Video Steganography for Cybersecurity Applications: A Systematic Review of Classical, Hybrid, and AI-Driven Techniques

Anamika Saini*, Kavita Rathi

Department of Computer Science and Engineering, Deen Bandhu Chhotu Ram University of Science & Technology, Sonipat, Haryana, India

***Corresponding Author**

DOI: https://dx.doi.org/10.51244/IJRSI.2026.1306000106

Received: 05 June 2026; Accepted: 10 June 2026; Published: 25 June 2026

ABSTRACT

The rapid growth of digital communication, cloud computing, Internet of Things (IoT), and intelligent surveillance systems has increased the demand for secure and covert information exchange. Video steganography has emerged as an effective information-hiding technique that enables confidential data transmission while concealing the existence of communication. Compared with im-age-based approaches, video steganography offers higher embedding capacity and improved imperceptibility due to the availability of multiple frames and temporal redundancy.

This paper presents a systematic review of video steganography techniques for cybersecurity applications. Existing approaches are categorized into classical spatial-domain methods, transform-domain techniques, hybrid models, and re-cent Artificial Intelligence (AI)-driven approaches. Major techniques including Least Significant Bit (LSB), Discrete Cosine Transform (DCT), Discrete Wave-let Transform (DWT), Random Pixel Selection (RPS), Huffman coding-based embedding, and deep learning-based methods are analyzed and compared. The review also examines commonly used benchmark datasets and performance metrics such as Peak Signal-to-Noise Ratio (PSNR), Mean Square Error (MSE), Root Mean Square Error (RMSE), embedding capacity, and robustness.

Furthermore, the study discusses applications in cybersecurity, healthcare, military communication, cloud environments, and smart surveillance systems. Key challenges and emerging research directions, including AI-assisted adaptive embedding, blockchain-enabled security, and quantum-resilient steganography, are highlighted. The review indicates that hybrid and AI-driven techniques provide improved security and robustness, making them promising solutions for next-generation secure multimedia communication systems.

Keywords: Video Steganography, Cybersecurity, Information Hiding, Multimedia Security, Deep Learning, Artificial Intelligence.

INTRODUCTION

The widespread adoption of digital technologies has transformed the way multimedia information is generated, transmitted, and stored. Videos have become one of the most dominant forms of digital content due to their extensive use in online communication, social media platforms, smart surveillance systems, healthcare services, military operations, and cloud-based applications. While these advancements have improved accessibility and connectivity, they have also increased concerns related to data confidentiality, unauthorized access, cyber espionage, and multimedia tampering [10], [7].

Conventional security mechanisms such as cryptography protect the content of a message by converting it into an unreadable format. However, the presence of encrypted communication may itself attract attention from potential attackers. Steganography addresses this limitation by concealing secret information within a digital carrier, thereby hiding the existence of communication. Depending on the carrier medium, steganography can be classified into text, image, audio, and video steganography [1], [8].

Among these categories, video steganography has gained significant research interest because videos contain a large number of frames and substantial temporal redundancy, enabling higher embedding capacity and improved imperceptibility compared with imagebased approaches [16]. Over the years, researchers have proposed a wide range of techniques, including spatial-domain methods, transform-domain approaches, hybrid embedding schemes, and more recently, Artificial Intelligence (AI)-based frameworks. The emergence of deep learning has further enhanced the capability of steganographic systems by enabling adaptive embedding, intelligent frame selection, and improved resistance to steganalysis attacks [9].

Despite the growing volume of research, existing studies are often fragmented across different embedding domains, performance metrics, datasets, and application areas [2]. Furthermore, the rapid development of AI-driven approaches has created a need for an updated review that systematically analyzes both traditional and modern video steganography techniques from a cybersecurity perspective [12], [7].

This paper presents a systematic review of video steganography techniques and their applications in secure multimedia communication. The study examines classical, hybrid, and AI-driven approaches, compares their strengths and limitations, analyzes commonly used datasets and evaluation metrics, and identifies emerging research trends and future directions for cybersecurity-oriented multimedia protection.

Contributions of This Review

The major contributions of this paper are summarized as follows:

1. A systematic classification of video steganography techniques into classical, hybrid, and AI-driven categories.
2. A comparative analysis of widely used embedding approaches based on security, robustness, visual quality, embedding capacity, and computational complexity.
3. A review of benchmark datasets and performance evaluation metrics used in contemporary video steganography research.
4. An examination of major application domains, including cybersecurity, healthcare, military communication, cloud computing, and intelligent surveil-lance systems.
5. Identification of current research challenges and emerging directions such as AI-assisted embedding, blockchain-enabled security, and quantum-resilient steganographic frameworks.

