A Study Of Steganography Methods Based On Image,Video And Audio

Ujjwala Rathod[1], Atharv Pawar[2] ,Siddhant Nilange[3] , Prof. Yogesh Shepal[4]

Computer Engineering Department[1,2,3,4]
Nutan Maharashtra Institute of Engineering and Technology, Pune, Maharashtra[1,2,3,4]

***Abstract*—**Presently, the focus on security intensifies owing to the widespread utilization of the internet. Correspondingly, the surge in internet usage has led to an increase in the daily exchange of data. This upsurge in data exchange poses a potential risk of deceit by hackers. An effective strategy to tackle this issue is Steganography. Steganography involves the covert embedding of confidential information within harmless cover files, rendering the detection of the hidden data challenging. This study delves into video Steganography, a technique wherein data is concealed within video frames. It proposes a dual-layered security strategy, employing both Steganography and cryptography. Initially, the data undergoes encryption using cryptographic algorithms, fol- lowing which the encrypted data is integrated into video frames. The embedding method employed is LSB coding, known for its simplicity and efficacy in concealing large amounts of data.

***Index Terms*—**Steganography, Multimedia Security, Video Steganography, LSB Coding, Adaptive Embedding, Content Authentication, Copyright Protection, Covert Communication.

I. INTRODUCTION

The term ”steganography” has its roots in the Greek words ”stegos” and ”grafia,” which translate to ”cover” and ”writing” respectively, giving rise to the concept of ”covered writing.” Steganography encompasses two fundamental processes: embedding, which conceals or compresses data, and extracting, which retrieves the concealed data. It embodies both an artistic and scientific approach, with historical techniques spanning centuries.

While not a novel concept, steganography has served as a clandestine communication method for ages. It enables individuals to discretely transmit messages by hiding them within various media formats, including text, audio, images, or digital videos. Specific algorithms are used to integrate the concealed message into the media, resulting in a ”stego” file that is then transmitted to the intended recipient.

Before utilizing steganography, several factors must be considered:

a. Embedding Capacity: The maximum amount of data that can be concealed within a cover file without compromising its original quality. The size of the embedded data must not exceed that of the cover file to ensure successful steganography.

b. Undetectability: The concealed data should remain invisible to unintended viewers within the original file. Any detection of the hidden message signifies a failure in steganographic concealment.

c. Robustness: The capability of the embedding algorithm to preserve the integrity of the concealed data even after compression and decompression processes.

d. Security: Guaranteeing that the hidden messages remain confidential and imperceptible to unauthorized individuals. Security in steganography involves hiding messages from unauthorized parties while facilitating communication between senders and recipients.

e. Tamper Resistance: Preventing deliberate tampering or sabotage of the embedded message by users with access to the carrier file. The resilience of the carrier file is crucial in thwarting decryption attempts.

The concealment of secret messages typically employs techniques such as Least Significant Bit (LSB) embedding and adaptive methods. Imperceptibility is closely linked to the security of steganography methods, ensuring the secrecy of the embedded message within the video.

A. Steganography

Steganography falls under the category of covert communication techniques, distinct from legitimate methods, aimed at concealing limited information within a cover medium[1]. It stands as one of the most commonly employed techniques for data concealment. The cover medium may comprise audio, video, images, or text. In this proposed approach, video serves as the cover medium for concealing sensitive information. While cryptography may reveal the presence of confidential data amidst jumbled text, steganography completely conceals the existence of such data within innocuous media. Detecting the presence of sensitive information hidden behind a video is exceptionally challenging. Once the data is concealed within the video, alterations in the original video size become apparent when comparing it to the encrypted video.

