Study of LSB Based Video Steganography: A Secure Method to Embed Secret Data in Video Files

Saumya Rao [1], Dr .Umadevi R[2]
[1] *Research Scholar, CMR University, Bengaluru, India*
[2] *Research Supervisor, CMR University, Bengaluru, India*

Abstract – Steganography involves concealing secret information within media such as text, images, audio, or video files by altering the bits of the cover media and substituting them with data bits. Among these methods, video steganography stands out for its higher capacity to embed text data compared to text, image, or audio-based steganography. However, despite this advantage, video steganography is challenged by issues related to robustness. Secret data embedded within video files may be compromised by transformation operations or cyber attacks. Therefore, an effective video steganography technique should offer high imperceptibility, support large payloads, and demonstrate resilience against visual, statistical, and transformation-based Steganalysis attacks. One widely used approach for embedding secret data in video files is the Least Significant Bit (LSB) method. This paper examines various LSB-based techniques for embedding hidden data in video files.

Keywords: LSB, Steganography, Steganalysis, spatial domain, Early Embedding, Delayed Embedding, Knight tour, Pseudo Random number, PSNR, MSE

I INTRODUCTION

In the current scenario of tremendous growth in the use of technology in our daily life, the need of information security has grown extremely. A huge volume of sensitive data such as personal data, medical data, financial data etc., is being transferred and stored. Providing security to such huge volume of sensitive data becomes a challenging task. Information hiding techniques are used to counter the attacks on data and provide proper security, confidentiality and integrity to the data [1]. Cryptography, Watermarking and Steganography are among a very few most popular information hiding techniques which are currently in use. Cryptography is a technique of encryption used to protect the data over the network, as various networks are related and admire attacks and intrusions [2]. In Cryptography, the plain data is converted into cipher text and then transmitted over to the destination and at destination cipher text is converted back into plain data. In digital watermarking technology a message is hidden into a multimedia object such as an image or text or other digital object. The proposed technique is majorly important in digital copyrights protection [3]. Even though Cryptography and digital watermarking is the most secured and unbreakable way of hiding data, the encrypted message is always visible to the human visual system. Hence to overcome this limitation Steganography is used for data hiding where secret information is hidden inside a carrier file without being noticed by human visual system.

Steganography is not new and has been in existence ever since the BC's even before the digital era. Video Steganography is the process of hiding secret information inside video files. The secret data can be anything such as text, audio, image, video, binary files etc.

Video Steganography is considered more secure than other type of Steganography like image Steganography, or audio Steganography because whenever any data is hidden in a video file and send to the receiver, there are very low chances of any intruder understanding the presence of data in the video file. This is because the frame in video file moves in an extremely high rate making it imperceptible. Even if the intruder manages to get hold of the frame in which data bit is hidden, he cannot identify it because there may be thousands of frames moving at faster rate and data may be hidden in any one of the frame.

Video Steganography has wide applications in the fields such as Intelligence agencies, the military, the medical sector and multimedia. The current advancement of the technology in all the sectors has led to increase in data storage and transmission in cloud area. Transferring these sensitive data over the internet is the critical problem since any data loss that happened due to cyber attacks can have negative affect.

Basically videos are treated as collection of still images taken in different time that run in continuous manner, so that we see a motion picture [10]. Still images are called Frames. Hence video Steganography

is extension of image Steganography and almost all the algorithm used for image Steganography can be applied on video Steganography with required modifications.
The most popular method for Steganography is the Least Significant Bits (LSB) substitution method for image, audio and video Steganography. This paper surveys the existing literature on LSB-based video Steganography, providing an in-depth analysis of its techniques, security measures, and challenges.
The following paper is organized as follows LSB algorithm, LSB Methodologies, Comparative analysis and Conclusion.

II LSB ALGORITHM

The Least Significant Bit (LSB) algorithm is one of the earliest methods used for video Steganography. It is widely favoured for its simplicity and effectiveness, as it enables the concealment of secret data by embedding it into the LSB of the cover video file. This process has minimal impact on the visual quality of the video, making the modifications imperceptible to the human eye.

The basic procedure for embedding a secret message using the LSB technique involves the following steps:

- Select a cover image of size M x N.
- Convert the message to be hidden into its binary form and embed it within the RGB components of the image.
- Apply a pixel selection filter to determine the optimal locations for embedding the data within the cover image.
- The filter is then used to modify the LSB of each pixel, ensuring that the most significant bits (MSB) remain unchanged.
- The message is then successfully embedded.

Different variations of the LSB method exist, depending on the technique used for selecting the pixels in the cover file for hiding the data bits.

