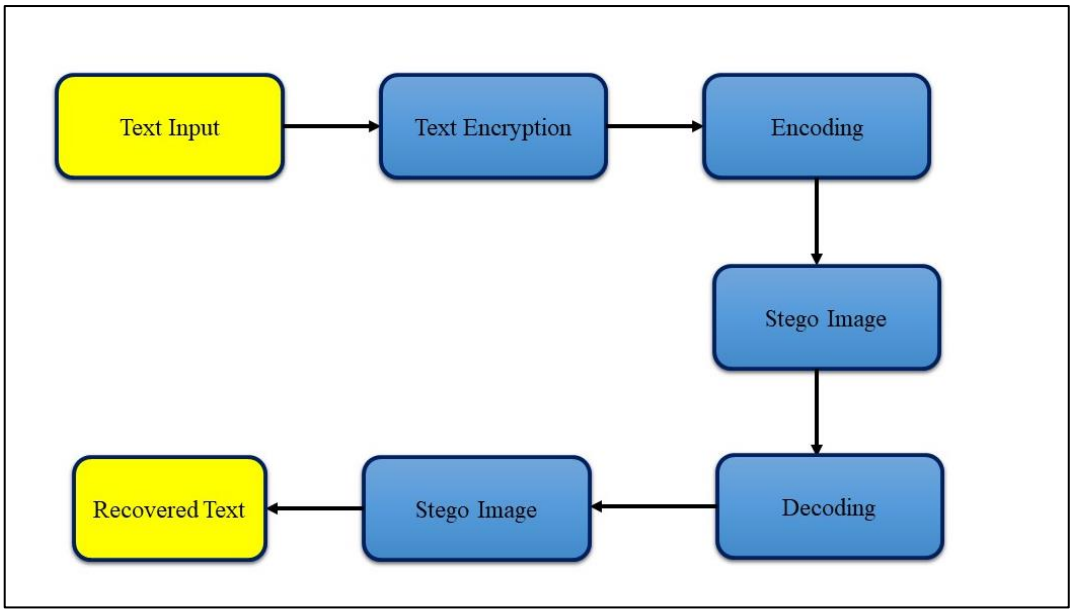

Figure 1: Steganography

II.RELATED WORK

Developers and investigators have recently placed a great deal of focus on steganography methods for concealing text in images because of how crucial they are for concealing data. Additionally, newer steganography techniques for data concealment, including XOR and XNOR logic gates, have improved security by limiting access to the confidential data to the intended audience.

In [9], a steganography method is suggested to safeguard data being transferred from hackers. This technique uses the encryption key and the XNOR gate to work on the encryption of confidential data. The Least Significant Bit (LSB) technique is used to conceal the data that has to be encrypted within a color image. In order to protect the information from prying eyes, the authors in [10] have proposed a technique for concealing text within color graphics. There are two primary phases to this approach. Using the XOR operation gate to conceal the text bit in the image bit and specifying a place of the image bits based on a random key (whose length is equal to that of the secret text), the steganography technique is used in the first stage to conceal the information in the transmission.

In [11], the steganography technique is used to conceal text messages behind 24-bit color graphics. Two schemes—the extraction strategy and the embedding data scheme—have been presented for this method. The LSB method will be used to conceal the text messages in the cover image when embedding data. The secret text was recovered from a stegoimage using the extraction scheme's Most Significant Bits (MSB) XOR technique. The object shape in the picture is identified by the MSB bits. Both of these techniques require a randomly generated key. In [12], a secure model with text messages incorporated for dependable communication was put forth. Additionally, this model incorporates embedded text message bits using the LSB technique. The logistic map and secret key serve as the foundation for the LSB in this approach, a spatial domain technique that adds additional data to color images without sacrificing image quality. The message fragments are randomly embedded in the image using the logistic map method. The Lena image type was utilized in this piece.

