Perceptions of Video Steganography Techniques for Secure Communication

Dr Umadevi R[1], Dr Vishal Jain[2]
[1]Post Doctoral Research Fellow, Department of Computer Science and Engineering, Lincoln University College, Malaysia. ;
[2] Department of Computer Science and Engineering, School of Engineering and Technology, Sharda University, Greater Noida, U.P. India.
mail2deviuma@gmail.com

Abstract: Video steganography is a technique for embedding secret data within video files to ensure secure communication. With the increasing demand for data security in multimedia applications, video steganography has gained significant attention due to its high capacity and perceptual transparency. This paper presents a wide-ranging review of current developments, trends, and challenges in video steganography. This review aims to analyses various embedding techniques, including spatial-domain, transform-domain, and motion-based approaches, along with their robustness, security, and payload capacity. Additionally, discuss emerging trends such as deep learning-based steganography and hybrid methods.

Keywords: Video Steganography; Data Hiding; Covert Communication; Deep Learning; Information Security; Secure Communication

---

Introduction

The rapid growth of digital communication has increased the need for secure data transmission. Steganography, the art of concealing information within cover media, provides an effective solution. Video steganography, in particular, offers advantages over image steganography due to its larger data capacity and temporal redundancy [1]. Recent advancements in machine learning and video compression techniques have introduced new opportunities and challenges in this field. This paper reviews state-of-the-art video steganography techniques, evaluates their strengths and limitations, and discusses its methodologies.

Steganography vs. Cryptography

It is important to differentiate steganography from cryptography. While cryptography encrypts data to render it unreadable, steganography's primary goal is to hide the very existence of the data. Combining both techniques can significantly enhance overall security.

Video Steganography Framework

A typical video steganography system operates through a structured framework that includes three main components. The embedding process involves inserting the secret data directly into the video frames, effectively concealing the information within the visual content. At the receiver's end, the extraction process is used to recover the hidden data from the modified video frames. To maintain confidentiality and ensure that only authorized parties can access the concealed information, key management plays a critical role by securely handling the keys required for both embedding and extraction.

Classification of Video Steganography Techniques

Video steganography techniques can be broadly classified based on their embedding approach, each offering distinct advantages in terms of robustness, capacity, and adaptability. Spatial domain techniques involve embedding data directly into the pixel values of video frames, with the Least Significant Bit (LSB) modification being a common method. In this approach, secret data replaces the least significant bits of pixel values, and recent research has focused on enhancing its robustness through adaptive embedding strategies. Transform domain techniques, on the other hand, embed data within the coefficients of transformed video frames, providing greater resilience against compression attacks. Popular transforms used in this domain include Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and methods leveraging High-Efficiency Video Coding (HEVC).

Performance Metrics

The effectiveness and quality of video steganography techniques are evaluated using several key performance metrics payload capacities that refers to the maximum amount of data that can be embedded within a video file. Imperceptibility measures how undetectable the hidden data is to human perception and is often quantified using metrics like PSNR (Peak Signal-to-Noise Ratio) and SSIM (Structural Similarity Index Measure), Robustness factor that indicates the technique's resistance to various attacks, such as compression, filtering, and noise addition, Security metric assesses the technique's resistance to steganalysis, which are methods designed to detect the presence of hidden data.

Recent Trends and Advancements

The field of video steganography is continuously evolving with new trends and advancements such as hybrid Steganography is the approach involves combining multiple embedding techniques (e.g., DWT + LSB) to achieve improved security and robustness, AI-Driven Steganalysis Resistance that

leveraging adversarial learning, researchers are developing methods to help steganography evade detection by advanced steganalysis tools, Real-Time Video Steganography is the emergence of efficient algorithms is enabling live streaming and IoT applications to incorporate real-time data hiding.

Challenges and Issues

Despite significant progress, several challenges and open issues remain in video steganography such as detection resistance for the development of advanced steganalysis tools, particularly those based on deep learning, poses a constant threat to hidden data detection, format compatibility that ensuring that steganographic methods remain compatible with modern video codecs like AV1 and VVC is a continuous challenge, computational complexity that Balancing the need for high security with the demand for real-time performance introduces a complex trade-off, ethical and legal concerns that the potential misuse of video steganography in cybercrime necessitates the establishment of appropriate regulatory frameworks.