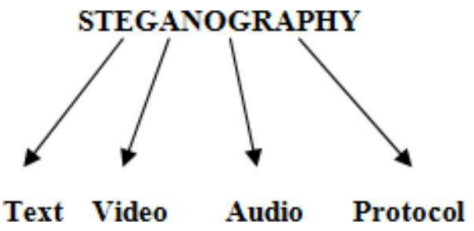

Fig. 1. Types of Steganography

The illustration illustrates the various methods of steganography. There are five categories available for concealing confidential data. Concealing data within protocols entails concealing it behind the OSI layer[5]. Concealing data within a video is analogous to concealing it within an image. In the proposed framework, videos serve as the cover medium, where they are segmented into frames or images to conceal the confidential information. The concealed information can be in text or document format, chosen for concealment within the video. The proposed system employs the DES encryption algorithm for data encryption. The LSB technique is utilized for embedding the encrypted data within the video, resulting in the creation of stego media. This stego media represents the encrypted video within which the data is concealed.

TYPES OF STEGANOGRAPHY METHODS

Image Steganography

Concealing information within a carrier image while maintaining image quality and robustness against unauthorized access is a meticulous process in image steganography [6]. The secret message is discretely embedded into the carrier imageas imperceptible noise, ensuring that it remains invisible to human eyes. Implementation details of image steganography involve various algorithms and techniques: Least Significant Bit (LSB) Embedding: This technique involves replacing the least significant bits of pixel values with the bits of the secret message. Since LSBs contribute minimally to the overall pixel value, the alterations are typically imperceptible. Spread Spec- trum Technique: This method disperses the secret message across the carrier image's frequency spectrum. By modulat- ing the frequency components, the hidden message blends seamlessly with the image's natural variations. Transform Domain Techniques: These techniques operate in frequency or spatial domains, such as Discrete Cosine Transform (DCT) or Discrete Wavelet Transform (DWT). The secret messageis embedded by manipulating coefficients in these domains, minimizing visual impact. These implementation methods ensure that the concealed information remains undetectable while preserving the integrity of the carrier image. Discuss the applications and uses of image steganography in various fields.

1) Spatial Domain Technique: To conceal data, certain bits are directly altered within the image pixel values on a bitwise basis. This technique involves manipulating pixel intensities and introducing noise. A prevalent approach in the spatial domain is the Least Significant Bit (LSB) embedding method.

2) Transformation Domain Technique: This method is susceptible to threats posed by image processing operations like compression, cropping, and enhancement. It conceals the secret message within significant areas of the carrier image.

3) Implementation in Transformation Domain: Initially, the image undergoes conversion from the spatial domain to the transformation domain. Subsequently, mathematical functions are employed to embed the secret message into the carrier image.

4) Distortion Technique: Data is embedded and preserved within signal distortion. This approach demands meticulous consideration to distinguish between the original carrier image and the stego image during the decoding process.

5) Masking and Filtering: This method is commonly utilized with 24-bit or grayscale images, employing masking and filtering processes to conceal a message. Comparable to paper watermarking, it incorporates information into prominent image areas rather than merely introducing noise.

Audio Steganography

Audio Steganography: The Human Auditory System (HAS) exhibits greater sensitivity compared to the Human Visual System (HVS), which poses a challenge in embedding messages within audio files using various methods, making it more complex than other formats.

These are the most common method that uses for embedding process in audio file:

1) LSB Coding
2) Parity Coding
3) Echo Data Hiding

In Audio steganography, there is some format that can use as a cover media for embedding the file such as MP3, WAV, MIDI etc.,[3].

a. LSB Coding: In this technique, the least significant byte of the carrier file is substituted with the bytes of the secret message. Typically, the rightmost bit is selected for replacement as it serves as the LSB, exerting minimal impact on the file's quality [1].

Parity Coding: This method involves checking the parity bit of the cover file for similarity. If similarity is detected, no action is taken. However, if dissimilarity is found, any least significant bit (LSB) will be subtly altered (either in the cover file or secret message) to ensure parity equality [4].

Echo Data Hiding: a) The information is inserted by introducing an echo sound to the cover file. The embedding of data is characterized by parameters such as decay rate, initial amplitude, and delay [8]. b) The initial amplitude is used to determine the original data sound. c) The decay rate is useful for the determination of the echo function to be made. d) The Offset function is used to determine the distance between the original speech signals with the echo that has been made.