In [13], a safe technique for encoding secret text communications into color pictures is suggested. This approach makes use of the LSB algorithm-based Integer Wavelet Transform (IWT) methodology. The LSB algorithm conceals the secret text messages, and the stego-image is created using the inverse IWT. The estimated coefficient in the blue and green color sections conceals the secret material. The LSB technique incorporates the sender's signature and the actual length of the secret data into the red portion of the cover image. For picture stenography, a new and innovative way for concealing the secret image in the cover image has been made possible by a high-quality image hiding strategy based on the Noise Visibility Function and a perfect chaotic based encryption algorithm [14]. This method seeks to increase both the secret image's security and the Stego image's visual quality. High embedded capacity is still provided by this method. This method can modify the payload of every pixel in the image. The issue with this strategy is that, in comparison to earlier approaches, it requires a significantly larger overhead computational time. The method is more sophisticated as a result of this longer computing time.

"An Affordable Image Encryption and Hiding Technique Performed by Double Random Phase Encoding" [6] has offered new optical techniques with numerous benefits, including high parallel, high scale, and processing speed. Using a novel methodology, this image encryption and concealment method is being used. The double arbitrary phase encoding process is the name given to this method. There are numerous benefits to this strategy: First, an analysis of the effectiveness of the current optical image concealment technology will be conducted. The specific statistical detection techniques for the optical image hiding system must be put into practice following system analysis. Following the implementation of the concealing system, an analysis of the visual image hiding system's retrieving assaults will be conducted. The primary disadvantage of this method is that, despite its high parallel, high dimension, and processing speed, etc. However, this method is still not commonly employed since it does not produce excellent experiment outcomes. Furthermore, this strategy is less successful than previous ones.

III.PROPOSED METHODOLOGY

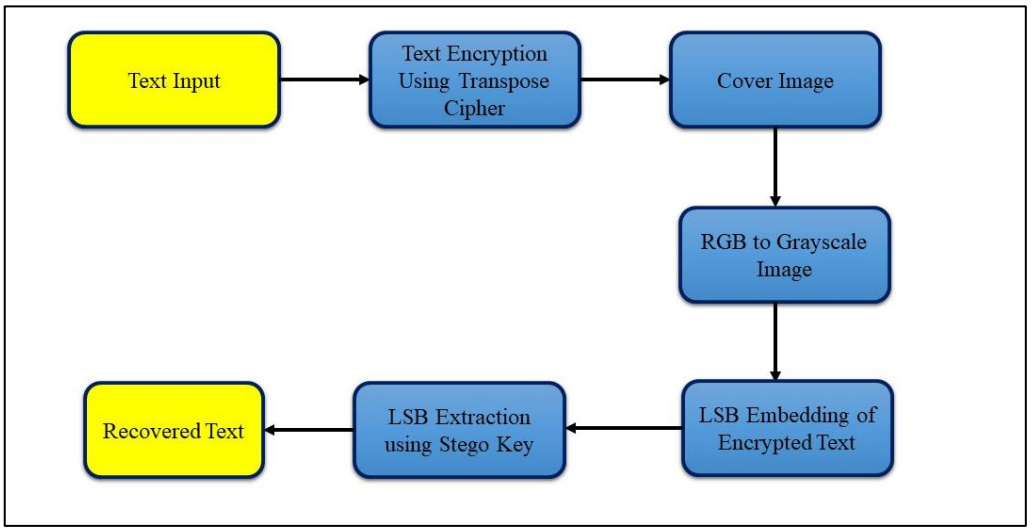

Figure 2: Proposed Methodology

Pre-processing:

The proposed method chooses a random cover image from a set of 20 images. This image is converted to grayscale image. Set dimensions of the image according to algorithm and prepare the secret message by following steps:

- It adds a special delimiter or known character at the end of the message to mark message end. Apply Transposition Cipher to the message (reorder the characters based on a key).
- Convert each character to its ASCII value. Convert ASCII values to binary format (typically 8 bits per character).

Embedding Process:

- Initialize the output image as a copy of the input grayscale image.
- Traverse the pixels of the image one by one: For each pixel, convert its intensity value to 8-bit binary.
- For each message bit: Compare message bit with LSB of pixel, take XOR of message bit and pixel LSB,
- Update pixel if needed: If XOR result is 0 → no change, If XOR result is 1 → flip the LSB of pixel.
- Replace the pixel value in the output image accordingly and repeat until all bits of the message are embedded.