RESEARCH METHODOLOGY

This systematic review was conducted to identify, analyze, and synthesize existing research on video steganography techniques and their cybersecurity applications. Relevant literature was collected from major scientific databases, including IEEE Xplore, SpringerLink, ScienceDirect, ACM Digital Library, and Google Scholar. The search process utilized keywords such as “video steganography,” “video information hiding,” “deep learning video steganography,” “GAN-based steganography,” “hybrid video steganography,” and “cybersecurity applications of steganography.”

Inclusion Criteria

- Peer-reviewed journal articles and conference papers.
- Studies focused on video steganography techniques.
- Research published in English.
- Studies published between 2015 and 2025.
- Articles reporting performance metrics such as PSNR, MSE, RMSE, embedding capacity, or robustness.

Exclusion Criteria

- Studies exclusively focused on image, audio, or text steganography were excluded from comparative analysis; however, highly cited foundational works were retained where relevant for conceptual background.
- Duplicate publications.
- Non-peer-reviewed articles, editorials, and short abstracts.
- Papers lacking sufficient experimental or methodological details.

Following the screening and eligibility assessment process, the most relevant studies were selected for qualitative analysis and comparative evaluation.

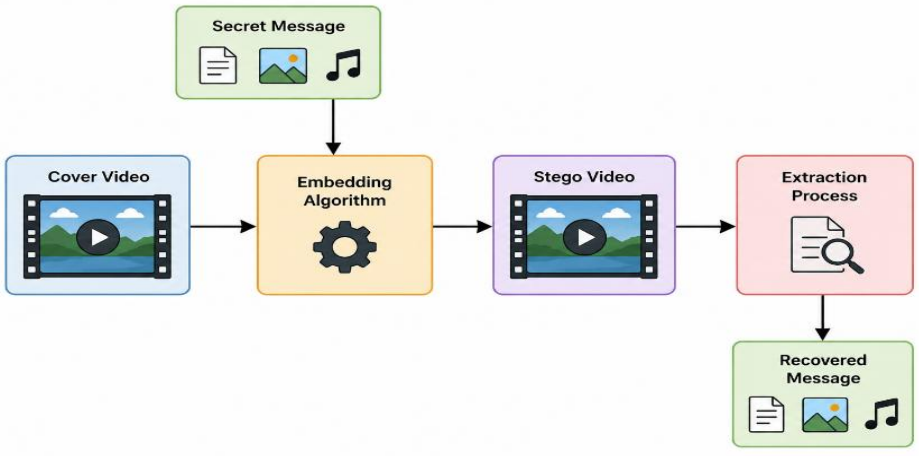
Table 1. The study selection process adopted in this review is illustrated in Table 1.

Sr. No.	Selection Stage	Number of Papers
1.	Records identified through database search	285
2.	After duplicate removal	240
3.	Screened articles	112
4.	Eligible studies	58
5.	Final studies included in review	20

FUNDAMENTALS OF VIDEO STEGANOGRAPHY

Video steganography is a multimedia security technique that conceals secret information within a digital video while preserving its visual quality and minimizing the possibility of detection. The primary objective is to establish covert communication by embedding confidential data into a video stream in such a way that the modifications remain imperceptible to human observers and resistant to steganalysis attacks [9], [10].

A typical video steganography system consists of five major components: the cover video, secret message, embedding algorithm, stego video, and extraction mechanism. The cover video serves as the carrier medium in which confidential information is hidden. Depending on the application requirements, the secret message may contain textual data, images, audio content, encrypted files, authentication credentials, or sensitive medical information [16], [9].



During the embedding phase, a steganographic algorithm selects suitable frames and modifies specific pixel values or transform coefficients to insert the secret information. The resulting output is referred to as the stego

