VIDEO STEGANOGRAPHY

Rahul Kumar[1]

Department of Master of Computer Applications,
Dayananda Sagar Academy of Technology and
Management Bangalore 560082, India

Shreedhara N Hegde[2]

Department of Master of Computer Applications,
Dayananda Sagar Academy of Technology and Management
Bangalore 560082, India

Abstract

Video steganography is a method for hiding sensitive information within video files without affecting the original video's quality. Building a technique for successfully and effi- ciently concealing data within a video file while simultaneously making sure that it will be simple to get the secret data and the original film remains the same would probably be the aim of a video steganography project.

Because safe communication is necessary in the digital age, A greater and greater importance is being placed on this technology. The video steganography procedure entails three steps: the secret data is being inserted, transmitting to obtain our secret message, extract an algorithm or approach using a secret key. During embedding, the secret data is fixed. Video is either kept on a device or sent across a network during the transmission phase. Finally, using the same steganographic technique, During the extraction process, the intended recipient extracts the video file's hidden information. Potentially, the study might investigate further tactics for enhancing the security of the buried data, including the use of sophisticated steganographic methods and encryption. In the abstract of a video steganography project inside of video files, the goals and methods used to achieve efficient and secure data concealment would likely be summed up. The rapid growth of digital media and the widespread use of videos have heightened the need for effective methods to protect sensitive information. Video steganography, an emerging field in information security, offers a valuable solution by enabling the hidden transmission of confidential data within video files. This project focuses on the development of a video steganography system without AI content, aiming to enhance data security and privacy without the complexity of artificial intelligence algorithms.

The proposed system employs a combination of image-based and motion-based techniques to achieve robust and imperceptible data embedding in video streams. Initially, the video frames are analyzed, and suitable frames are selected for embedding the hidden information. The selected frames undergo a series of preprocessing steps to ensure optimal concealment of the data while maintaining the video's visual quality and integrity. To embed the confidential information, a secure and efficient data embedding algorithm is employed. This algorithm employs a spatial domain technique to modify the pixel values of selected frames subtly, thus embedding the data without raising suspicion. The video frames' statistical qualities are carefully maintained during the embedding procedure. ensuring minimal visual distortion and preserving the original video's temporal characteristics. The stegovideo's hidden information is recovered during the decoding stage using the same technique used for embedding. The extracted data is then reconstructed into its original format, providing the intended recipient with access to the concealed information. The decoding process ensures that only authorized individuals can retrieve the hidden data, reinforcing the system's security. The suggested video steganography solution comes with a number of benefits.

The absence of AI content reduces computational complexity while maintaining a high level of data security. The system can find applications in various domains, such as secure communication, digital rights management, and copyright protection.

Keywords —Steganography, LSB Technique, Splitting, Em- bedding, extraction.

I. INTRODUCTION

Video steganography is a technique for concealing sensitive data without altering how a video file is viewed. For safe data transfer and communication in the digital age, it is a crucial strategy. Using a cover medium that appears harmless, steganography, a type of information security, involves hiding data. like a picture, audio, or video file. Given that videos can store a lot of data and are widely used, video steganography is particularly beneficial. Identify applicable funding agency here. If none, delete this. are frequently employed for internet

business, leisure, and communication. The technique of steganography in videos involves a number of steps. Using a steganographic method, the hidden material is first integrated into the cover video. There are numerous steganography algorithms for video steganography techniques, such as (LSB) embedding, the F5 algorithm, and (DCT)-based techniques. These algorithms ensure that the hidden data remains unobservable to the human eye. The second stage involves sending or storing the steganographic movie. Several techniques can be used to relay the video, including email, instant messaging, and cloud storage. In the third stage, the secret data is extracted by the intended receiver using the same steganographic process. The quality of the cover movie, the skill of the attacker, and the steganographic technique used

all have an impact on how effective video steganography is. To avoid being discovered, the cover movie needs to be of the highest calibre and should not display any traces of modification. The assailant must possess a thorough comprehension of

Goals of this project to use different steganographic methods and create a system for secure data transmission and communication using video steganography. We shall investigate the numerous steganographic techniques and evaluate each one's performance, payload size, and security attributes. We will also look into the restrictions and difficulties that come with video steganography, for instance, there's always a chance that data will be lost during transmission or that an attacker would discover material that's been disguised. We will have developed a thorough understanding of video steganography and its useful applications by the project's conclusion. There are several uses for video steganography systems, including secure internet communication, commerce, and entertainment. The system in a video steganography project must first encode the secret message into an embeddable format. the secret message into a digital format and then using an algorithm to hide it within the video file. The secret message must be undetectable and the video quality must not be compromised, so the algorithm must be created accordingly. After the secret message has been encoded and inserted into the movie, the system must provide a mechanism to retrieve it. This is typically done by providing a decoder or extraction tool that can retrieve the hidden message from the video. The decoder must be able to find out the secret message and extract
it without damaging the video.