Related work

Various well-organized data hiding algorithms are designed for video steganography. Motion features-based approach is a type of steganographic algorithm with video coding crafts. In most of the techniques, the selection of features on identified video quality are based on the blurring and blocking results without variance and intensity of temporal changes in irreversible video steganography. The generic data hiding methods and dissimilar Steganography types are examined. In this paper, a survey on video steganography systems is presented and different video steganography models are discussed. An important enhancement in computer systems has resulted in the introduction of new technologies for video steganography. In this study, their applications are thoroughly addressed with the help of literature to identify specific models.

Table 1. Comparison of Video Steganography Techniques

Category/Method	Embedding Domain/Mechanism	Advantages	Disadvantages/Limitations
General Video Steganography	Embedding secret data within video files for secure communication. Exploits high capacity and temporal redundancy.	High capacity, perceptual transparency.	Trade-off between security, robustness, and hiding capacity.
Spatial Domain: LSB-based	Directly modifies pixel values, typically the Least Significant Bit (LSB). Many variants (1-LSB, 4-LSB, HASH LSB, adaptive).	Simple, effective, quick. Relatively high capacity.	Low robustness against attacks (compression, noise). Prone to steganalysis. PSNR decreases significantly with increased capacity. Significant visual degradation with 4-LSB.
Spatial Domain: Others	K-means clustering + LBP features. CB component utilization. Regional histogram optimization. Luminance component (lossless). Average histogram values. Random RGB components.	Improved imperceptibility over LSB-based. Some show robustness against H.264/AVC compression.	Robustness is a concern; many methods lack quantitative analysis. Security not verified for many [337, Table 2]. Computational expense for adaptive skin detection.
Transform Domain: DWT-based	Embeds data in transformed coefficients (e.g., LL, HL, HH, LH sub bands). Often combines with LSB, encryption, or ECC. Adaptive methods use motion analysis, object tracking, skin tone detection.	Better robustness against compression compared to spatial domain. Improved security with encryption/ECC.	Can be computationally expensive. Reducing embedding capacity with multiple DWT levels. Robustness not always quantified for all attacks.

Transform Domain: DCT-based	Embeds data in DCT coefficients (e.g., 4x4 luminance blocks). Addresses intra-frame distortion drift using compensating coefficients, prediction directions, or STC.	Higher frequency resolution than DWT. Good robustness against noise attacks. Improved security with encryption/ECC.	Not as frequently used in raw video domain compared to DWT. Can have less hiding capacity without optimization. Steganalytic security not always tested [367, Table 3].
Compressed Domain: Intra Prediction Modes	Maps secret data bits to intra-prediction modes (e.g., 4x4, 16x16 blocks in H.264/AVC; 35 modes in HEVC). Uses matrix coding or STC for adaptive selection of complex textures.	Low complexity. Can achieve minimal embedding distortion [397, Table 4].	Usually only applicable to I-frames. Security not always tested [397, Table 4].
High-Security HEVC MV Steganography (MVP Index & MVD)	Embeds in MVP's index and Motion Vector Difference (MVD) in HEVC. Designs distortion function to maintain MVP optimality. Combines with STC codes.	Resists MVPO steganalysis (100% MVP optimality), unlike other mainstream methods. High security against traditional steganalysis (e.g., AoSO, NPELO, LOCL, VSRNet). High visual quality with minimal degradation.	Lower embedding capacity if only PUs satisfying optimality are chosen. Slight bitrate growth due to twice compression.

The table 1 shows the various steganography methods and techniques that are discussed with its merits and demerits. The arena of video steganography has seen important developments, particularly in the context of secure communication within IoT networks and resilience against modern compression standards. The author explored [1] secure video steganography tailored for IoT environments, emphasizing the need for lightweight and robust techniques suitable for constrained devices. The author

laid the foundational principles of steganography in digital media, offering a comprehensive theoretical framework that continues to guide contemporary research [2]. Building on spatial domain methods, Author proposed [3] an adaptive Least Significant Bit (LSB) technique that enhances robustness by dynamically adjusting embedding based on video content characteristics.