III LSB ALGORITHM METHODOLOGIES

A] Simple LSB Substitution

This is the simplest LSB algorithm where a single Least Significant bit of each color(Red, blue or green) pixel is replaced with the bits from the secret data.
Example:
Consider a pixel with RGB values as R=170(10101010), G=85(01010101), B=200(11001000)
Let us hide following message in above pixel: `101` (3 bits)
Modified Pixel after hiding secret message in LSB is as follows (R=171, G=84, B=201):
Red: `10101011`
Green: `01010100`
Blue: `11001001`

B] LSB in multiple bits (n-LSB)

In this technique we modify multiple bits across multiple bytes instead of modifying single LSB.
Example, you might modify the 2 least significant bits (or even more) of each byte, or distribute the hidden data across multiple adjacent bytes.
Example:
Secret Data to hide = A (65) Binary equivalent=01000001
Cover Data bytes = Byte 1: `11101101`
Byte 2: `10011011`
First 4 bits of the data: `0100`
Last 4 bits of the data: `0001`

Modify 2 LSBs per byte:
Byte 1 (before): `11101101` → Byte 1 (after): `11101100` (the last 2 bits change to `00`)
Byte 2 (before): `10011011` → Byte 2 (after): `10011001` (the last 2 bits change to `01`)

C] Hash based LSB Algorithm

A video file can be treated as a sequence of frames, with secret data being embedded into these frames as a payload. Information from the cover video, such as the number of frames (n), frame rate (fps), and frame dimensions (height H and width W), can be extracted from the file's header. Once the cover file containing data is obtained, the video (cover file) is divided into individual frames, and a Least Significant Bit (LSB)-based technique is applied to embed the secret data within the carrier frames. The message size is not a limitation in video steganography, as the data (secret message) can be easily distributed across multiple frames.

In the hash-based LSB algorithm, eight bits of secret data are embedded at a time into the LSB of the RGB (Red, Green, and Blue) pixel values of the carrier frames, following a 3, 3, 2 pattern. This means that six bits are inserted into the red and green pixels, while the remaining two bits are placed in the blue pixel. This distribution is chosen because the human eye is less sensitive to variations in the blue channel than in

the red and green channels, preserving video quality while increasing the data capacity.

Additionally, this slight color variation is difficult for the human eye to perceive. The specific LSB bit position used for embedding is determined by a hash function:

k=p%n

where k represents the bit position within the pixel, p denotes the position of the hidden data pixel, and n refers to the number of LSB bits. By distributing the bits randomly during the embedding process, this approach enhances the robustness of the technique compared to other LSB methods.

After embedding the data into multiple frames, the frames are reassembled to create the final stego video, which can be streamed as a regular video sequence.

D] Pseudo Random number generator LSB algorithm

In Random LSB algorithm a Pseudo random number is generated. Pixel are selected from the cover file based on the above generated pseudo random number. Calculate the LSB of the randomly selected pixel and embed the random id into the image array. Replace Least Significant Bit(LSB) of cover image with each bit of secret message one by one. Finally write the stego image.

Xn+1 = (aXn + c) MOD m

where X is the sequence of pseudo-random values that are generated.

m is the modulus which should be greater than 0

a is a multiplier that should be greater than 0 and less than m

c is a increment value that should be greater than or equal to 0 and less than m

X0 is the seed or start value that should be greater than or equal to 0 and less than m

E] Knight tour LSB Algorithm

The Knight's Tour algorithm is inspired by the movement of a knight on a chessboard, where the knight visits each square exactly once. After dividing a video into frames, this method represents the selected frame as a chessboard. The knight's movement—an "L" shape, consisting of one row and two columns or two rows and one column—is used to randomly select pixels for embedding data. This strategy enhances the robustness of the proposed method by addressing the limitations of the traditional LSB method, which selects pixels in a sequential manner, making it more vulnerable to electronic attacks.

The key distinction between the Knight's Tour method and the Pseudo-Random Number Generator technique is that the Knight's Tour algorithm is a custom-developed approach based on the classic Knight's Tour problem. This makes it highly resistant to detection by unauthorized receivers.

The general steps of the Knight's Tour algorithm are as follows:

1. Divide the image's width and height by four, ignoring any extra pixels.
2. Split the image into 4x4 pixel blocks.
3. Begin at the pixel indicated by the stego-key, and traverse all pixels in a block before moving on to the next.
4. Ensure that all four squares within a block are traversed before advancing to the next block.
5. After completing the traversal for one colour channel, proceed with the next.
6. Repeat these steps until all pixels in the image have been covered.

Once the pixels are selected using this algorithm, the LSB technique is then applied to embed data bits into the chosen pixels.