II. LITERATURE SURVEY

The many deep learning techniques used by researchers to
identify plant diseases are presented. According to

In their research, M. Sadek et al. created a blind and reliable method for video steganography based on the sections of video frames that depict human skin [1]. Before asking map developed They offer a method for identifying the skin parts in each frame of the cover video. Afterwards, the skin map is changed into a skin-block map, where error-prone skin pixels are not taken into account during the hiding stage.
The secret information is next quantized and written into the coefficients of the identified skin pixels in the skin-block map using a three-level DWT on the blue and red colour channels of each frame. Experiments have revealed that the suggested strategy is effective in achieving a high level.[1]

By employing cover movies with the H.264/AVC extension, K. Niu et al. established a novel reversible method for video steganography in their work They used histogram shifting (HS) of motion vector values to conceal the secret data inside the acknowledged reference frames of the cover film. The secret data can be recovered without any loss from the compressed cover video using their technique. The results revealed that, in terms of capacity and invisibility, their suggested technique performs better than other recently established alternatives in the literature. [2].

In their study ,K. Rajalakshmi and K. Mahesh proposed Zero Level Binary Mapping (ZLBM), a revolutionary method for video steganography. In their recommended method, First, frames are created from the cover video. The frames are then cleaned up using the Fuzzy Adaptive Median Filtering (FAMF) technique. The impulsive noise. Organising the pixels within the improved frames is done using the block-wise pixel grouping technique. The secret data is encrypted using the ZLBM technique and patch-wise code creation. The experimental findings show that, in comparison to other comparable solutions, the suggested technique outperforms them in terms of PSNR rate. [3]

Based on the H.265/High-efficiency video coding scheme, Y. Liu et al. proposed a novel and reliable approach for video steganography. in the paper, Their proposed method uses the BCH coding strategy to encrypt the private data before embedding. They employed three groups of the prediction directions to limit the intra-frame deformation drift. The encrypted secret data was then inserted into the multi coefficients of the chosen four by four luminance discrete sine transform blocks, which fit the groups. According to experimental findings, their suggested strategy produces superior visual quality than the earlier methods investigated.[4]

According to the research, Based on the dynamic and observable sections of a cover video, M. Hashem Zadeh proposes a successful method for video steganography. According to his approach, the feature points' motion cues are used to identify the dynamic regions, and these regions are subsequently used to determine the areas of interest. He employed the least-significant-bit replacement approach to hide the secret data inside the boundaries. When compared to the most recent methodologies described in the literature, experimental results demonstrated that his proposed method achieves a greater hiding capacity.[5]

The video-steganography technique is used in the paper to conceal data in a different medium, such as an audio recording. Using video steganography, we can cloak the message in sound files that mimic MP3s. More difficult than with other steganography types or mediums, the act of concealing the data behind the audio file. In this essay, the
benefits and drawbacks of several audio steganographic methods are discussed. The most well-known and essential technique, LSB coding, is the first and provides the highest level of security. Phase coding, the second-placed approach, has a low data transmission rate issue. The third, referred to as spread spectrum, entails the addition of noise while data is concealed under audio recordings.[6]

In the paper, A brand-new technology called the Steganography Imaging technology (SIS) is described in the publication. In the suggested system, there are two security levels. In this setup, a username and password serve as the first layer of login protection instead of cryptography. Here, rather than being used for encryption, the secret key is simply used to extract the hidden message from the image. In the suggested system, a text file containing the secret message is first transferred. The text file is then compressed to produce a zip file. In order to embed the message in an image, the zip file is next transformed into binary codes. A zip file should be used since it is safer than a standard text file.[7]

The combination of video steganography and digit watermarking used in the paper provides a strong foundation for security. In this research, a unique method for enhanced data security and effective data transfer between sources and destinations is presented. This article makes use of both digit watermarking and steganography. During digit watermarking, the digital sign or pattern is inserted into the digital content. Using steganography of any kind, including audio image, and text, can be concealed using this method. Fir binary transformation of the secret data is performed in this process. Then With the LSB method, the cover image pixel's least bit is changed for a binary bit. We get the stego picture following LSB. A watermarked image is created at this stage by processing the stego image using a combined DWT and DCT method. After that, the watermarked image is securely delivered to the destination. [8]