Post-processing: Save the input (grayscale) image and the output (stego) image to local disk.

Pseudo code:

Figure 3a and 3b shows the pseudo code of proposed method. The transposition cipher rearranges the characters of the message rendering to a predefined key (simple columnar transposition or permutation of indices). The use of '#' or any unique delimiter ensures the extractor knows where the embedded message ends. XOR ensures that embedding is not merely substituting LSB sightlessly — it increases a minimal level of encryption.

Extraction Pseudo Code: Figure 4 shows the pseudo code for the extraction.

At sender side: apply transposition cipher on message, extract binary values, Using LSB and XOR gate embed it and create a stego Image (cover image). At receiver side: Extract LSB and reconstruct binary image, convert to characters, halt at delimiter, apply inverse transposition cipher and extract original message.

Table 1: Comparison Table of different steganography techniques

Method	Security	Payload Capacity	Robustness vs. Attacks	Image Quality (PSNR)	Complexity
LSB (Basic)	Low	High	Low	High	Low
LSB with XOR + Transposition Cipher	Medium	High	Medium	High	Medium
LSB Matching (LSBM)	Medium	High	Medium	High	Medium
Spread Spectrum (SS)	High	Low	High	Medium	High
Discrete Cosine Transform (DCT)	High	Medium	High	High	High
Discrete Wavelet Transform (DWT)	High	Medium	High	High	High

```
BEGIN
  // Step 1: Load and preprocess the image
  INPUT: cover_image, secret_message, transposition_key
  image = LoadImage(cover_image)
  grayscale_image = ConvertToGrayscale(image)
  SetImageDimensions(grayscale_image, width, height)
    // Step 2: Prepare the secret message
  secret_message = secret_message + '#'
  ciphered_message = ApplyTranspositionCipher(secret_message, transposition_key)
     // Convert message to binary
  binary_message = ""
  FOR each character c in ciphered_message DO
     ascii_value = ASCII(c)
     binary_char = To8BitBinary(ascii_value)
     binary_message = binary_message + binary_char
  END FOR
     message_length = Length(binary_message)
  bit_index = 0

  // Step 3: Initialize output image
  output_image = Copy(grayscale_image)

  // Step 4: Embed the message bits using LSB substitution with XOR
  FOR each pixel in output_image (row-major order) DO
     IF bit_index < message_length THEN
        pixel_value = GetPixelValue(pixel)
        pixel_binary = To8BitBinary(pixel_value)
         // Get LSB of pixel
        pixel_lsb = pixel_binary[7]
```

Figure 3a: Pseudocode part 1

```
            // Get next message bit
            message_bit = binary_message[bit_index]

            // XOR operation
            xor_result = XOR(pixel_lsb, message_bit)

            // Update pixel LSB if needed
            IF xor_result == '1' THEN
               IF pixel_lsb == '0' THEN
                  pixel_binary[7] = '1'
               ELSE
                  pixel_binary[7] = '0'
               END IF
            END IF

            // Update pixel value in output image
            new_pixel_value = BinaryToDecimal(pixel_binary)
            SetPixelValue(output_image, pixel, new_pixel_value)

            // Move to next message bit
            bit_index = bit_index + 1
         ELSE
            BREAK // All message bits are embedded
         END IF
      END FOR

      // Step 5: Save the images
      SaveImage(grayscale_image, "grayscale_image.png")
      SaveImage(output_image, "stego_image.png")

   END
```