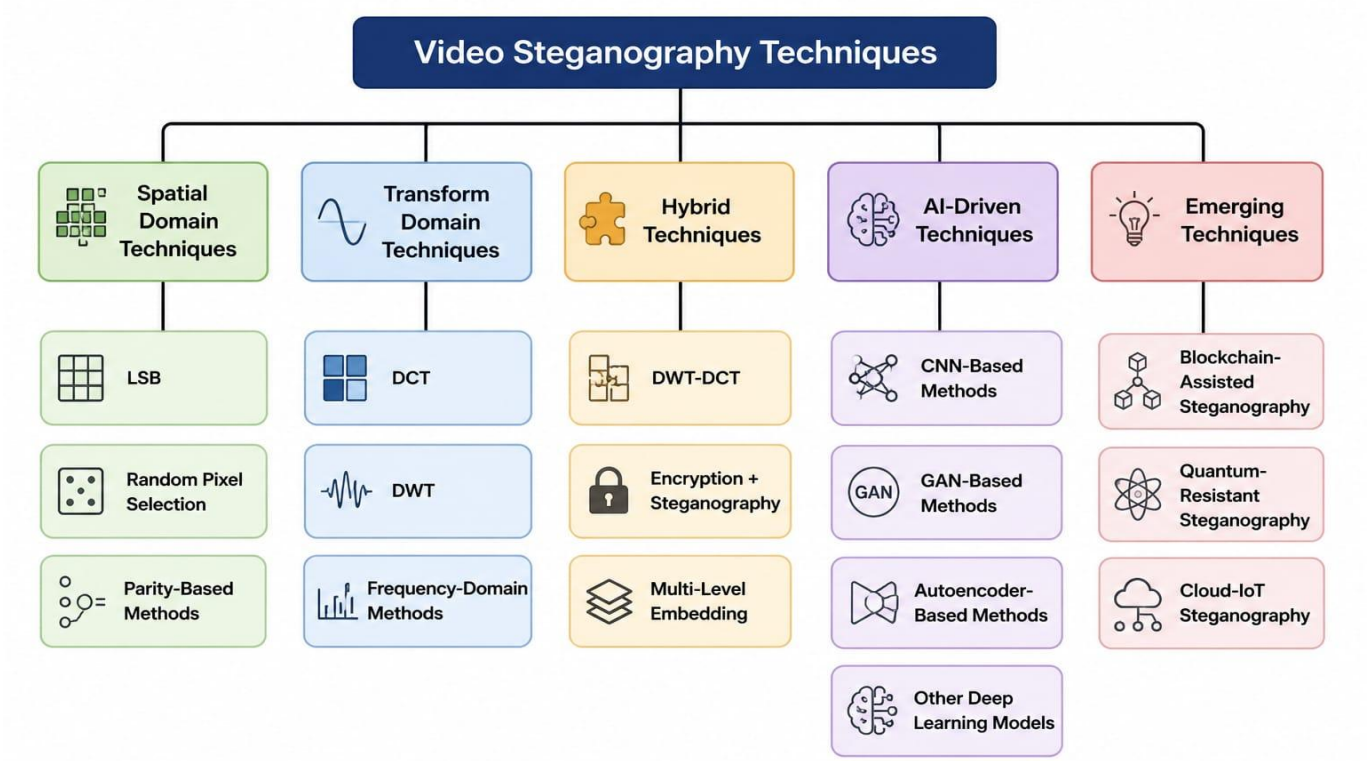
ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

video, which visually resembles the original video while carrying the hidden payload. At the receiver side, the extraction process retrieves the embedded information using the corresponding extraction algorithm and, when applicable, a secret key [8], [10].

The effectiveness of a video steganography system is generally evaluated using several performance criteria, including embedding capacity, imperceptibility, robustness, security, and computational efficiency. An ideal steganographic framework should maximize payload capacity while maintaining high visual quality and strong resistance against compression, noise, frame manipulation, and statistical steganalysis attacks.

CLASSIFICATION OF VIDEO STEGANOGRAPHY TECHNIQUES

Video steganography techniques have evolved significantly over the past two decades, ranging from simple pixel modification methods to sophisticated Artificial Intelligence (AI)-driven frameworks. Based on the embedding strategy and computational characteristics, existing approaches can be broadly categorized into spatial-domain, transform-domain, hybrid, and AI-driven techniques. Each category offers different trade-offs in terms of embedding capacity, imperceptibility, robustness, computational complexity, and resistance to steganalysis attacks. Figure 2 presents the taxonomy of video steganography techniques discussed in this review.



Spatial-Domain Techniques

Spatial-domain techniques represent one of the earliest and most widely used approaches in video steganography. These methods embed secret information directly into the pixel values of selected video frames without transforming the video into another domain. Due to their simplicity, low computational requirements, and high embedding capacity, spatial-domain techniques remain popular in applications where real-time processing and implementation efficiency are important.

The Least Significant Bit (LSB) method is the most commonly adopted spatial-domain technique. In LSB-based embedding, the least significant bits of pixel values are modified to store secret information while producing minimal visual distortion. The method offers high payload capacity and fast execution; however, it is generally vulnerable to statistical steganalysis, compression operations, and image processing attacks [11], [8].

To improve security, researchers have proposed Random Pixel Selection (RPS) techniques, where embedding locations are selected using predefined keys or randomization strategies. By distributing hidden information

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

across different regions of video frames, RPS-based methods increase unpredictability and reduce the likelihood of successful detection by attackers [1].

