**VIDEO STEGANOGRAPHY USING LSB TECHNIQUES**

Lee Yung Yau 11, Dr Asif I Asif Iqbal Hajamydeen 21,,

*1Faculty of Information Sciences and Engineering, Management and Science University, Section 13, 40100 Shah Alam, Selangor Malaysia*

*1Faculty of Information Sciences and Engineering, Management and Science University, Section 13, 40100 Shah Alam, Selangor Malaysia*

**ABSTRACT**

Video steganography is a vital medium for covert communication, which enables the hiding of confidential and secret data within video files while preserving their visual quality. The Least Significant Bit (LSB) technique has been widely used in video steganography due to its simplicity and efficiency. However, existing LSB-based systems suffer from limitations such as low embedding capacity and vulnerability to steganalysis attacks. One of the primary objectives of the project is to increase the embedding capacity further while maintaining the visual integrity of the video. Additionally, with advanced LSB embedding techniques and encryption mechanisms, the systems maximise the amount of data hidden within the video while safeguarding its security and confidentiality. Rigorous testing and evaluation validate the system’s performance and demonstrate its effectiveness in securely embedding and extracting hidden data within video files. The developed video steganography system utilizing the LSB technique offers an efficient and reliable solution for covert communication.

*Keywords:* Least Significant Bit (LSB), Cover image, Stego-image, Mean Square Error (MSE), Peak Signal to Noise Ratio(PSNR)

**INTRODUCTION**

Steganography is the art/science of hiding the existence of the communication between the sender and the receiver. The word steganography comes from the Greek words Steganós (Covered) and Graptos (Writing) and means "hidden writing" [1]. Video steganography is a branch of information hiding focusing on concealing confidential or sensitive data within video frames while maintaining visual quality. Similar to image steganography, video steganography aims to hide data within the video frames so that the changes are imperceptible to human observers.[2] One widely used technique in video steganography is the Least Significant Bit (LSB) embedding technique. The technique of hidden messages mentioned is used to counter the attacks on data and provide security, privacy, confidentiality, and integrity to the sensitivity of the data it represents. [3].

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Article history:*

Received:

Accepted:

Published:

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

*E-mail addresses:*

[012021071606@fise.msu.edu.my](mailto:012021071606@fise.msu.edu.my)

asif@msu.edu.my

**MATERIALS AND METHODS**

*Materials*

In this study on video steganography using the Least Significant Bit (LSB) technique, a collection of standard 1080p resolution videos, primarily featuring basic RGB videos, were used as cover media for data embedding. These videos, with durations ranging from 30 seconds to 2 minutes and encoded in H.264 format, were processed using Python and OpenCV, along with a custom-developed LSB steganography library. The secret data embedded consisted of only text messages, compressed using gzip to optimize the payload. The LSB embedding algorithm was employed to modify the least significant bits of selected pixels within the video frames, primarily targeting the blue channel due to its minimal impact on visual perception. A strategic approach was adopted by embedding data in every 10th frame, and a key parameter in this process was maintaining the embedding rate below 2% of the total bits in a frame, ensuring data integrity and steganographic efficiency.

*Methods*

The experimental setup involved hardware consisting of the processor of AMD Ryzen 5 4600H with Radeon Graphics, with Windows 11 Home as the operating system and Python 3.10.11 with OpenCV as the development environment. The study's focus was on evaluating the steganographic capacity, imperceptibility (measured by PSNR), robustness against compression, and computational efficiency. Ethical considerations were paramount; the study avoided using sensitive or personal data, emphasizing the importance of legal and ethical usage of steganography. The research highlighted both the capabilities and the limitations of LSB in video steganography, providing insights into its practical applications and the challenges posed by compression techniques.

**RESULTS AND DISCUSSION**

Figure 1 illustrates the overview of the test diagram for the proposed Video Steganography using Least Significant Bit (LSB) techniques, it represents an innovative approach method that optimizes imperceptibility and robustness, achieving high hiding capacity and a high hiding ratio in digital video files [4]. This extended abstract delineates the core findings and discussions of a research project focused on implementing and evaluating LSB steganography in video content. The methodology centred around embedding data into LSB layers of video frames, utilizing developing tools such as Python and OpenCV for processing. The methodology also improvises extracting text and decrypting it with features to save the text as a file to the document folder. The algorithm targeted the blue channel for data embedding due to its lower impact on perceived image quality.