IV PARAMETERS USED FOR COMPARISON

1) Peak Signal to noise ratio (PSNR)

The Peak Signal-to-Noise Ratio (PSNR) is an indicator used to evaluate the quality of a signal by comparing its maximum possible strength with the amount of noise that distorts it. In image processing, PSNR measures the difference between a stego-image (which holds embedded secret data) and the original, unmodified cover-image [4]. The Peak Signal-to-Noise Ratio (PSNR) is calculated using the following formula:

$$PSNR = 10\log_{10} \frac{MAXI^2}{MSE}$$

2) Mean Square Error (MSE)

The Mean Squared Error (MSE) is a metric that quantifies the average squared difference between an estimator's prediction and the true value it aims to estimate. This discrepancy arises due to factors like randomness or limitations in the estimator's ability to incorporate all relevant information for a more accurate prediction [2]. Mean Squared Error (MSE)

and Peak Signal-to-Noise Ratio (PSNR) are inversely related, meaning that as one increases, the other tends to decrease. The MSE can be evaluated using the following formula:

$$\text{MSE}=\frac{1}{M \times N}\sum_{i=0}^{M} \quad \sum_{j=0}^{N}[I(i,j)-K(i,j)]^2$$

Where
M and N are the dimensions (height and width) of the image.
I (i, j) is the pixel value at position in the original image.
K (i, j) is the pixel value at position in the processed or reconstructed image.
The summation is taken over all pixels in the image.
The MSE value calculates the average squared error between the two images, with a lower value indicating higher similarity between the images.

3) Security

In data hiding, security is a critical factor. It assesses how well-protected the hidden information is and how challenging it would be for an unauthorized party to bypass the algorithm and retrieve the concealed data.

4) Text Retrieval

Text retrieval pertains to the quantity of text that an intruder could access if they successfully compromise the security measures. This metric is important because an attacker may occasionally extract partial information and subsequently use a brute force approach to reconstruct the complete text pattern. This concept is related to the confusion property in cryptography, which states that the cipher text should be derived from every position of the plaintext.

V COMPARATIVE ANALYSIS

Algorithm	PSNR	MSE	Security	Text Retrieval
Simple LSB Substitution	Moderate	Low	Low	High
LSB in multiple bits (n-LSB)	Low	High	Moderate	High(Less Reliable if altered)
Hash based LSB Algorithm	Higher	Lower	Moderate to High	Reliable
Pseudo Random number generator LSB algorithm	Higher	Low	High	Good (Seed Dependent)
Knight tour LSB Algorithm	High	Low	High	High(PatternDependent)

VI CONCLUSION

In the given paper we have tried to explain about different methodologies of LSB algorithm and how the algorithm work. We even tried to compare different methodologies by considering the following parameters PSNR, MSE, Security and Text Retrieval.

REFERENCES

[1] Kunhoth, J., Subramanian, N., Al-Maadeed, S. et al. Video steganography: recent advances and challenges. Multimed Tools Appl (2023). https://doi.org/10.1007/s11042-023-14844-w

[2] V. Esther Jyothi *et al* 2020 *IOP Conf. Ser.: Mater. Sci. Eng.* 981 022028DOI 10.1088/1757-899X/981/2/022028

[3] H. O. Nasereddin, Hebah. (2011). DIGITAL WATERMARKING A TECHNOLOGY OVERVIEW. IJRRAS. 6.

[4] Arijit Basu, Gaurav Kumar , Soumyajit Sarkar A Video Steganography Approach using Random Least Significant Bit Algorithm International Journal of Science and Research (IJSR)

[5] Younus, Zeyad Safaa and Younus, Ghada Thanoon. "Video Steganography Using Knight Tour Algorithm and LSB Method for Encrypted Data" Journal of Intelligent Systems, vol. 29, no. 1, 2020, pp. 1216-1225. https://doi.org/10.1515/jisys-2018-0225

[6] Soo Ann Nie1 , Ghazali Sulong2 , Rozniza Ali3 , Andrew Abel4 The use of least significant bit (LSB) and knight tour algorithm for image steganography of cover image Vol. 9, No. 6,

December 2019, pp. 5218~5226 ISSN: 2088-8708, DOI: 10.11591/ijece.v9i6.pp5218-5226

[7] Huma Jabeen, Prof. Abdul Wahid Image Steganography using Pseudo Random Number Generator, International Journal of Advanced research in Computer Engineering and Technology (IJARCET) , volume 8, issue 3 , March 2019, ISSN- 2278-1323

[8] Bhagyashri Rahangdale et al Int. Journal of Engineering Research and Applications www.ijera.com ISSN : 2248-9622, Vol. 4, Issue 1(Version 3), January 2014, pp.44-49

[9] Kousik Dasgupta , J.K. Mandal and Paramartha Dutta HASH BASED LEAST SIGNIFICANT BIT TECHNIQUE FOR VIDEO STEGANOGRAPHY(HLSB) International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No 2, April 2012

[10] Iti Naidu, Deepak Xaxa, Survey on Video Steganography Algorithms, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878 (Online), Volume-6 Issue-2, May 2017