Steganography using MLEA and LSB technique

P. Uma Sankar
Asst. Professor, Sri Vasavi Engineering College, Tadepalligudem

Atyam K N V Pratyusha[1]

Kovela Indraja[1]

Polisetty Pavan Kumar[1]

Vaddi Madhumiitha[1]

Kusumanchi A Vaishnavi Tripura[1]

Addepalli Naveen Kumar[1]

[1]Department of Computer Science and Engineering, Sri Vasavi Engineering College, Tadepalligudem

Abstract:

Communication has become a lot easier in this era of technology. Therefore, data transmission has become vulnerable and unsafe from different external attacks. So, to secure the data while communicating over the internet we use Steganography. Steganography refers to information or data that has been concealed inside a files like Audio, Video & Image. In the proposed methodology we will provide security for the confidential information. By this approach no one is allowed to view the confidential data, they can view only Audio, Video & Image file when it is being passed over the internet. Then at the recipient side the original information i.e., plain text will be extracted from the Audio, Video & Image by performing decryption operations. This involves three major phases i.e., encrypting the message, embedding the message into file, and decrypting the file to retrieve the message. To increase the security and robustness we use MLEA (The Multilevel Encryption Algorithm).

1. INTRODUCTION:

Security often requires that data be kept safe from unauthorized access. The main defence is physical security i.e., machine will be protected beyond physical walls. However, physical security is not always an option (due to cost and/or efficiency considerations). Steganography secures information by protecting its confidentiality [1]. Data integrity and authentication will also be maintained by using this. So far Steganography is used in many forms but using it with Audio, Video & Image files is another Stronger Technique. The given message will be encrypted with a given Audio, Video & Image file using a secret key. The System will then embed the secret message into the Audio, Video & Image file. The result will be a new Audio, Video & Image file, which has the secret message in it. The key which you are using decryption should be same as the one you have used for encrypting audio, video and image to get the secret message from it.

The advent of MLEA brings a new dimension to steganographic techniques by leveraging the power of machine learning to optimize the embedding process. MLEA analyses patterns and features within the cover media, enhancing the efficiency and robustness of the steganographic algorithm. This integration not only improves the concealment capacity but also adapts dynamically to diverse types of content, making it a potent tool for secure information exchange.

LSB, on the other hand, is a classical steganographic method that focuses on altering the least significant bits of digital data without perceptible changes to the human eye. When combined with MLEA, it forms a symbiotic relationship where MLEA optimizes the selection of bits to modify, ensuring minimal visual impact while maximizing the payload capacity.

This amalgamation of MLEA and LSB offers a sophisticated and adaptable solution for concealing sensitive information within digital media. The synergy between machine learning and traditional steganography not only strengthens the security of communication but also aligns with the evolving landscape of cybersecurity challenges. In this exploration of "Steganography using MLEA and LSB," we delve into the intricacies of this innovative approach, uncovering its potential applications, challenges, and the broader implications for secure data transmission in the digital age.

2. REVIEW RELATED WORK:

2.1. Literature Review

In An effective and Secure Digital Image Steganography scheme using two random function and chaotic map [2], they used New Stego Key Adaptive LSB (NSKA-LSB) scheme, which depends on four stages for the provision of better data-hiding algorithm in cover images by the volume, image quality, and security. The method is established on a novel transformation of least significant bit exchange technique, a fusion of two arbitrary functions, and a chaotic map.

LSB substitution is a widely used method in steganography, which involves hiding secret information within a cover image. This technique is based on the idea of replacing the least significant bit (LSB) of each pixel in the cover image with the bits of the secret data. With regards to the gray-scale images whose pixels possess just a single value ranging from 0 to 255 and the bit depth of 8 bits, the bits of the in the context of steganography, the method being described involves a unique approach. Instead of converting the secret information into binary format, it is directly employed to modify the cover object's image. The cover object, in this case, is a color image with three color channels: Red, Green, and Blue (RGB), and each channel has a bit depth of 24 bits. information is embedded in each of the channels. Finally, the three paths are combined to produce the stego image. The modification of the LSB bits does not allow the HVS to detect the stego-image. When utilizing a unique form of the LSB substitution method in a proposed scheme, it is beneficial to present a mathematical expression to offer a more detailed comprehension of the approach. The primary goal of this mathematical representation is to provide a deeper insight into the core concept of the scheme. Diverse embedding percentage (EP) of LSB, which include 6.25% and 12.5%, which means 0.5 and 1.0 bpp respectively are used based on the capacity that is to be embedded.