Parity-based approaches constitute another category of spatial-domain methods. These techniques embed information by manipulating the parity of pixel groups rather than directly altering individual pixel values. Such methods typically provide improved resistance against simple detection mechanisms while maintaining acceptable visual quality [8], [16].

Despite their advantages, spatial-domain techniques generally offer lower robustness against compression, noise addition, frame manipulation, and advanced steganalysis attacks compared with transform-domain and AI-driven approaches. Consequently, they are often employed in applications that prioritize embedding capacity and computational efficiency over long-term robustness.

Transform-Domain Techniques

Transform-domain techniques embed secret information into the frequency components of video frames rather than directly modifying pixel values. These approaches first transform the frame data into a frequency domain and then insert hidden information into selected transform coefficients. As a result, transform-domain methods generally provide improved robustness against compression, noise, filtering operations, and various signal processing attacks.

Among the most widely used transform-domain approaches, the Discrete Cosine Transform (DCT) technique embeds secret data into selected DCT coefficients. Since DCT is extensively utilized in image and video compression standards, including JPEG and MPEG formats, DCT-based steganography offers a suitable balance between imperceptibility and robustness. However, the embedding process is computationally more complex than conventional spatial-domain methods [17].

The Discrete Wavelet Transform (DWT) is another popular technique that decomposes video frames into multiple frequency sub-bands. Secret information can be embedded within specific sub-bands to achieve improved resistance against compression and image processing operations. DWT-based methods are particularly effective in maintaining visual quality while providing enhanced security and robustness [17], [10].

In addition to DCT and DWT, several frequency-domain approaches utilize transform coefficients to optimize embedding locations and reduce perceptual distortion. These methods often exploit the characteristics of human visual perception to conceal information more effectively while preserving the quality of the cover video.

Although transform-domain techniques require greater computational resources than spatial-domain methods, they generally achieve superior robustness and security. Consequently, they are widely employed in multimedia protection, secure communication systems, and cybersecurity applications where resistance to attacks and data integrity are critical requirements [9], [10].

Hybrid Techniques

Hybrid video steganography techniques combine two or more embedding strategies to overcome the limitations of individual methods and achieve improved security, robustness, and embedding performance. By integrating the advantages of different domains, hybrid approaches aim to provide better resistance against attacks while maintaining high visual quality and payload capacity.

One of the most widely adopted hybrid approaches combines Discrete Wavelet Trans-form (DWT) and Discrete Cosine Transform (DCT). In these methods, video frames are first decomposed using DWT, and secret information is subsequently embedded into selected DCT coefficients. The combination of spatial-frequency characteristics enhances robustness against compression, filtering, and signal processing attacks while preserving imperceptibility [17].

Another important category involves the integration of cryptography and steganography. In such systems, the secret message is encrypted before the embedding process. Even if hidden information is detected, encryption

provides an additional layer of protection, thereby strengthening overall communication security. These approaches are particularly useful in military communication, healthcare systems, and cybersecurity applications where data confidentiality is critical [8], [10].
Multi-level embedding techniques further enhance security by distributing hidden information across multiple frames, frequency bands, or embedding layers. This strategy increases the difficulty of unauthorized extraction and improves resistance against steganalysis attacks. Some advanced frameworks also employ adaptive embedding mechanisms that dynamically select embedding locations based on frame characteristics and security requirements [10], [14].

Although hybrid techniques generally require higher computational resources and implementation complexity, they offer a favorable balance between embedding capacity, visual quality, and robustness. As a result, they have become increasingly popular in modern secure multimedia communication systems and cybersecurity-oriented applications.

AI-driven Techniques

The rapid advancement of Artificial Intelligence (AI) and deep learning has significantly transformed the field of video steganography. Unlike traditional approaches that rely on predefined embedding rules, AI-driven techniques can automatically learn optimal embedding and extraction strategies from large datasets. These methods improve security, adaptability, and resistance to steganalysis while maintaining high visual quality.

Convolutional Neural Network (CNN)-based approaches are widely used for intelligent feature extraction and adaptive data embedding. CNN models can identify suitable regions within video frames for information hiding, thereby minimizing visual distortion and enhancing imperceptibility. Furthermore, CNN-based systems have demonstrated improved resistance against statistical detection techniques compared with conventional steganographic methods [15], [6], [20].

Generative Adversarial Networks (GANs) have emerged as another promising solution for secure video steganography. A GAN consists of a generator and a discriminator that operate in a competitive learning framework. The generator attempts to create stego content that is visually indistinguishable from the original video, while the discriminator attempts to detect hidden information. This adversarial process enables the development of highly secure and difficult-to-detect steganographic systems [4], [19].