Spread Spectrum: In this technique, the secret message is encoded and dispersed across the entire frequency spectrum. It entails transmitting a narrow band of information signal across

existing broadband channels. The spreading of the signal is aimed at augmenting the signal's redundancy level. The degree of redundancy is determined by a scalar multiplier known as cr. The length of the scalar value of cr dictates the number of bits involved [5].

Video Steganography

Embedding a message within a video parallels the art of concealing information, where the sender's goal is not only to hide the message but also to ensure its confidentiality from anyone other than the intended recipient. This process forms a core component of information concealment, safeguarding hidden messages from exposure. Video-based steganography techniques closely resemble those used in image-based methods, categorized [6].

In evaluating performance, the capacity and imperfections of video steganography play crucial roles. Spatial domain algorithms demonstrate superior steganography capacity by directly integrating information into the carrier image without causing noticeable visual alterations, thereby preserving high-quality output. Conversely, transformation domain algorithms embed secret information within the transform space. Although offering improved stability, this method generally supports a smaller capacity [2].

II. LITERATURE SURVEY

The study implements Audio-Steganography, concealing data within another medium, such as an audio file. In this technique, messages can be obscured within MP3-like sound files. Concealing data within audio files presents greater complexity compared to other steganography types or mediums. The paper delves into various audio steganographic methods, elucidating their respective advantages and disadvantages. Firstly, LSB coding is examined, recognized as the most prevalent and straightforward technique, yet efficient in ensuring security. Secondly, Phase coding is explored, though it suffers from a drawback of low data transmission rates. Lastly, spread spectrum is discussed, which introduces noise during the process of concealing data within audio files [5] .

The paper presents a novel system termed Steganography Imaging System (SIS), providing dual-layer security. In this system, cryptography is not utilized for the initial security level; rather, a username and password are employed for login authentication. The secret key is exclusively used for extracting the hidden message from the image, not for encryption. The proposed system transfers the secret message to a text file, which is subsequently compressed into a zip file. Following this, the zip file undergoes conversion into binary codes for embedding the message into the image. Utilizing a zip file enhances security compared to a conventional text file [8].

Khosala et al.'s paper merges Video Steganography and Digital Watermarking to establish a robust security framework. A novel algorithm is introduced to enhance security and streamline data transfer between the source and destination.This paper integrates Digital Watermarking with steganogra- phy, wherein a digital signal or pattern is embedded into digital content. Initially, the secret data is converted into binary form, followed by the application of the Least Significant Bit (LSB) technique to substitute the least significant bit of the cover image pixel with the binary bit. Post-LSB application, a combination of Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) techniques is employed on the stego image to generate a watermarked image. This watermarked image is then securely transmitted to the destination.

This paper concentrates on concealing images as confidential information within video frames. In addition to employing the LSB approach, Masking-Filtering techniques are utilized to conceal the secret image within a frame. Initially, the video is converted into frames and stored in individual files, with only one frame designated for hiding the input image. Masking and Filtering techniques are then employed to analyze the image, identifying significant areas for embedding the secret image to enhance security. These techniques are commonly applied to 24-bit and grayscale images. A stego key is employed to embed the message into the video clips [9].

The initial step outlined in this paper entails encrypting the data using the AES algorithm, a widely adopted encryption technique. Furthermore, the pixel swapping technique is employed to conceal the message within the video. A frame is randomly chosen, and its Red, Green, and Blue channels are separated. To hide the data, a specific channel is chosen, with the blue channel being utilized in this scenario. For each selected frame, the pixel positions of the blue channel are swapped using a designated key.