Figure 3b: Pseudocode part 1

```
BEGIN
  INPUT: stego_image
  stego_image = LoadImage(stego_image)
    binary_message = ""
    // Traverse each pixel of the stego image in same order
  FOR each pixel in stego_image (row-major order) DO
    pixel_value = GetPixelValue(pixel)
    pixel_binary = To8BitBinary(pixel_value)
      // Extract the LSB of pixel
    pixel_lsb = pixel_binary[7]
     // Append LSB to binary message
    binary_message = binary_message + pixel_lsb
      // Optional: stop if message delimiter is found after reconstruction
  END FOR
    // Now, convert binary_message back to characters
  message = ""
  FOR i from 0 to Length(binary_message)-1 STEP 8 DO
    binary_char = binary_message[i : i+8]
    ascii_value = BinaryToDecimal(binary_char)
    character = ASCII_to_Char(ascii_value)
          IF character == '#' THEN
       BREAK // End of message reached
    ELSE
       message = message + character
    END IF
  END FOR
    // Step: Decrypt using inverse of transposition cipher
  decrypted_message = transposition_cipher_decrypt(message, key)

  OUTPUT decrypted_message
END
```

Figure 4: Extraction Pseudo Code

IV.SIMULATION OUTCOMES

Test 1: Do Text Hiding: First of all choose a sample image and then enter secret message. We have entered the secret message 'I love India'. The original image is shown in image 5. The image with secret message is shown in figure 6.

Figure 5: Original Image

Figure 6: Image with secret message

Enter Image Name ('stegoImage.png'): 'stegoImage.png'. Message revealed: {'I love India'}
Message extracted successfully.

Analysis:

The LSB + Transposition Cipher enhances basic LSB by introducing cryptographic security through transposition. Spread Spectrum and DCT/DWT are more robust but more complex and lower in capacity. Basic LSB is simple but vulnerable. Our method offers a good balance between simplicity, security, and image quality. A comparison of different steganographic techniques is shown in Figure 7, emphasizing the trade-offs between computing cost, security, payload capacity, and robustness. While keeping a high payload capacity andminimal complexity, the suggested LSB with XOR and Transposition Cipher technique exhibits balanced performance, providing enhanced security and robustness over simple LSB.

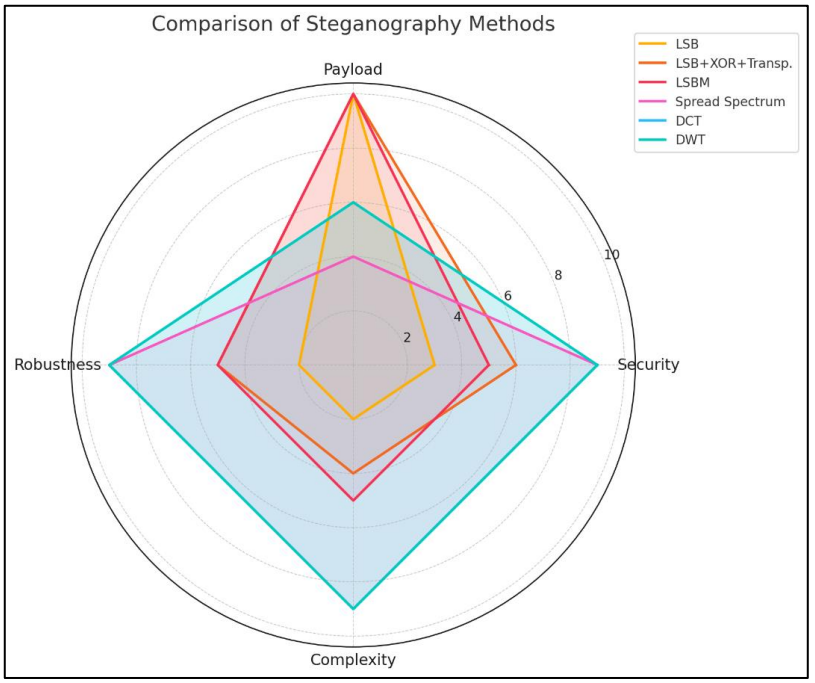

Figure 7: comparison of the security, payload capacity, robustness, and complexity of various steganography techniques

V.CONCLUSION

In order to increase security, we combined the Least Significant Bit (LSB) technique with the Transposition Cipher in this work to propose a straightforward yet efficient way for text-in-image steganography. The suggested method uses an XOR-based replacement mechanism to embed the secret message in the LSBs of a grayscale image, ensuring that the cover image introduces the least amount of perceptual distortion possible. The secret message is encrypted using a transposition cipher before it is embedded, which adds another degree of obfuscation that makes it more difficult for unauthorized parties to recover the message.