Autoencoder-based frameworks have also gained considerable attention in recent years. These architectures learn compact feature representations and can simultaneous-ly optimize embedding and extraction processes. By leveraging end-to-end learning, autoencoder models achieve improved embedding efficiency and enhanced robustness against various multimedia attacks [2], [12].

Despite their advantages, AI-driven techniques face several challenges, including high computational complexity, extensive training requirements, and dependence on large annotated datasets. Nevertheless, their ability to provide adaptive embedding, im-proved security, and strong resistance to modern steganalysis methods makes them a promising direction for next-generation video steganography research [12], [7].

Emerging Trends in Video Steganography

Recent advancements in video steganography are increasingly focused on intelligent and secure multimedia communication. AI-based adaptive embedding techniques dynamically select embedding locations according to video characteristics, thereby improving imperceptibility and robustness. Blockchain-assisted steganography pro-vides enhanced integrity verification, authentication, and secure access control for multimedia data. In addition, cloud-IoT environments have created a demand for lightweight steganographic solutions capable of supporting secure real-time communication with limited computational resources. Researchers are also exploring quantum-resistant steganographic frameworks to ensure long-term security against future quantum computing threats. These emerging directions are expected to significantly influence the next generation of secure video steganography systems [10], [7], [6].

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

DATA SETS USED IN VIDEO STEGANOGRAPHY RESEARCH

The performance and reliability of video steganography algorithms largely depend on the datasets used during experimentation and evaluation. Different datasets provide varying levels of scene complexity, motion characteristics, frame quality, and environmental conditions, enabling researchers to assess the effectiveness of embedding and extraction techniques under diverse scenarios. The selection of an appropriate dataset is essential for evaluating imperceptibility, robustness, embedding capacity, and resistance to steganalysis attacks [9], [10].

Several benchmark datasets have been widely adopted in video steganography research, ranging from human activity datasets and surveillance videos to medical and multimedia video collections. Table 2 summarizes commonly used datasets and their characteristics.

Table 2. Commonly Used Datasets in Video Steganography Research

Sr. No.	Dataset Name	Type	Resolution	Total Videos	Application Area	Features
1.	UCF101	Human Action Videos	320×240	13,320 videos	Action recognition & steganography	Diverse motion patterns
2.	HMDB51	Human Activity Dataset	Various	6,766 videos	Video security research	Complex scene variations
3.	Kinetics-400	Large-scale video dataset	256×256	400 classes	Deep learning steganography	High diversity
4.	Hollywood2	Movie video clips	Various	3,669 clips	Multimedia hiding	Real-world scenes
5.	DAVIS Dataset	Object segmentation videos	480p/1080p	150 sequences	Frame-based embed-ding	High-quality frames
6.	UCID Dataset	Uncompressed frames	512×384	1,338 images	LSB and DCT methods	Bench-mark dataset
7.	BOSSBase	Image/frame dataset	512×512	10,000 images	Steganalysis testing	High-quality grayscale data
8.	VIRAT Video Dataset	Surveil-lance videos	HD	12+ hours video	Smart surveil-lance	CCTV footage
9.	Medical Video Dataset	Medical videos	Various	Multiple sequences	Healthcare security	Sensitive medical content

The choice of dataset depends on the objectives of the steganographic system and the target application domain. Human activity datasets such as UCF101 and HMDB51 are frequently employed for evaluating general-purpose video steganography methods due to their diverse motion patterns and scene variations. Surveillance datasets are commonly used for cybersecurity and intelligent monitoring applications, whereas medical video datasets support research related to secure healthcare communication. Large-scale datasets with substantial visual diversity are particularly valuable for training and evaluating modern AI-driven steganography frameworks [10], [14]. The increasing adoption of deep learning techniques has further emphasized the need for high-quality and diverse datasets capable of supporting robust model training and comprehensive performance evaluation.

COMPARATIVE ANALYSIS OF VIDEO STEGANOGRAPHY TECHNIQUES

Different video steganography techniques exhibit distinct characteristics with respect to security, embedding capacity, robustness, computational complexity, and visual quality. Consequently, selecting an appropriate technique depends on the specific requirements of the target application. For instance, applications requiring high pay-load capacity may prefer spatial-domain methods, whereas security-sensitive environments often rely on transform-domain, hybrid, or AI-driven approaches.

To provide a comprehensive understanding of existing methods, a comparative analysis of major video steganography techniques is presented based on commonly used evaluation criteria. These criteria include security level, computational complexity, robustness against attacks, embedding capacity, and imperceptibility. The comparison highlights the strengths and limitations of different approaches and assists researchers in selecting suitable techniques for various cybersecurity and multimedia protection applications [9], [10].