This paper delves into the most common steganographic technique, namely the Least Significant Bit (LSB). It explores an advanced LSB technique for concealing data within images. While the conventional method involves altering the least significant bits of the image with the message bit, the advanced technique randomly inserts message bits into the image. This advanced LSB technique aims to enhance security by randomly inserting message bits not only into the least significant bit but also into other bits. If the message bit and pixel bit match, a 1 is inserted into the least significant bit; otherwise, a 0 is inserted. The stego image is assessed against the original image using Mean-Squared Error (MSE) and Peak Signal-to-Noise Ratio to gauge the effectiveness of the techniques.A lower MSE value signifies minimal alteration between the original and encrypted images.

III. METHODOLOGY

Initially, the project was developed using MATLAB version 2015, which was also utilized for designing the user interface. Two algorithms were integrated for internal computation within the project. The first is the DES algorithm, utilized for encrypting the secret data and decrypting it at the receiver's end. The second is the LSB (Least Significant Bit) algorithm,

utilized for concealing the secret data behind the frames of videos. Moreover, the ”audioread” function of MATLAB was utilized to extract the audio file separately from the video file.

A. DES Algorithm

The DES algorithm, a symmetric key algorithm, employs a single private key for both encryption and decryption processes. It remains one of the most widely used algorithms for encryption and decryption owing to its speed and efficiency compared to others. Its computational efficiency is attributed to its 16 rounds of iterations, each performing various operations.

During encryption, the DES algorithm executes bit shuffling, non-linear substitutions (S-box), and exclusive-OR operations within each iteration. Particularly significant are the Substitution and Permutation operations. Substitution involves mapping different values to each other, while Permutation rearranges the bit positions to achieve the permuted input. These techniques are iteratively applied throughout each round.

The DES encryption algorithm requires two inputs-

1. Plain text to be encrypted.
2. Secret key.

The DES algorithm functions on a 64-bit block of plaintext, generating a 64-bit block of ciphertext as output. The input to DES comprises the plaintext block and a secret key, which remains consistent at both the sender and receiver ends. Usually, the secret key has a length of 64 bits. However, every eighth bit of the total key length is omitted as it is allocated for parity checking purposes [7].

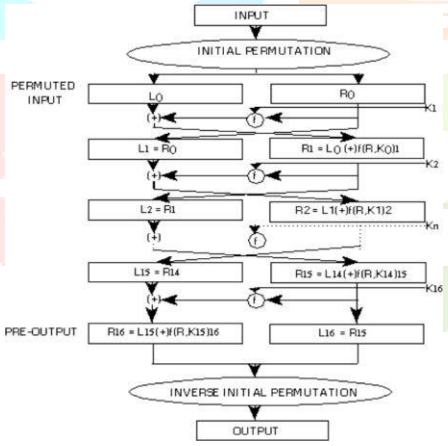

Fig. 2. DES Algorithm

The process commences with the initial permutation, rearranging the bits to produce the permuted input. Subsequently, the input is divided into two halves, each consisting of 32 bits. In each iteration, the function f is applied, as illustrated in the figure [11].

The diagram illustrates the initial step, wherein the right half of the input is expanded from 32 to 48 bits to match the length of the 48-bit key. Subsequently, an XOR operation is conducted between the key and the right half of the input, resulting in a 48-bit output. This output serves as the input

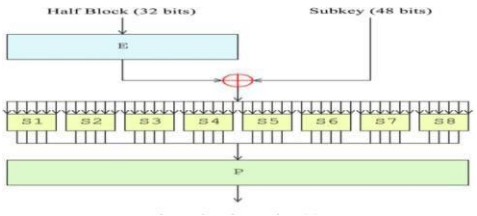

Fig. 3. Fiestel Function (F)

to the S-boxes, where each S-box accepts a 6-bit input and generates a 4-bit output. This process yields a total of 32 bits from 8 S-boxes. The output from the S-boxes undergoes permutation using the P-box. This entire process constitutes one round. Upon completion of all rounds, the left and right halves are concatenated without being exchanged, resulting in the encrypted data.

Throughout the encryption process, the 48-bit key undergoes modification. Different combinations of 48-bit subkeys are generated at each round through circular shifts. [5] The decryption process mirrors the encryption process, but with the key used in reverse order. Instead of left shifts, right shifts are employed to generate the subkeys.