In the transform domain, authors introduced [4] a DWT-based video hiding method that demonstrates strong resistance to H.264/AVC compression, while combining DWT and LSB approaches to create a hybrid model that balances imperceptibility and security [7]. Motion-based techniques have also gained traction, with authors presenting an optimized motion vector steganography method specifically designed for HEVC, significantly improving payload capacity [5]. Deep learning has further revolutionized the field; authors developed a CNN-based model that achieves undetectable embedding [6], and authors leveraged Generative Adversarial Networks (GANs) to counter steganalysis, enhancing the stealth of hidden data [8].

Authors focused on real-time steganography for IoT applications, addressing latency and computational efficiency [9]. Moreover, authors proposed a chaos-based encryption technique for compressed H.264/AVC videos, adding a layer of cryptographic security to steganographic systems [10]. Authors introduced a novel method for hiding data within thumbnail videos using adaptive down sampling, offering resilience against resolution changes and further expanding the versatility of video steganography [11]. Collectively, these studies highlight a dynamic and evolving landscape, where traditional methods are being enhanced by adaptive algorithms and AI-driven models to meet the demands of modern multimedia security.

The author provided a study of video steganography methods, classifying them into raw domain and compressed domain approaches. Raw domain techniques include spatial methods like Least Significant Bit (LSB) substitution and transform domain methods such as Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) [12].

Authors proposed a high-security steganographic method tailored for HEVC (High Efficiency Video Coding) videos. Their approach utilizes the Motion Vector Prediction Index and Motion Vector Difference to embed secret data while preserving the local optimality of motion vectors—a key feature exploited by steganalysis techniques. By designing a distortion-minimizing embedding algorithm, the method achieves high imperceptibility and coding efficiency, making it suitable for practical covert communication scenarios [13].

In parallel, authors addressed the security of medical image transmission through a novel Colour Secret Sharing Protocol (CSSP). This protocol enhances visual cryptography by dividing secret colour images into shares, which are later recombined to reconstruct the original image. CSSP improves image quality, reduces pixel expansion, and lowers computational complexity, making it ideal for healthcare applications where confidentiality and image fidelity are critical. Validated using MATLAB, the protocol shows measurable improvements over existing methods, reinforcing the importance of secure multimedia transmission in sensitive domains like telemedicine and electronic health records [14].

Key Contribution

In spite of important developments in video steganography, several critical research gaps remain that limit its practical implementation and effectiveness. One major challenge is the lack of robustness against modern steganalysis techniques, particularly those employing deep learning, which can sense hidden data with increasing accuracy. Many existing methods also struggle to maintain security and imperceptibility when videos undergo compression or transcoding. Another significant gap lies in real-time performance, as most current algorithms are computationally intensive and unable to handle high-resolution videos or live streaming efficiently.

The field also lacks standardized benchmarks and diverse datasets, making fair evaluation and comparison of different techniques difficult. Additionally, while spatial-domain methods are well-studied, temporal-domain techniques that can withstand frame-dropping or other temporal manipulations remain underdeveloped. Modern video codecs like H.265/HEVC present new challenges, as traditional embedding methods often fail to adapt to their advanced compression mechanisms. Furthermore, the ethical implications of steganography, particularly its potential misuse, have not been sufficiently addressed, nor have effective countermeasures been thoroughly explored. Addressing these gaps requires innovative approaches that balance embedding capacity, security**,** and computational efficiency while adapting to evolving video technologies and threat models. Future research should focus on developing adaptive, AI-driven techniques that can operate in real-time, resist advanced detection methods, and comply with emerging ethical and legal standards.