Table 3. Comparative Analysis of Video Steganography Techniques

Sr. No.	Technique	Security	Complexity	Robustness	Embedding Capacity	Visual Quality
1.	LSB	Medium	Low	Low	High	High
2.	DCT/DWT	High	High	High	Medium	High
3.	Random Pixel Selection	High	Medium	Medium	Medium	High
4.	Huffman Coding	Medium	Medium	Medium	High	Medium
5.	Parity-based Methods	Medium	Low	Medium	Medium	Medium
6.	AI-assisted Methods	Very High	High	High	High	Very High

The comparative analysis reveals that spatial-domain techniques offer high embedding capacity and low computational complexity but are generally more susceptible to steganalysis and signal processing attacks. Transform-domain approaches improve robustness and security by embedding information within frequency components, although they require greater computational resources. Hybrid techniques attempt to balance security, visual quality, and embedding performance by combining multiple embedding strategies. In recent years, AI-driven methods have demonstrated significant improvements in imperceptibility, adaptive embedding, and resistance to detection. Despite their promising performance, these approaches often require extensive training data and substantial computational resources. Therefore, the choice of a steganographic technique should be guided by the desired trade-off among security, robustness, payload capacity, and implementation complexity [17], [10], [20].

PERFORMANCE PARAMETERS

The effectiveness of a video steganography system is evaluated using a set of quantitative and qualitative performance metrics. These parameters help researchers assess the quality of the stego video, the amount of information that can be embedded, and the system's resistance to various attacks. An ideal steganographic framework should maintain high visual quality while providing sufficient embedding capacity, robustness, and security. The most commonly used evaluation metrics in video steganography research are discussed below.

Peak Signal-to-Noise Ratio (PSNR)

PSNR is one of the most widely used metrics for evaluating the visual quality of a stego video. It measures the difference between the original and modified video frames after the embedding process. Higher PSNR values generally indicate better visual quality and lower perceptual distortion between the original and stego video frames [8], [9].

Mean Square Error (MSE)

MSE quantifies the average squared difference between the original and stego video frames and is commonly used to evaluate embedding distortion. A lower MSE value indicates that the embedding process introduces minimal distortion into the cover video [8].

Root Mean Square Error (RMSE)

RMSE is derived from MSE and provides a direct measure of reconstruction error between original and stego

frames. Lower RMSE values indicate better preservation of visual quality after the embedding process. RMSE is commonly used to compare the performance of different steganographic techniques [8].

Embedding Capacity

Embedding capacity refers to the amount of secret information that can be embedded within a video without significantly affecting its visual quality. Higher embedding capacity is desirable for secure multimedia communication; however, excessive payload may increase the risk of detection and visual distortion [9], [10].

Robustness

Robustness represents the ability of a steganographic system to preserve hidden information when the stego video undergoes various processing operations or attacks. A robust system should successfully recover the embedded message even after compression, noise addition, filtering, frame manipulation, or steganalysis attempts.

The combined evaluation of PSNR, MSE, RMSE, embedding capacity, and robustness provides a comprehensive assessment of video steganography performance. Since no single metric can fully represent system effectiveness, researchers often analyze multiple parameters simultaneously to determine the suitability of a technique for specific cybersecurity and multimedia security applications.

RESULT ANALYSIS OF EXISTING VIDEO STEGANOGRAPHY METHODS

The effectiveness of video steganography techniques can be evaluated through various performance indicators, including PSNR, MSE, RMSE, embedding capacity, and robustness. These metrics provide valuable insights into the trade-offs between visual quality, security, payload capacity, and resistance to attacks. Table 4 presents an approximate comparison of representative video steganography techniques based on commonly reported performance characteristics in the literature.

Table 4. Performance Comparison of Existing Video Steganography Methods

Sr. No.	Technique	PSNR (dB)	MSE	RMSE	Embedding Capacity	Robustness
1.	LSB-based Method	42–48	0.20–0.45	0.44–0.67	High	Low
2.	DCT-based Method	38–44	0.35–0.70	0.59–0.83	Medium	High
3.	DWT-based Method	40–46	0.25–0.60	0.50–0.77	Medium	High
4.	RPS-based Method	41–47	0.22–0.50	0.46–0.70	Medium	Medium
5.	Huffman Coding Method	43–49	0.18–0.40	0.42–0.63	High	Medium
6.	Parity-based Method	39–45	0.30–0.65	0.55–0.80	Medium	Medium
7.	CNN-based Steganography	45–52	0.10–0.28	0.31–0.53	High	Very High
8.	GAN-based Steganography	46–54	0.08–0.25	0.28–0.50	High	Very High
9.	Hybrid DWT-DCT Method	44–50	0.15–0.35	0.38–0.59	Medium	High