The embedding test results were promising, pushing up to 500 KB of data could be embedded into a one-minute 1080p video clip without noticeable quality loss. Standard 1080p resolution videos in H.264 format were chosen due to their wide usage and compatibility across various platforms. The videos varied in duration and content to mimic real-world scenarios. The process was relatively efficient, with data embedding and extraction times averaging 2 minutes and under 1 minute, respectively, on standard hardware. Embedding data in every 10th frame was a deliberate choice. This approach balances the need for a higher data capacity while reducing the risk of visual detection

As for Figure 2, it illustrates the overview of the test diagram for extracting and decrypting hidden text from the embedded test. Judging from the test results of the Video Text Extractor application, it was designed to extract and decrypt text from video frames. It underwent comprehensive testing to evaluate its functionality, performance, user interface, and error correction capabilities. The application adeptly handled mp4 video file formats and demonstrated high accuracy in frame extraction and text recognition using Tesseract OCR under controlled conditions. The AES decryption effectively processed the base64-encoded text using user-provided keys. Performance tests showed that the application maintained moderate CPU and memory usage while processing videos, with an average extraction time of 1 second per frame for a video consisting of 200 frames. The implementation of the Reed-Solomon error correction algorithm was successful in ensuring data reliability, even in the presence of minor data corruption during video processing. However, the research testing also identified potential limitations and areas for improvement. While the embedded data remained intact under moderate video compression, higher compression levels resulted in data loss, suggesting a need for balance between data capacity and robustness.

