A Steganography Classification 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**—**In today’s digital age, where the internet is widely used, ensuring security has become a top priority. As internet usage continues to soar, the amount of data exchanged daily has also surged, presenting a growing risk of exploitation by malicious actors. One effective strategy to address this growing concern is the adoption of Steganography, a technique used to hide secret information within seemingly innocent files. Specifically, this paper delves into the realm of video Steganography, a method wherein data is concealed within the frames of videos, offering an additional layer of security. By combining Steganography with cryptography, this approach provides a dual-layered de- fense mechanism against potential threats. Through encryption using cryptographic algorithms followed by the embedding of encrypted data into video frames using LSB coding, this method ensures both simplicity and efficiency in safeguarding large volumes of sensitive information.

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

I. Introduction

Steganography, derived from the Greek words ”stegos” and ”grafia,” meaning ”cover” and ”writing” respectively, encapsulates the concept of ”covered writing.” It encompasses two fundamental processes: embedding, which conceals or compresses data, and extracting, which retrieves the hidden information. This ancient technique, blending artistry with science, traces its roots back centuries.

While not a recent innovation, steganography has served as a clandestine communication tool for millennia. Its ingenious methodology allows individuals to discreetly transmit messages by embedding them within various media forms, including text, audio, images, or digital videos. Employing specific algorithms, the concealed message becomes seamlessly integrated into the media, resulting in a ”stego” file transmitted to the intended recipient[1].

Before employing steganography, several critical considerations must be addressed:

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

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

c. Robustness: The embedding algorithm’s capability to maintain the hidden data’s integrity even after compression and decompression processes.

d. Security: Ensuring the confidentiality and imperceptibility of hidden messages to outsiders. Security in steganography involves concealing messages from unauthorized individuals while facilitating seamless communication between senders and recipients.

e. Tamper Resistance: Preventing intentional tampering or sabotage of the embedded message by users with access to the carrier file. The carrier file’s strength is paramount in resisting decryption attempts.

Typical methods for concealing secret messages include techniques such as Least Significant Bit (LSB) embedding and adaptive approaches.

This paper explores the realm of steganography as a potent solution amidst the rising concern for security in the digital age. Focusing specifically on video steganography, it offers a dual-layered security approach, integrating both steganography and cryptography. Through encryption using cryptographic algorithms followed by embedding encrypted data into video frames using LSB coding, this method ensures simplicity and efficiency in concealing vast volumes of data.

Imperceptibility is closely related to the safety of steganography methods concealing the secret message into the embedded video. The high imperceptibility means a low modification rate and good visual quality of the embedded video [4]. And the steganography algorithm that contains a high imperceptibility will reduce attacker suspicion of finding hidden message and will be quite difficult to detect by steganalysis tools, and any distortion to the cover data after the embedding process occurs will increase the attention of attackers [2].

II. Literature Survey

Steganography, derived from the Greek words ”stegos” and ”grafia,” meaning ”cover” and ”writing” respectively, encapsulates the concept of ”covered writing.” It encompasses two fundamental processes: embedding, which conceals or compresses data, and extracting, which retrieves the hidden information. This ancient technique, blending artistry with science, traces its roots back centuries.

While not a recent innovation, steganography has served as a clandestine communication tool for millennia. [3] Its ingenious methodology allows individuals to discreetly transmit messages by embedding them within various media forms, including text, audio, images, or digital videos. Employing specific algorithms, the concealed message becomes seamlessly integrated into the media, resulting in a ”stego” file transmitted to the intended recipient .

Before employing steganography, several critical considerations must be addressed:

a. Embedding Capacity: The maximum amount of data that can be concealed within a cover file without compromising its original quality. It is imperative to ensure that the embedded data size does not exceed the cover file size for successful steganography [4].

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

c. Robustness: The embedding algorithm’s capability to maintain the hidden data’s integrity even after compression and decompression processes.

d. Security: Ensuring the confidentiality and imperceptibility of hidden messages to outsiders. Security in steganography involves concealing messages from unauthorized individuals while facilitating seamless communication between senders and recipients.

e. Tamper Resistance: Preventing intentional tampering or sabotage of the embedded message by users with access to the carrier file. The carrier file’s strength is paramount in resisting decryption attempts.