The performance ranges presented in Table 3 are synthesized from representative studies reported in the literature. The values are derived from experiments conducted on benchmark datasets such as UCF101, HMDB51, VIRAT, and BOSSBase under varying payload embedding rates and video processing conditions. Actual performance may vary depending on dataset characteristics, payload size, compression settings, and embedding strategies. The comparative analysis demonstrates that different video steganography techniques offer distinct trade-offs among security, robustness, embedding capacity, and visual quality. Spatial-domain approaches such as LSB provide high payload capacity and low computational complexity but exhibit limited resistance to compression and steganalysis attacks. Transform-domain methods, including DCT and DWT, improve robustness and security by embedding information within frequency coefficients. Hybrid techniques further enhance performance by combining multiple embedding strategies, resulting in improved reliability and

attack resistance. AI-driven approaches, particularly CNN- and GAN-based frameworks, achieve superior visual quality, adaptive embedding, and stronger resistance to detection. Overall, hybrid and AI-assisted methods currently represent the most promising solutions for cybersecurity-oriented video steganography applications [17], [10], [6], [20].

CHALLENGES AND FUTURE RESEARCH DIRECTIONS

Despite significant advancements in video steganography, several challenges continue to limit the effectiveness of existing approaches. One of the primary concerns is resistance to steganalysis attacks, as modern statistical and AI-based detection techniques can identify hidden information with increasing accuracy. Video compression standards such as MPEG and H.264 may also distort embedded data, reducing extraction reliability and overall system performance [12], [7].

Another major challenge is the computational complexity associated with advanced hybrid and AI-driven techniques. Deep learning-based models often require extensive training datasets, high processing power, and significant memory resources. Further-more, achieving an optimal balance among embedding capacity, imperceptibility, robustness, and security remains a difficult task, as improvements in one parameter may negatively affect another.

Future research is expected to focus on AI-assisted adaptive embedding strategies capable of dynamically selecting optimal embedding locations based on video content and security requirements. The integration of blockchain technology may enhance data integrity, authentication, and access control in multimedia communication systems. In addition, the development of lightweight steganographic frameworks for cloud and IoT environments will support secure real-time communication with limited computational resources. Emerging areas such as quantum-resilient security mechanisms, intelligent steganalysis resistance, and hybrid multimedia protection frameworks are also expected to play an important role in the next generation of secure video steganography systems [10], [7], [6].

CONCLUSION

Video steganography has emerged as an important research area in cybersecurity and multimedia security due to its ability to provide covert and secure communication. Compared with conventional imagebased approaches, video steganography offers higher embedding capacity, improved imperceptibility, and enhanced robustness by utilizing the spatial and temporal characteristics of video data.

This paper presented a systematic review of video steganography techniques, covering classical spatial-domain methods, transform-domain approaches, hybrid frameworks, and recent AI-driven solutions. Widely used techniques, benchmark datasets, performance evaluation metrics, and application domains were analyzed to provide a com-prehensive understanding of the current research landscape. A comparative assessment of different approaches highlighted the trade-offs among security, robustness, computational complexity, embedding capacity, and visual quality.

The review indicates that traditional methods such as LSB-based embedding remain attractive because of their simplicity and high payload capacity, whereas transform-domain and hybrid techniques offer improved robustness against compression and signal processing attacks. Furthermore, AI-driven approaches, including deep learning-based frameworks, have demonstrated significant potential in enhancing adaptive embedding, imperceptibility, and resistance to steganalysis.

Despite these advancements, several challenges remain, including computational complexity, real-time implementation constraints, and the continuous evolution of steganalysis techniques. Future developments are expected to focus on intelligent embedding strategies, blockchain-assisted security, lightweight cloud-IoT frameworks, and quantum-resilient multimedia protection mechanisms. Overall, video steganography continues to be a promising technology for next-generation secure multimedia communication and cybersecurity applications.