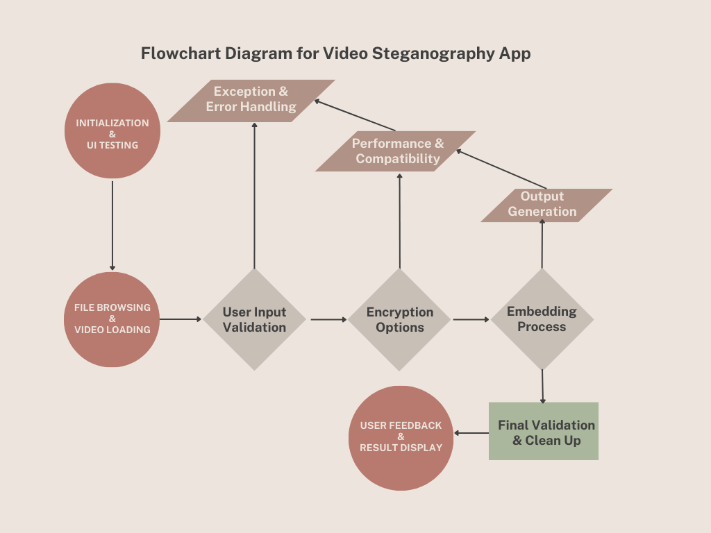


Figure 1: Test Diagram for Video Steganography App

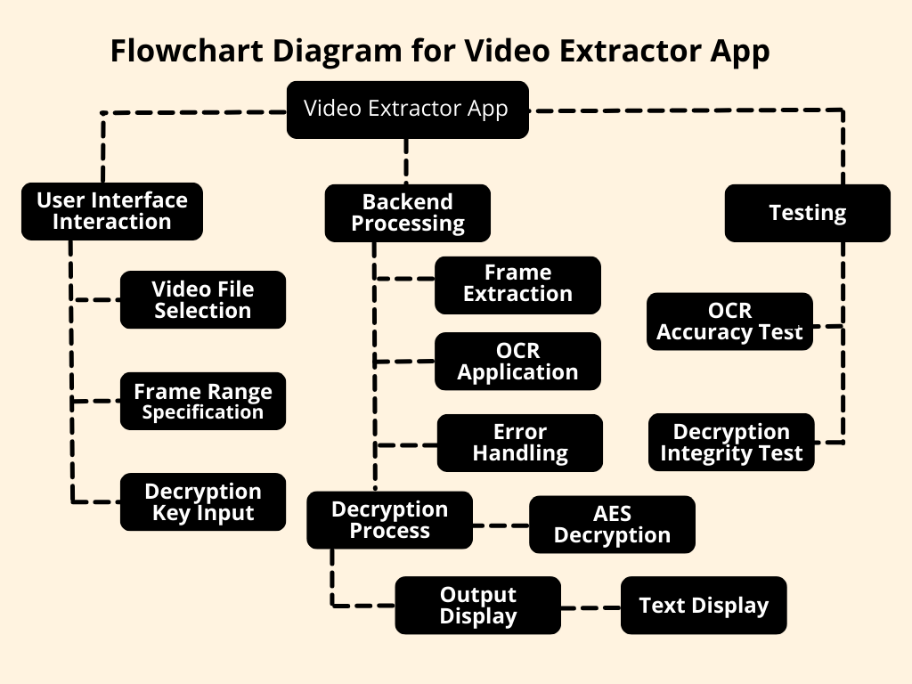


Figure 2: Test Diagram for Video Extractor App

**CONCLUSIONS**

This paper presented a novel approach for video steganography using LSB which showcases the possible encrypting and embedding of hidden text into a specific video frame by focusing on enhancing its capacity while preserving video quality. The test results were accomplished by strategically employing LSB manipulation in the blue channel and limiting data embedding to every 10th frame, a method that not only improved data security but also maintained a high level of computational efficiency. The system is capable of embedding up to 500 KB of data in a minute-long 1080p video without losing quality. The developed Video Text Extractor application, incorporating Tesseract OCR and AES decryption, showed high efficiency and accuracy in extracting and decrypting hidden data. Despite its success, the research also highlighted challenges, particularly the vulnerability and susceptibility of LSB techniques to lossy compression and data loss under high compression levels which still may be exposed to other forms of steganalysis [5]. These insights pave the way for future research, especially in developing adaptive LSB methods and enhancing robustness against compression, thus refining the balance between data security, embedding capacity, and computational efficiency in video steganography.

**ACKNOWLEDGEMENTS**

My sincere appreciation to my supervisor Assoc Prof. Ts Dr Asif Iqbal and evaluator Dr. Mir for all of their help, advice, and helpful recommendations with unwavering support in making this study. Additionally, I want to express my gratitude to the faculty member of Management & Science University for their inspiration and assistance. Additionally, I would like to express my gratitude to the authors of the studies and articles that have been cited in this project because their work has been a tremendous aid in understanding the theories and methods underlying video steganography using the LSB (Least Significant Bit) technique.

**REFERENCES**

[1] Anderson, Ross & Petitcolas, Fabien. (1998). On The Limits of Steganography. IEEE Journal on Selected Areas in Communications. 16. 474-481. 10.1109/49.668971.

[2] Kunhoth, J., Subramanian, N., Al-Maadeed, S. *et al.* Video steganography: recent advances and challenges. *Multimed Tools Appl* **82**, 41943–41985 (2023). https://doi.org/10.1007/s11042-023-14844-w

[3] Khater, Abdullah & Al-Ma'adeed, Somaya & Ahmed, Abdulghani & Sadiq, Ali & Khan, Khurram. (2020). Comprehensive Review of Cybercrime Detection Techniques. IEEE Access. PP. 1-1. 10.1109/ACCESS.2020.3011259.

[4] Patel, R., Lad, K., Patel, M., & Desai, M. (2021). An efficient DCT-SBPM based video steganography in compressed domain. International Journal of Information Technology, 13, 1073 - 1078. <https://doi.org/10.1007/s41870-021-00648-4>.

[5] Reddy, V., Subramanyam, A., & Reddy, P. (2012). Implementation of Least Significant Bit Steganography and Statistical Steganalysis. , 671-675. https://doi.org/10.1145/2393216.2393328.