In Image Steganography: A Review of the Recent Advances[3] Generative Adversarial Networks (GANs) leverage principles from game theory to train models for tasks like image generation. Introduced in 2014, GANs have become a powerful framework for creating realistic synthetic data Multi-Level Encryption Algorithm for making the cypher text.

The cipher is embedded into shuffled blocks of blue channels. After completion of the embedding process then, a steganographic process where data embedding involves rearranging sub-images and color channels, and the extraction algorithm is the reverse of the embedding algorithm.

In Image steganography performance analysis using Discrete Wavelet Transform and Alpha blending for secure communication, the proposed work introduces a versatile scaling parameter called alpha to enhance the adaptability of the steganography technique. Unlike traditional methods, this approach extends beyond standard cover and payload images, accommodating various types and dimensions, including live webcam images and predefined images of different formats. Prior to processing, these images undergo normalization and preprocessing.

The proposed work introduces a versatile scaling parameter called alpha to enhance the adaptability of the steganography technique. Unlike traditional methods, this approach extends beyond standard cover and payload images, accommodating various types and dimensions, including live webcam images and predefined images of different formats. Prior to processing, these images undergo normalization and preprocessing.

A crucial step in the process involves applying the Haar Discrete Wavelet Transformation (DWT) to both cover and payload images. The payload image is then encrypted and fused with the cover image to generate a stego image, effectively concealing the confidential information within the seemingly unaltered cover. To assess the efficacy of this approach, the study measures parameters such as Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), and Entropy, providing quantitative metrics for evaluating the success of the steganographic process. This innovative steganographic method, integrating established techniques like Haar DWT, encryption, and alpha scaling, not only strengthens the security of information exchange but also introduces adaptability crucial for addressing the challenges posed by the dynamic digital landscape. As we explore the nuances of this work, we uncover its potential applications, implications, and advancements in the realm of secure information exchange within the ever-evolving web environment.

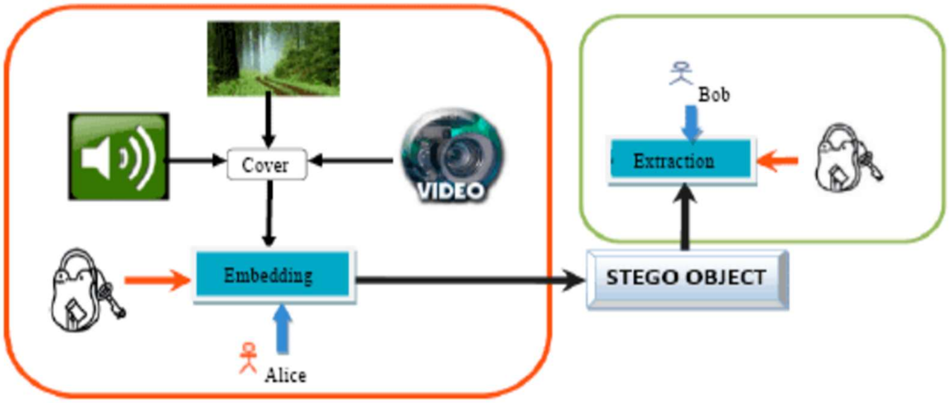
In Enhanced Least Significant Bit algorithm For Image Steganography[4], Enhanced Least Significant Bit (LSB) algorithm for image steganography represents a refined and advanced approach to concealing information within digital images. Steganography, the art of covert communication, is particularly effective when applied to LSB, as it focuses on manipulating the least significant bits of pixel values in an image without noticeably altering its appearance to the human eye. The enhanced LSB algorithm builds upon the traditional method by incorporating additional features or modifications to enhance security, capacity, and robustness.

The enhanced LSB algorithm, with its combination of encryption, dynamic bit selection, randomization, error correction, adaptive capacity, multilayered embedding, and thresholding, represents a sophisticated and robust solution for image steganography. As the digital landscape evolves, these enhancements address the challenges posed by advanced detection methods and contribute to the ongoing development of secure communication through steganographic techniques.