The paper describes how to hide an image behind video frames as hidden data. In addition to the LSB technique, the hidden image in the frame is hidden using the Masking- Filtering techniques. The movie is first divided into frames for this study and saved in a different file. The input image is hidden using only one frame. Masking and filtering techniques are frequently used during the examination of photographs. The secret image is strategically positioned in order to improve security. Only grayscale and 24 bit images are typically used with these two techniques. The message is integrated into the video segments using a key called the stego key.[9]

In the paper, encrypting the data comes first. For data encryption, the AES algorithm is the most widely used technique. In order to embed messages in videos, both the pixel swapping method and the AES algorithm are utilised. Once a random frame has been chosen, the pixel swapping method separates the Red, Green, and Blue channels of that frame. The concealing channel is then selected; in this instance, The blue channel is selected by the paper. With the aid of key, the blue channel's pixel coordinates a switched for each selected frame. protect the message using the AES encryption method. Embed this encrypted message using pixels to increase the double security. This article uses the concept of PSNR val computation to compare the original and stego photos. PSN, or peak signal-to-noise ratio, is anacronym. If comparing the two PSNR values, the stego picture has a higher value, the suggested system is regarded secure.[10]

III. METHODOLOGY

The LSB (Least Significant Bit) technique, a steganographic method, is employed in Fig. 1 to hide data in digital media files like images, audio files, and video files. It entails erasing every pixel of the final meaningful bit or audio sample using a piece of the secret text.

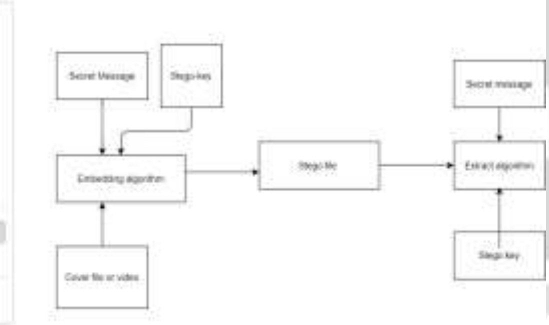


Fig. 1. methodology used in steganography

For legitimate objectives like encoding copyright information or putting a watermark to digital files, the LSB method is commonly used. However, it can also be employed maliciously for things like stealing confidential data or disguising malware. This makes it essential to be aware of the potential hazards associated with LSB steganography and to put the required security measures in place to prevent unauthorized access from being discovered by advanced analysis tools, especially when the steganography is not carried out properly.

Therefore, it is important to use this technique or algorithm of encryption and authentication techniques to protect sensitive message LSB steganography is not impenetrable and is susceptible to detection by advanced analytical methods, particularly when the steganography is not carried out correctly. Consequently, it is It is crucial to employ this encryption method or algorithm along with authentication methods to protect the vital information.

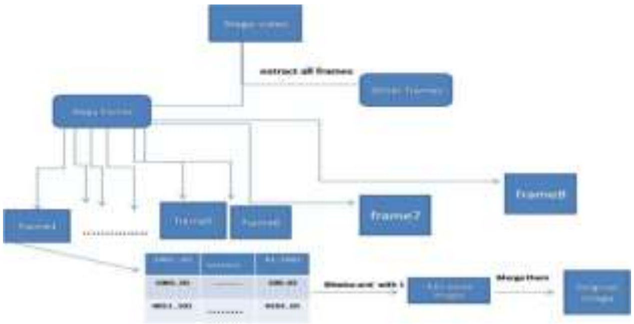


Fig. 2. System Architecture Diagram

In Fig 2 the architecture diagram of a video steganography project showcases the flow and interactions between these components, allowing for the seamless embedding and extraction of secret information within video files while maintaining the integrity and imperceptibility of the video content.

The architecture diagram of a video steganography project consists of several interconnected components that work together to achieve the goal of hiding secret information within video files. At a high level, the architecture typically includes a user interface, steganography engine, video file input/output module, encryption module (optional), and a steganalysis module (optional). The user interface component serves as the point of interaction for users, allowing them to input the secret message, Configure the steganography settings after choosing the video files to be utilized. To make user interaction with the system easier, this component offers either a graphical or command-line user interface. The essential component in charge of inserting the covert message into the video file and removing the covert message from the video is the steganography engine.