Numerous cryptography algorithms are available for encryption and decryption. Initially, symmetric cryptography is preferred due to its use of only one secret key, simplifying implementation. In contrast, asymmetric cryptography involves two keys - a private and a public key - rendering it more complex and time-consuming compared to symmetric cryptography. Within symmetric cryptography, the preference for using the DES algorithm lies in its relatively lower time consumption compared to AES.

B. LSB Coding

This paper employs the well-established method of embedding messages into frames, known as the Least Significant Bit (LSB) technique. In this method, the least significant bits of the pixel values within the frames are modified to accommodate 1 bit of secret data per pixel. The LSB technique is renowned for its simplicity and speed in concealing data within video frames, making it a popular choice for embedding data into video clips.

With the LSB technique, secret data can be embedded into the least significant bits of the pixel values within the frame. During the embedding process, 3 bits of the message can be concealed within the pixels, with each RGB component housing 1 bit of data. This enables efficient and inconspicuous data embedding within the video frames.

The Bitmap (BMP) image format is utilized in this study. Consider the following pixels from a 24-bit image: (00101110 00001110 11001101) (00011101 10101101 00001100) (11101111 10100000 11000011)

As an example, let’s embed the character ”b”. First, it is converted into its ASCII value, which is 98. Then, we obtain the binary representation of this ASCII value, resulting in

1100010. Subsequently, we embed this character into the pixels of the image: (00101111 00001111 11001100) (00011100 10101100 00001101) (11101110 10100000 11000011)

As demonstrated in the example, only a single-bit change in each pixel is imperceptible.

LSB coding serves as a common and straightforward technique. Despite its simplicity, it facilitates a swift embedding process, ensuring accurate data extraction at the receiver's end. Its ease of implementation and ability to provide enhanced security contribute to its widespread adoption.

IV. SYSTEM ARCHITECTURE

The System Architecture delineates the overarching procedure of the concept implemented in this paper. Figure 4 illustrates the array of algorithms and techniques employed in this implementation.

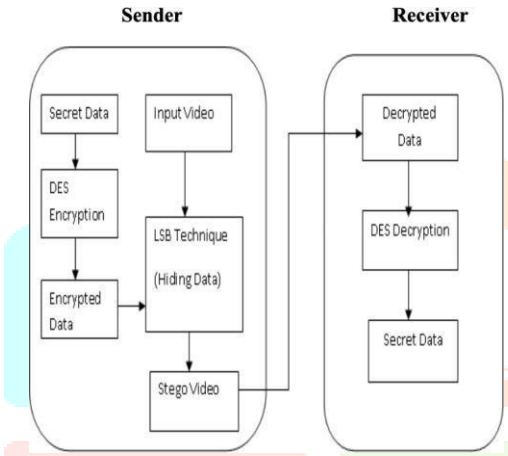

Fig. 4. System Architecture

In the current system, the initial step involves receiving input from the user, which serves as the cover file behind which data will be concealed. The cover file may be in various formats such as text, audio, or video. However, for this project, video serves as the cover file. The system then prompts the user to provide the secret data to be hidden within the frames. In this implementation, the secret data is limited to text documents, although it could theoretically include images. Due to the complexity of processing and concealing data within images, text data is chosen for this project.

The secret data undergoes DES encryption, involving 16 rounds of processing. The DES algorithm requires the user to input a secret key, acting as a password to ensure data security. This key must also be known to the receiver to decrypt the data successfully. Once the encryption process is complete, the encrypted data is obtained.

Next, the encrypted data and the cover video are supplied as inputs to the embedding process, which employs the LSB technique to conceal the secret data within the video frames. The "audioread" function is utilized to read the audio file associated with the video. The number of bits in the secret message is stored in the first frame of the video. Subsequent frames each contain one bit of the message, enabling the distribution of the entire secret message across the video frames. The outcome of this process is a stego video, where the encrypted data is hidden behind the frames.