3.PROBLEM STATEMENT

In so many steganography projects LSB technique is used which is less secure. Here we use a combination of both MLEA and LSB technique to enhance data hiding efficiency and a different approach for robustness

4. SYSTEM ARCHITECTURE



5.PROPOSED METHODOLOGY

Multi-level encryption algorithms involve using multiple layers of encryption to enhance the security of data. Each layer typically employs a different encryption method, making it more challenging for unauthorized parties to decrypt the information. For example, you might start with encrypting the data using a symmetric encryption algorithm like AES (Advanced Encryption Standard) at the first level. Then, at the second level, you could apply asymmetric encryption using algorithms like RSA. This creates a layered approach, where even if one encryption method is compromised, the other layers provide an additional barrier. The key advantage is that breaking through multiple layers of encryption requires a deep understanding of different algorithms, making it more complex and time-consuming for attackers to decipher the original data. However, it is important to strike a balance between increased security and the potential complexity and computational overhead introduced by multiple encryption layers

LSB (Least Significant Bit): In image steganography, the Least Significant Bit (LSB) technique is a common method used to hide information within the pixel values of an image. The LSB is the rightmost bit in a binary representation of a number. The basic idea is to replace the least significant bits of certain pixel values with the bits of the secret message. LSB technique works as follows:

1. Pixel Values: In a digital image, each pixel is represented by a set of color values (RGB for a colored image). Each color channel (Red, Green, Blue) is represented by 8 bits, ranging from 0 to 255.

2. Least Significant Bit: Altering the least significant bit of a pixel value has a minimal impact on the color. This small change is less likely to be visually noticeable.

3. Encoding: To hide a message, the binary representation of each character in the message is embedded into the least significant bits of the corresponding pixel values. This is done sequentially, typically using one color channel.

4. Decoding: To retrieve the hidden message, one needs to extract the least significant bits from the pixels and convert them back into characters.

LSB Algorithm:

Strengths: A. The embedding algorithm at the sender side

Get the input cover image and secret message.

Accept the stego-key from the user and calculate average value of them.

Convert each character of secret message and each LSB bit of cover image (R channel) from the position of average of stego-key.

Substitute the LSB bit of cover image (R channel) with binary values of secret message with respect to the starting point until the end of secret message.

Insert the end character value at the end of secret message.

Calculate the PSNR, SNR of original and resulting images.

Send a stego-image to the receiver

B. The extracting algorithm at the receiver side

Get the input stego calculate average value

Load the stego-image that is sent from the sender.

Extract each of LSB bit from the stego image until to find out the end bit.

Reconstruct the collecting LSB bits from the stego-image.

Transform the LSB bits to correspondent characters

This method is very fast and easy to implement in comparison to other methods of image Steganography.
The output image has very slight difference to the input image.
Instead of embedding the message in only the LSB, we can embed the message in last two LSBs, thus embedding even large messages.

This method forms the basics of many other complex algorithms
Instead of embedding the message in only the LSB, we can embed the message in last two LSBs, thus embedding even large messages.

Methodology:

1)Encrypting the secret message using MLEA algorithm
To increase the security, MLEA algorithm encrypts the secret message and produces a cipher and embeds the cipher text into cover image or video or audio.

2)The Embedding process
In this process, we'll flip the cover image and convert into three channels which are Red, Green and Blue(RGB) and hides the encrypted message into the blue channel and produces a stego image.

3)The Extraction Process
In this process, we'll flip the stego image and convert into three channels of Red, blue and Green and the encrypted message is taken from the blue channel and decrypted using MLEA algorithm.
In this way we can securely send and receive the secret information using any communication channel over the internet.

MLEA Algorithm:

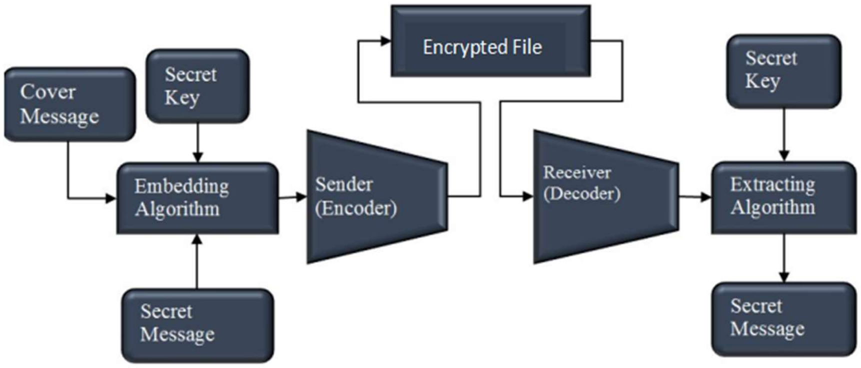
Input**:** Secret Message Si
Output**:** Concatenation of B1 and B2