It employs various steganography techniques and algorithms, such as LSB (Least Significant Bit) manipulation, transform domain methods, or data hiding within specific video frames, to ensure the secrecy and imperceptibility of the embedded message. After the hidden message has been embedded, the video file input/output module handles loading video files from storage media and saves the steganographic video file. This module supports popular video formats such as AVI, MP4, or MKV, and provides functionalities for reading and writing video data. To provide another level of security for the secret message, the architecture can contain an encryption module. Before embedding the message into the video file, this module encrypts it using cryptographic techniques. Upon extraction, the message is decrypted using the corresponding decryption algorithm. An optional steganalysis module that scans a steganographic video for concealed information can be added to the architecture.

IV. Results and Discussions

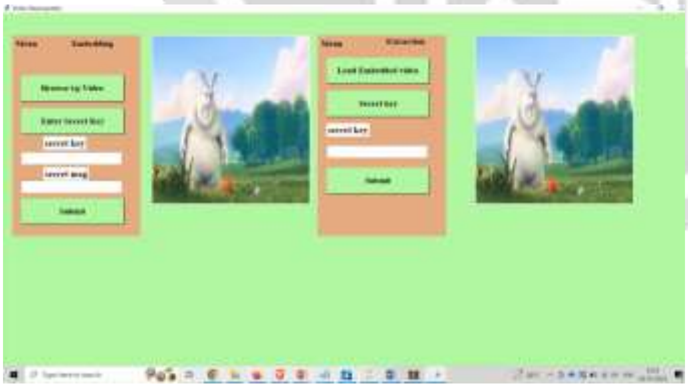
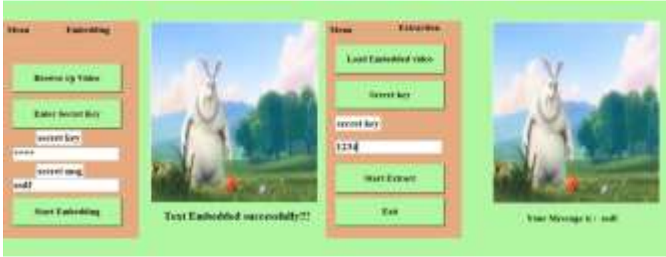


Fig. 3. Result Choose video and Enter key and message

The Fig. 3 and 4 shows the output screen where user can input details like secret key secret message with secret video to get the output. Following these guidelines, the user should input the values. The sender must first select the movie and enter the secret key before entering the secret message and submitting it. Then, they must click start embedding.



****

sndf

Text Embedded successfully!!

1234

Your Message is : sndf

Fig. 4. Result of Secret Message Extraction

For extracting load and embedding the video, enter the secret key which was set by sender. Submit it and extraction will start and secret text will displayed.

Video steganography is an intriguing field that holds significant potential for secure communication, data hiding, and covert transmission within video files. It involves concealing secret information within the visual and/or audio components of a video, making it a technology that has promise for a variety of applications, including digital watermarking, copyright protection, and content authentication. One of the key advantages of video steganography is making use of the large amount of storage that video files provide. Videos typically contain a vast amount of data, allowing for substantial hiding capacity. Additionally, the dynamic nature of videos, with a sequence of frames and audio, provides opportunities for embedding secret information at various levels, such as individual frames or groups of frames. However, video steganography also poses several challenges. The main concern is making sure the secret message cannot be detected. The visual and audio quality of the video should be maintained while the embedded information should be undetectable to a human observer. The complex challenge of striking a balance between imperceptibility and embedding capacity necessitates careful consideration of steganographic techniques and algorithms. The discovery of hidden information presents another difficulty for video steganography. Security of a steganography system is seriously jeo pardised by steganography analysis, which is the act of locating steganographic content. Steganalysis techniques constantly evolve, requiring steganographers to develop robust embedding methods that can withstand detection attempts. Moreover, the real-time constraints of video transmission and playback introduce additional complexities to video steganography. The embedding and extraction processes should be efficient and fast to accommodate real-time applications without compromising the quality and continuity of the video stream.