REFERENCES

1. Cheddad, A., Condell, J., Curran, K., & McKevitt, P. (2010). Digital image steganography: Survey and analysis of current methods. Signal Processing, 90(3), 727–752. https://doi.org/10.1016/j.sigpro.2009.08.010
2. Fridrich, J., & Kodovský, J. (2012). Rich models for steganalysis of digital images. IEEE Transactions on Information Forensics and Security, 7(3), 868–882. https://doi.org/10.1109/TIFS.2012.2190402
3. Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative adversarial nets. In Z. Ghahramani & M. Welling (Eds.), Advances in Neural Information Processing Systems 27 (NeurIPS 2014) (pp. 2672–2680). https://scholar.google.com/scholar?q=Generative+Adversarial+Nets+Goodfellow+2014
4. Gupta, R., & Verma, S. (2020). Secure video steganography using random pixel selection and encryption. In P. Singh & A. Kumar (Eds.), Intelligent Computing and Communication (LNCS Vol. 11871, pp. 411–420). Springer, Singapore. https://scholar.google.com/scholar?q=Secure+video+steganography+using+random+pixel+selection+and+encryption
5. Khan, M., Shaukat, K., Alghamdi, A., et al. (2024). CNN-based adaptive video steganography for secure IoT communication. In Proceedings of the International Conference on Intelligent Computing and Cyber Security (pp. 89–96). IEEE. https://scholar.google.com/scholar?q=CNNbased+adaptive+video+steganography+for+secure+IoT+communication
6. Kheddar, H., Hemis, M., Himeur, Y., Megías, D., & Amira, A. (2024). Deep learning for steganalysis of diverse data types: A review of methods, taxonomy, challenges and future directions. Neurocomputing, 587, 127588. https://doi.org/10.1016/j.neucom.2024.127588
7. Li, B., He, J., Huang, J., & Shi, Y. Q. (2015). A survey on image steganography and steganalysis. Journal of Information Hiding and Multimedia Signal Processing, 6(4), 706–719. https://scholar.google.com/scholar?q=A+survey+on+image+steganography+and+steganalysis
8. Li, Y., Zhang, X., & Wang, S. (2019). Video steganography: A review. Neurocomputing, 335, 238–250. https://doi.org/10.1016/j.neucom.2018.12.083
9. Liu, S., Zhang, H., Zhao, Y., & Wang, J. (2023). Video steganography: Recent advances and challenges. Multimedia Tools and Applications, 82(27), 41943–41985. https://doi.org/10.1007/s11042-023-15158-0
10. Luo, W., Huang, F., & Huang, J. (2010). Edge adaptive image steganography based on LSB matching revisited. IEEE Transactions on Information Forensics and Security, 5(2), 201–214. https://doi.org/10.1109/TIFS.2010.2041812
11. Luo, X., Liu, F., Lian, S., et al. (2021). Deep learning-based steganography and steganalysis: A survey. ACM Computing Surveys, 54(2), 1–36. https://doi.org/10.1145/3437479
12. Manjula, G. R., & Sushma, R. B. (2021). Video steganography: A survey of techniques and methodologies. In Smart Data Intelligence 2021 (pp. 1–11). Springer, Singapore. https://scholar.google.com/scholar?q=Video+steganography+A+survey+of+techniques+and+methodologies
13. Mou, C., Xu, Y., Song, J., Zhao, C., Ghanem, B., & Zhang, J. (2023). Large-capacity and flexible video steganography via invertible neural network. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (pp. 1–10). https://scholar.google.com/scholar?q=Largecapacity+and+flexible+video+steganography+via+invertible+neural+network
14. Qian, Y., Dong, J., Wang, W., & Tan, T. (2015). Deep learning for steganalysis via convolutional neural networks. In Media Watermarking, Security, and Forensics 2015 (pp. 1–10). SPIE. https://doi.org/10.1117/12.2075239
15. Schmidhuber, J. (2015). Deep learning in neural networks: An overview. Neural Networks, 61, 85–117. https://doi.org/10.1016/j.neunet.2014.09.003
16. Singh, K. U., & Singhal, A. (2017). Video steganography techniques: A survey. International Journal on Recent and Innovation Trends in Computing and Communication, 5(5), 687–695. https://scholar.google.com/scholar?q=Video+steganography+techniques+A+survey
17. Wang, Y., & Chen, B. (2022). DWT–DCT based secure video steganography for multimedia

communication. In Proceedings of the IEEE International Conference on Communication and Signal Processing (pp. 233–237). IEEE. https://scholar.google.com/scholar?q=DWTDCT+based+secure+video+steganography+for+multimedia+communication

18. Weng, X., Li, Y., Chi, L., & Mu, Y. (2018). Convolutional video steganography with temporal residual modeling. In L. Leal-Taixé & S. Roth (Eds.), ECCV 2018 Workshops (LNCS Vol. 11134, pp. 237–253). Springer, Cham. https://doi.org/10.1007/978-3-030-11021-5_18
19. Zhang, J., Dong, J., Wang, W., & Tan, T. (2020). Adaptive steganography based on adversarial examples. IEEE Signal Processing Letters, 27, 1535–1539. https://doi.org/10.1109/LSP.2020.3019924
20. Zhang, R., Zhu, H., Liu, F., & Liu, J. (2024). Video steganography based on deep convolutional neural networks. Multimedia Tools and Applications, 83(4), 10357–10378. https://doi.org/10.1007/s11042-023-17158-6