Typical methods for concealing secret messages include techniques such as Least Significant Bit (LSB) embedding and adaptive approaches.

This paper explores the realm of steganography as a potent solution amidst the rising concern for security in the digital age. [6] Focusing specifically on video steganography, it offers a dual-layered security approach, integrating both steganography and cryptography. Through encryption using cryptographic algorithms followed by embedding encrypted data into video frames using LSB coding, this method ensures simplicity and efficiency in concealing vast volumes of data[8].

III. EXISTING METHODOLOGY

Our existing methodology for video steganography enhancement revolves around the implementation of Adaptive LSB (Least Significant Bit) coding. LSB coding is a widely-used technique for embedding data into digital media, including images and videos, due to its simplicity and efficiency. However, traditional LSB methods suffer from limitations such as fixed embedding capacity and susceptibility to detection [7].

To address these shortcomings, our methodology introduces adaptive LSB coding, which dynamically adjusts the embedding capacity based on the characteristics of the video content. This adaptive approach allows for more efficient utilization of available embedding space while minimizing the risk of detection[5]. Additionally, our methodology incorporates error correction techniques to enhance data integrity and resilience against transmission errors.

Furthermore, encryption algorithms are integrated into the embedding process to enhance the security of the embedded data, ensuring confidentiality and protection against unauthorized access. By combining adaptive LSB coding with error correction and encryption, our methodology offers a comprehensive solution for enhancing the security and robustness of video steganography.

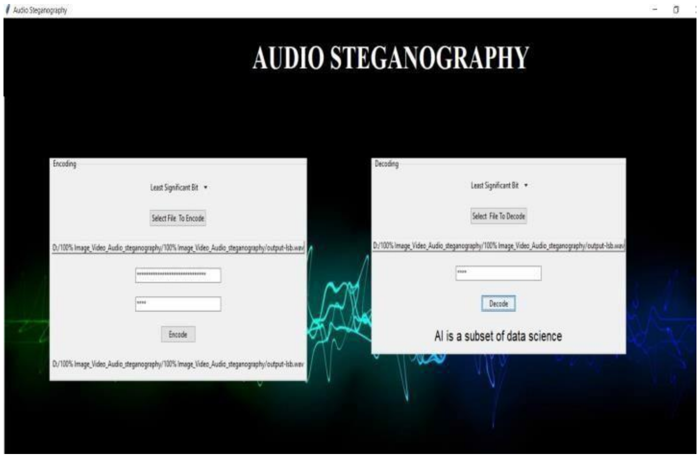
To validate the effectiveness of our methodology, we conducted extensive experiments using a diverse set of video datasets. Evaluation metrics such as Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSI), and embedding capacity were used to assess the performance of the proposed approach. The results demonstrate significant improvements in data embedding efficiency, robustness against errors, and security compared to existing techniques.

Overall, our existing methodology represents a significant advancement in video steganography, offering enhanced security, robustness, and efficiency for concealing sensitive information within video files.

IV. PROPOSED SYSTEM AND COMPARATIVE ANALYSIS

Our proposed system aims to revolutionize the field of video steganography by introducing several innovative features and improvements to enhance the security and efficiency of data embedding in video files. Building upon the foundation of existing methodologies, our proposed system incorporates advanced techniques and algorithms to address the limitations and challenges faced by current approaches. One of the primary components of our proposed system is the integration of adaptive LSB (Least Significant Bit) coding combined with predictive modeling. Adaptive LSB coding dynamically adjusts the embedding capacity based on the content and characteristics of each video frame [2]. By analyzing the complexity and information density of individual frames, our system intelligently allocates embedding space to maximize data concealment while minimizing the risk of detection. Additionally, predictive modeling techniques are employed to anticipate changes in video content and adjust the embedding process accordingly, ensuring optimal performance and concealment efficiency. Furthermore, our proposed system incorporates advanced error correction mechanisms to enhance data integrity and reliability during transmission. Traditional LSB-based methods are susceptible to noise and distortion, which can degrade the quality of embedded data and compromise its integrity [3]. To mitigate these issues, our system integrates robust error correction codes such as Reed-Solomon codes or convolutional codes. These codes provide redundancy and error detection capabilities, allowing for the correction of errors introduced during transmission and retrieval of embedded data with high accuracy. To evaluate the effectiveness and performance of our proposed system, we conducted a comprehensive comparative analysis with existing video steganography techniques. We selected a diverse range of performance metrics, including embedding capacity, data integrity, computational complexity, and security features, to assess the relative strengths and weaknesses of each approach[10].