Upon receiving the stego video, the receiver can utilize the same LSB technique to extract the encrypted data from the video. Since the first frame contains the number of bits comprising the message, only that many frames are processed to retrieve the data. [4] The output of this process is the encrypted data. The DES decryption algorithm is then applied to the encrypted data to recover the original secret data. This decryption process mirrors the encryption process, with 16 rounds of iteration applied.

In contrast to the existing system, where the data is concealed behind only one frame (with the frame number provided by the user), the proposed system conceals the data across multiple frames. This modification mitigates the potential introduction of noise in the video caused by data concealment in a single frame.

In the proposed system, each frame hides 3 bits of the message, distributing it across the entire video. [6] This prevents any single frame alteration from significantly affecting the entire video.

An advantage of this system is that the first frame always contains the total number of bits in the message. This allows the receiver to determine the number of frames containing hidden data, simplifying message retrieval without additional processing [2].

CONCLUSION

The proposed video Steganography system offers two layers of security: first with cryptography and second with Steganography. The system conceals encrypted information within video clips, with each frame hiding 3 bits of data. Testing with various sizes of videos and secret data demonstrates that no noticeable noise is introduced in the encrypted video, maintaining similarity to the original video. The stego video, containing hidden data, is sent to the receiver who possesses the secret key. The existence of secret information is virtually undetectable, ensuring safe and secure data transfer to the destination.

The DES algorithm utilized for data encryption is simple yet efficient, providing a fast and effective means of securely transferring data. Despite its simplicity and common usage, the DES algorithm remains a robust choice for encryption purposes.

REFERENCES

[1] Yogesh R Shepal and Ashraf Shaikh. A fast clustering-based feature subset selection algorithm for high dimensional data. *International Journal of Research Studies in Science*, 1(7):1–6, 2014.

[2] Chhaya Varade, Danish Shaikh, Girish Gund, Vishal Kumar, Shahrukh Qureshi. "A Technique for Data Hiding using Audio and Video Steganography." *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 6, Issue 2, February 2016.

[3] Rosziati Ibrahim and Teoh Suk Kuan. "Steganography algorithm to hide secret message inside an image." *Com- puter Technology and Application*, 2 (2011), 102-108.

[4] Shivani Khosla, Paramjeet Kaur. "Secure Data Hiding Technique using Video Steganography and Watermark- ing." *International Journal of Computer Applications*, Volume 95, No.20, June 2014.

[5] K. Steffy Jenifer, G. Yogaraj, K. Rajalakshmi. "LSB Approach for Video Steganography to Embed Images." *International Journal of Computer Science and Informa- tion Technologies*, Vol. 5 (1), 2014, 319-322.

[6] Miss. Uma Sahu, Mr. Saurabh Mitra. "A Secure Data Hiding Technique Using Video Steganography." *Interna- tional Journal of Computer Science & Communication Networks*, Vol 5(5), 348-357.

[7] Obaida Mohammad Awad Al-Hazaimeh. "Hiding Data in Images Using New Random Technique." *International Journal of Computer Science Issues*, Vol. 9, Issue 4, No 2, July 2012.

[8] Hsien-Chu Wu, Na-I Wu, Chwei-Shyong Tsai, Min- Shiang Hwang. "An Image Steganographic Scheme Based on Pixel-Value Differencing and LSB Replace- ments Methods."

[9] K. Saranya, Dr. C. Suresh Gnanadhas, Minu George. "Data Embedding Techniques in Steganography." *Inter- national Journal of Latest Trends in Engineering and Technology*, Volume 3, Issue 2, November 2013.

[10] Syeda Musfia Nasreen, Gaurav Jalewal, Saurabh Su- tradhar "A Study on Video Steganographic Techniques", Internatinal Journal of Computational Engineering Re- search Volume 05, Issue 10, October 2015.

[11] Shikha, Vidhu Kiran Dutt "Text Steganography", Interna- tional Journal of Advanced Research in computer science and Software engineering, Volume 4, Issue 10,October 2014.