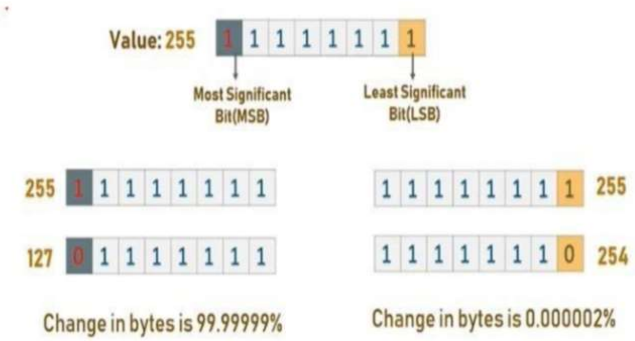
```
Begin

 Select the secret message and convert it into bits

   Perform bitXor (message bits, logical 1)

    Take the 8bits combination and replace the first 4 bits with the last 4bits

      Perform left circular shift to every 8bits combination

       Divide whole bits' array into 2 equals size blocks b1 and b2

 After that, take a bit from b1, then check the condition

         Is b1 bit equal to 1?

              If yes, then

                   Perform bitXor (b2, logical 1) and goes to b1 for next bit
```

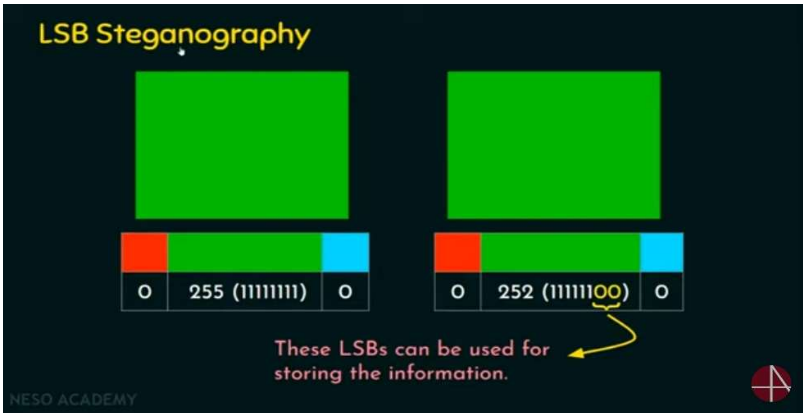
```
        If not, then
            Leave the b2 bit unchanged and go to the next bit of b1
    Is this the last bit?
            If yes, then concatenate b1 and b2
            If no, then Repeat step 7 until all bits perform
End
```

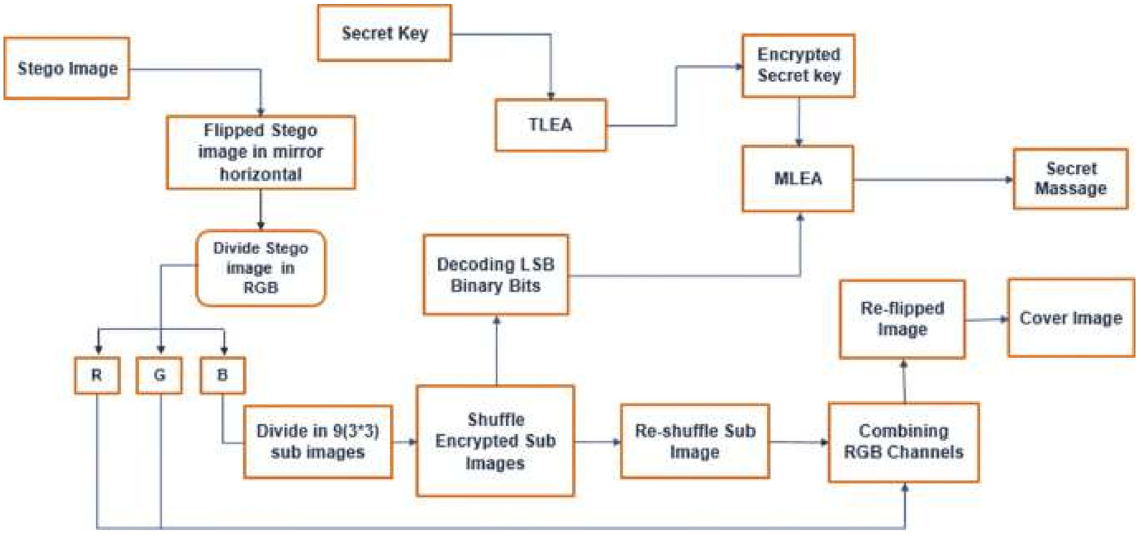
Strengths:

As a general estimate, security could be reasonably effective for several years. In our project security could be provided for several months. We will regularly update the algorithm to prevent attack from advance methods. We will add more information to the cover data so to decrease the detection of original data.




Value: 255
1 1 1 1 1 1 1 1
Most Significant Bit(MSB)
Least Significant Bit(LSB)
255
1 1 1 1 1 1 1 1
127
0 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1
255
1 1 1 1 1 1 1 0
254
Change in bytes is 99.99999%
Change in bytes is 0.000002%





6.CONCLUSION

Our aim is to reveal the hidden secret message within the Image or Audio or video file and send that file which contains data to others securely in such a Way that others cannot discern the presence of the hidden message and we have achieved our objective.

In the coming future, the most important use of steganographic techniques will be in the field of digital watermarking. Content providers are desperate to protect their copyrighted works against distribution of illegal things and digital watermarks give a way of tracking the owners of these materials.

7.REFERENCES

[1] Wikipedia. (2020). Steganography. [Online]. Available: https://en. wikipedia.org/wiki/Steganography

[2] Mohanad Najm Abdulwahed, “An effective and Secure Digital Image Steganography scheme using two random function and chaotic map”, January 2021

[3] Nandhini Subramanian, Omar Elharrouss, Somaya al-maadeed, and ahmed bouridane, “Image Steganography: A Review of the Recent Advances”, January 2021

[4] Saleem S Tevaramani, Ravi J, “Image steganography performance analysis using Discrete Wavelet Transform and Alpha blending for secure communication”, June 2022

[5] Shilpa Gupta, Geeta Gujral and Neha Aggarwal, “Enhanced Least Significant Bit Algorithm for Image Steganography”, June 2018

[6] S. Gupta, G. Gujral, and N. Aggarwal, “Enhanced least significant bit algorithm for image steganography”, 2012.

[7] R. Das and T. Tuithung, “A novel steganography method for image based on Huffman encoding”, March 2012.

[8] Taha, Mustafa Sabah, Et Al. “Combination of Steganography And Cryptography: A Short Survey”, 2019.

[9] Mahdi Hashim, M. O. H. A. M. M. E. D., Mohd Rahim, And Mohd Shafry. “Image Steganography Based On Odd/Even Pixels Distribution Scheme and Two Parameters Random Function”, Journal Of Theoretical & Applied Information Technology 95.22 (2017).

[10] Muhammad, Khan, Et Al. “Cisska-Lsb: Color Image Steganography Using Stego Key Directed Adaptive Lsb Substitution Method”, 2017

[11] Sahu, Aditya Kumar, Gandharba Swain, And E. Suresh Babu. “Digital Image Steganography Using Bit Flipping”, 2018

[12] Yeung, Yuileong, Et Al. “Secure Binary Image Steganography Based On Ltp Distortion Minimization”, 2019

[13] Sahu, Aditya Kumar, And Gandharba Swain. “A Novel N-Rightmost Bit Replacement Image Steganography Technique,” 2019.

[14] Taha, Mustafa Sabah, Et Al. “Wireless Body Area Network Revisited”, 2018.

[15] Saad, Mohammed Ayad, S. T. Mustafa, Mohammed Hussein Ali, M. M. Hashim, Mahamod Bin Ismail, And Adnan H. Ali. ‘Spectrum Sensing And Energy Detection In Cognitive Networks”, 2019.