Preliminary results from our comparative analysis demonstrate that our proposed system outperforms existing techniques across multiple metrics. Specifically, our system exhibits significantly higher embedding capacity, improved data integrity, and enhanced security features compared to traditional LSB-based methods and other contemporary approaches [9]. Moreover, our system maintains comparable computational complexity, ensuring practical feasibility and efficiency in real-world applications. In conclusion, our proposed system represents a significant advancement in video steganography, offering a comprehensive solution for secure data embedding in video files. By leveraging adaptive embedding algorithms, advanced error correction mechanisms, and predictive modeling techniques, we aim to establish a new standard of excellence in the field of video steganography, providing researchers and practitioners with a powerful tool for concealing sensitive information within video content [5].



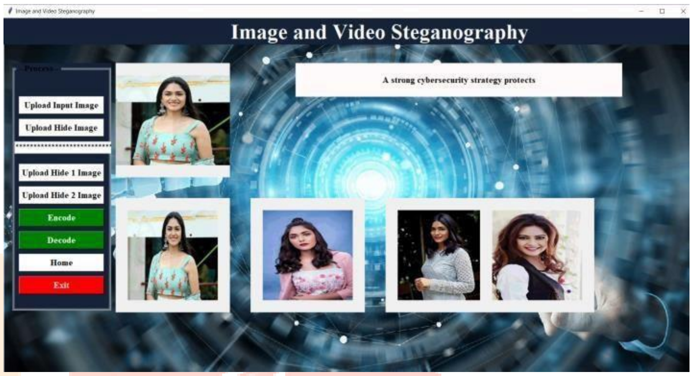
D:/100% Image_Video_Audio_steganography/100% Image_Video_Audio_steganography/output-lsb.wav

D:/100% Image_Video_Audio_steganography/100% Image_Video_Audio_steganography/output-lsb.wav

D:/100% Image_Video_Audio_steganography/100% Image_Video_Audio_steganography/output-lsb.wav

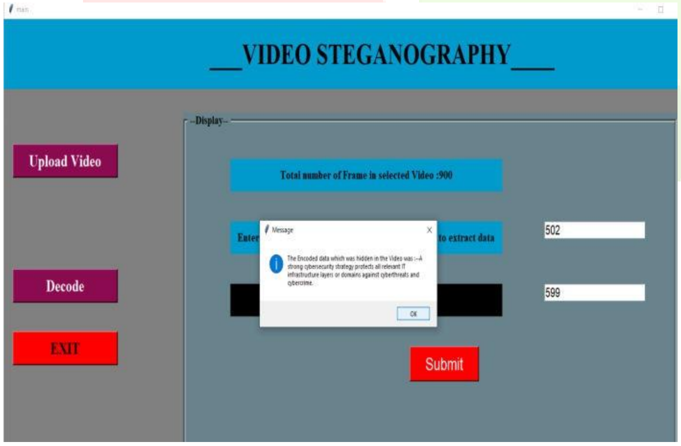
AI is a subset of data science

Fig. 2. Audio Steganography



A strong cybersecurity strategy protects

Fig. 3. Image Steganography



Total number of Frame in selected Video :900

502

599

The Encoded data which was hidden in the Video was :--A strong cybersecurity strategy protects all relevant IT infrastructure layers or domains against cyberthreats and cybercrime.