Motivation of the Research

The rising need for secure and covert communication in the digital age has driven significant interest in video steganography, a technique that hides sensitive data within video files without fascinating attention. Unlike encryption, which protects data but reveals its existence, steganography conceals the very presence of secret information, making it invaluable for military, intelligence, and corporate applications where confidentiality is paramount. Videos are particularly advantageous for steganography due to their large storage capacity, temporal redundancy, and complex structure, allowing more data to be embedded compared to images or audio files. Additionally, the widespread use of video streaming and social media platforms presents opportunities for real-time covert communication, digital watermarking, and copyright protection. However, with advancements in machine learning-based steganalysis, researchers must continuously develop more robust and undetectable embedding techniques to stay ahead of detection methods. Furthermore, video steganography has applications in bypassing censorship in restricted networks, enabling secure data transmission for journalists and activists in oppressive rules. The field also intersects with digital forensics, where law enforcement agencies work to detect hidden malicious content, while cybersecurity experts refine steganographic methods to prevent data breaches. As cyber threats evolve, research in video steganography remains serious to ensure secure, high-capacity, and resilient data hiding solutions for the future.

Conclusion

Video steganography has occurred as a powerful tool for secure data communication, leveraging the high capacity and inherent complexity of video files to conceal information efficiently. This paper has provided a comprehensive review of the modern improvements, methodologies, and challenges in the field, highlighting key developments in spatial-domain, transform-domain, and motion-based embedding techniques. Each approach offers distinct advantages in terms of robustness, security, and payload capacity, yet trade-offs persist between imperceptibility and resistance to detection. Recent trends, particularly deep learning-based and hybrid steganography methods, show promise in enhancing adaptive embedding strategies and evading advanced steganalysis. However, significant challenges remain, including the need for real-time processing in streaming applications, compatibility with modern video compression standards (e.g., H.265/HEVC, AV1)

References

1. K. Muhammad et al., "Secure Video Steganography in IoT Networks," IEEE Transactions on Multimedia, 2022.
2. J. Fridrich, Steganography in Digital Media, Cambridge Univ. Press, 2010.
3. Y. Liu et al., "Adaptive LSB for Video Steganography," Elsevier J. of Information Security, 2021.
4. H. Wang et al., "DWT-Based Robust Video Hiding," Springer Multimedia Tools and Applications, 2023.
5. S. Kumar et al., "HEVC Motion Vector Steganography," IEEE Access, 2022.
6. L. Zhang et al., "CNN-Based Video Steganography," IEEE Transactions on Dependable and Secure Computing, 2023.
7. M. Ali et al., "Hybrid DWT-LSB for Secure Videos," Elsevier Computers & Security, 2022.
8. R. Balu et al., "GANs for Anti-Steganalysis," IEEE ICCV Workshops, 2023.
9. T. Nguyen et al., "Real-Time Steganography for IoT," Springer IoT Journal, 2023.
10. El-Mowafy, M. A., et al. "Chaos Based Encryption Technique for Compressed H264/AVC Videos." IEEE Access, vol. 10, 2022, pp. 124002–124016, doi:10.1109/ACCESS.2022.3223445.
11. Wang, Yongzhi. "Hiding Data Within Thumbnail Videos: An Adaptive Down sampling - Resilient Video Steganography Method." IEEE Access, vol. 12, 2024, pp. 52963–52976, doi:10.1109/ACCESS.2024.3386798.
12. Ayakanth Kunhoth, Nandhini Subramanian, Somaya Al -Maadeed, Ahmed Bouridane," Video steganography: recent advances and challenges", Multimedia Tools and Applications (2023) 82:41943–41985 https://doi.org/10.1007/s11042-023-14844-w.
13. Jun Li, Minqing Zhang, Ke Niu, Yingnan Zhang, Yan Ke, and Xiaoyuan Yang "High-Security HEVC Video Steganography Method Using the Motion Vector Prediction Index and Motion Vector Difference", Tsinghua Science and Technology, ISSN 1007 0214, 25 / 32, pp 813−829. Volume 30, Number 2, April 2025. DOI:10.26599/TST.2024.9010016.
14. Suresh Sankaranarayanan, (Senior Member, IEEE), Prema Bhushan Sahane, Maheshwari Divate, A. John blesswin, (Member, IEEE), G. Selva Mary, (Member, IEEE), A. Catherine Esther Karunya, and Pascal Lorenz, (Senior Member, IEEE), "Enhancing Healthcare Imaging Security: Color Secret Sharing Protocol for the Secure Transmission of Medical Images", IEEE Access, Volume 12, 2024, Digital Object Identifier 10.1109/ACCESS.2024.3426935.