V. CONCLUSION

To summarise, video steganography is a technique that enables the concealment of information in a way that prevents it from being detected by the human eye, such as a message, a picture, or a file, within a video file. The practise of video steganography is expected to grow in popularity over the future years, particularly in the fields of security and technical forensics. The goal of this research was to develop a method for successfully and effectively concealing data within a video clip, ensuring that the original movie isn't changed, and ensuring that the hidden data is accessible. The study also investigated the use of sophisticated encryption and steganographic technologies to boost the security of the disseminated data. The suggested method combined numerous strategies, including steganography, encryption, and digital watermarking, and putting them into practise in a software programmer. The proposed solution was contrasted with the state-of-the-art video steganography techniques in order to determine its effectiveness and efficiency. The findings indicated that the suggested approach may cover up bigger amounts of data, provide a higher level of security, and and improve the quality of the original video once the data has been hidden. Overall, the suggested technique offers a fresh and enhanced way for video steganography that may be applied to many different situations, including secure communication and digi- tal forensics. of the video frame that resemble noise. In order to confirm that the secret message may be correctly extracted from the movie without any discernible video quality deteri- oration, the changed video file is tested and reviewed in the final step. Encryption, various steganographic techniques, a dynamic payload size, robustness, adaptive thresholding, and real-time processing are potential future improvements for a video steganography project. movie without any discernible movies.

VI. FUTURE WORK

Detected by sophisticated analysis techniques, especially when the steganography is not executed properly. Therefore, it is important to use this technique or algorithm of encryption and authentication techniques to protect sensitive message In a video file, secret information is concealed using video steganography. Several methods, including LSB embedding, DCT-based embedding, and F5, can be utilised to accomplish This algorithm. In LSB embedding, the bits of the concealed message are deleted along with the (LSB) of the pixel values in the video frame. In DCT-based embedding, the video frame's DCT coefficients are changed, and bits that contain the concealed message are inserted into the lower frequency bits. The F5 algorithm embeds the hidden message in the areas movie without any discernible video quality deterioration, the changed video file is tested and reviewed in the final step. Encryption, various steganographic techniques, a dynamic payload size, robustness, adaptive thresholding, and real-time processing are potential future improvements for a video steganography project. of the video frame that resemble noise. In order to confirm that the secret message may be correctly extracted from the movie without any discernible video with- out any discernible video quality deteri- oration, the changed video file is tested and reviewed in the final step. Encryption, various steganographic techniques, a dynamic payload size, robustness, adaptive thresholding, and real-time processing are potential future improvements for a video steganography project. me of the video frame that resemble noise. In order to confirm that the secret message may be correctly extracted from the movie without any discernible video quality deterioration, the changed video file is tested and reviewed in the final step. Encryption, various steganographic techniques, a dynamic payload size, robustness, adaptive thresholding, and real-time processing are potential future improvements for a video steganography project. movie without any discernible movie

REFERENCES

[1] M. M. Sadek, A. S. Khalifa and M. G. M. Mostafa, ”Robust video steganography algorithm using adaptive skin-tone detection”, Multime- dia Tools Appl., vol. 76, no. 2, pp. 3065-3085, Jan. 2017

[2] Himanshu Wadekar, Aishwarya Babu, Vaishali Bharvadia, P. N. Tat- wadarshi, ”A new approach to video steganography using pixel pattern matching and key segmentation”, 2017 (ICIIECS), pp.1-5, 2017.

[3] K. Niu, X. Yang and Y. Zhang, ”A novel video reversible data hiding algorithm using motion vector for H.264/AVC”, Tsinghua Sci. Technol., vol. 22, no. 5, pp. 489-498, Sep. 2017.

[4] K. Rajalakshmi and K. Mahesh, ”ZLBM: Zero level binary mapping technique for video security”, Multimedia Tools Appl., vol. 77, no. 11,
pp. 13225-13247, Jun. 2018.

[5] M. Hashemzadeh, ”Hiding information in videos using motion clues of feature points”, Comput. Electr. Eng., vol. 68, pp. 14-25, May 2018.

[6] Chhaya Varade, Danish Shaikh, Girish Gund, Vishal Kumar, Shahrukh Qureshi “A Technique for Data Hiding using Audio and Video Steganog- raphy”, International Journal of advanced Reseach in Computer Science and Software Engineering, Volume 6, Issue 2, February 2016.

[7] Rosziati Ibrahim and Teoh Suk Kuan “Steganography algorithm to hide secret message inside an image”, Computer Technology and Application 2 (2011) 102-108

[8] Shivani Khosla, Paramjeet Kaur “Secure Data Hiding Technique using Video Steganography and Watermarking”, International Journal of Com- puter Applications (0975 – 8887) Volume 95– No.20, June 2014.

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

[10] Miss. Uma Sahu, Mr. Saurabh Mitra “A Secure Data Hiding Technique Using Video Steganography”, International Journal of Computer Science Communication Networks, Vol 5(5), 348-357.