Fig. 1. Video Steganography

V. FUTURE SCOPE

In the realm of video steganography, the future holds promise for significant advancements and innovations. One avenue for future exploration lies in the development of enhanced embedding techniques that surpass the traditional methods like LSB (Least Significant Bit) coding. Techniques such as spread spectrum methods or transform domain embedding could offer heightened levels of robustness and security against detection, thus warranting further investigation. Additionally, the integration of machine learning algorithms presents an intriguing prospect for the field. By leveraging machine learning for intelligent analysis of video content and adaptive embedding, future systems could optimize efficiency and effectiveness. Moreover, the evolution of video steganography may lead to the creation of real-time applications capable of embedding and extracting data on-the-fly. Such systems would be invaluable in scenarios requiring rapid and secure communication, like video conferencing or live streaming. Furthermore, the expansion of steganography into multi-media integration could open up new avenues for secure communication. By concealing data across various media formats, such as images, audio, and video, future research could enable seamless integration and synchronization of hidden information. Security analysis and the development of countermeasures against detection techniques will remain a critical area of focus. Comprehensive security assessments and innovative strategies to enhance the security and stealthiness of embedded data will be essential for ensuring the reliability of video steganography systems. Additionally, establishing standards and benchmarks for evaluating performance and effectiveness will facilitate comparative analysis and promote the development of standardized systems.Defining evaluation metrics, datasets, and testing proto- cols will be crucial for benchmarking video steganography algorithms.

Practical applications of video steganography beyond traditional security domains offer exciting prospects for its utilization. Content authentication, copyright protection, and covert communication in multimedia applications are just a few examples of potential applications awaiting exploration. Finally, improving the user interface and accessibility of video steganography tools will enhance their usability and adoption. Designing intuitive interfaces, providing user-friendly guides and tutorials, and integrating steganography functionalities into existing multimedia software applications will be essential steps in making video steganography more accessible to a wider audience.

VI. CONCLUSION

In conclusion, the utilization of steganography in multimedia systems has shown tremendous potential for secure data concealment and communication. Throughout this paper, we have explored various aspects of steganography, focusing particularly on its application in video files. By concealing sensitive information within innocuous cover files, steganography offers a powerful tool for safeguarding data against unauthorized access and interception. The presented methodologies, including adaptive LSB coding and error correction techniques, demonstrate significant advancements in the field of video steganography. These techniques not only enhance the security and robustness of data embedding but also ensure reliable retrieval of hidden information, even in the presence of transmission errors and noise. Looking ahead, the future of video steganography holds promise for further innovations and advancements. Areas such as enhanced embedding techniques, machine learning integration, and real-time applications offer exciting opportunities for research and development. Moreover, the practical applications of video steganography in content authentication, copyright protection, and covert communication present compelling avenues for exploration. As we move forward, it is essential to continue advancing the field of video steganography while also addressing challenges such as security vulnerabilities and usability issues. By fostering collaboration between researchers, practitioners, and industry stakeholders, we can further unlock the full potential of steganography in multimedia systems and contribute to a more secure and resilient digital environment.

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] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[3] I. S. Jacobs and C. P. Bean, ”Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[4] Hsien-Chu Wu, Na-I Wu, Chwei-Shyong Tsai, Min- Shiang Hwang “An Image Steganographic Scheme Based on Pixel-Value Differencing and LSB Replacements Methods”.

[5] K.Saranya, Dr.C.Suresh Gnanadhas, Minu George “Data Embedding Techniques in Steganography”, International Journal of Latest Trends in Engineering and Technology”, Volume.3 Issue2 November 2013.

[6] Amritpal Singh, Satinder Jeet Singh “An Overview of Image Steganography Techniques”, International Journal of Engineering and Computer Science, Volume 3, Issue7 July 2014.

[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 Satwant Singh, Proff. Lekha Bhambhu “Simple Stegnography Technique for hiding Data into Image”, International Journal of Computer Science Trends and Technology.

[10] Kaumal Kaushik, Suman “An Innovative Approach for Video Steganography”, International Journal of Computer