In our approach, the cover image is converted to grayscale, the secret message is prepared by adding a delimiter and transforming it to binary format, and the message bits are embedded by iterating through each pixel. At the receiver's end, the original message may be easily and precisely extracted thanks to the XOR process between the message bit and the pixel's LSB, which guarantees effective embedding. By guaranteeing that the plaintext message cannot be decrypted without the proper decryption key, even if the bits are taken, the transposition cipher further increases the system's resilience against steganalysis attacks. All things considered, this method strikes a compromise between security, computational effectiveness, and simplicity, which makes it ideal for lightweight steganographic systems where deployment ease and image quality are crucial. To further improve the security of hidden communications, future studies can investigate expanding this framework to color images, using adaptive embedding schemes, or integrating it with more sophisticated cryptographic algorithms.

REFERENCES

[1] *K. Benett, "Linguistic steganography- survey, analysis and robustness concerns for hiding information in text," Purdue University, CERIAS Tech. Report 2004-13, 2004.*

[2] *M. S. Shahreza, and M. H. S. Shahreza, "Text steganography in SMS," 2007 Int. Conf. on Convergence Information Technology, 2007, pp. 2260-2265.*

[3] *M. Elhoseny et al., "Security and privacy issues in medical internet of things: overview, countermeasures, challenges and future directions," Sustainability, vol. 13, no. 21, p. 11645, 2021.*

[4] *T. Naqash, A. Iqbal, and S. H. Shah, "Review on Safe Reversible Image Data Hiding," in 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), 2019: IEEE, pp. 0929-0932.*

[5] *M. K. I. Rahmani, K. Arora, and N. Pal, "A crypto-steganography: A survey," International Journal of Advanced computer science and applications, vol. 5, no. 7, 2014.*

[6] *F. Sharmin and M. I. Khan, "Image steganography using combined nearest and farthest neighbors methods," International Journal of Advanced Computer Science and Applications, vol. 10, no. 11, 2019.*

[7] *N. Singh, "Survey paper on steganography," International Refereed Journal of Engineering and Science (IRJES), vol. 6, no. 1, pp. 68-71, 2017.*

[8] *R. A. Watheq, F. Almasalha, and M. H. Qutqut, "A new steganography technique using JPEG images," International Journal of Advanced Computer Science and Applications, vol. 9, no. 11, 2018.*

[9] *R. M. Neamah, J. A. Abed, and E. A. Abbood, "Hide text depending on the three channels of pixels in color images using the modified LSB algorithm," International Journal of Electrical and Computer Engineering, vol. 10, no. 1, p. 809, 2020.*

[10] *H. R. Kareem, H. H. Madhi, and K. A.-A. Mutlaq, "Hiding encrypted text in image steganography," Periodicals of Engineering and Natural Sciences, vol. 8, no. 2, pp. 703-707, 2020.*

[11] *D. Ratnasari and A. S. Aji, "Text to Color Image Steganography Using LSB Technique and XOR Operations," International Journal of Applied Business and Information Systems, vol. 3, no. 2, pp. 59-65, 2019.*

[12] *M. Ulker and B. Arslan, "A novel secure model: Image steganography with logistic map and secret key," in 2018 6th International Symposium on Digital Forensic and Security (ISDFS), 2018: IEEE, pp. 1-5.*

[13] *E. Emad, A. Safey, A. Refaat, Z. Osama, E. Sayed, and E. Mohamed, "A secure image steganography algorithm based on least significant bit and integer wavelet transform," Journal of Systems Engineering and Electronics, vol. 29, no. 3, pp. 639-649, 2018.*

[14] *Shaveta Mahajan, Arpinder Singh, "A Review of Methods and Approach for Secure Stegnography", International Journal of Advanced Research in Computer Science and Software Engineering, Vo1.2, No.1 0, pp. 67-70,2012.*