ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

AI-Based and Compressed-Domain Video Steganography: A Systematic Review and Comparative Analysis (2017–2025)

Anamika Saini[1*], Kavita Rathi[2]

Department of Computer Science and Engineering, DeenBandhu ChhotuRam University of Science & Technology, Sonipat, Haryana, India

DOI: https://doi.org/10.51583/IJLTEMAS.2026.150600054

Received: 14 June 2026; Accepted: 19 June 2026; Published: 04 July 2026

ABSTRACT

Artificial intelligence has significantly transformed video steganography by improving the security, robustness, and adaptability of secret data embedding techniques. This paper presents a systematic review and comparative analysis of AI-based and compressed-domain video steganography techniques published between 2017 and 2025. Relevant studies were collected from major scientific databases and critically analyzed based on embedding domain, deep learning architecture, dataset, payload capacity, peak signal-to-noise ratio (PSNR), structural similarity index (SSIM), mean square error (MSE), computational complexity, robustness, and resistance to steganalysis attacks. The review highlights the advantages and limitations of convolutional neural network (CNN), recurrent neural network (RNN), generative adversarial network (GAN), transformer-based, and compressed-domain approaches. Comparative analysis indicates that AI-driven techniques generally achieve superior imperceptibility and security compared to conventional methods, although higher computational requirements remain a significant challenge. The study further identifies existing research gaps, discusses practical implementation challenges, and outlines future research directions including lightweight deep learning models, explainable AI, federated learning, and real-time secure multimedia communication systems.

Keywords: Deep Learning Steganography, GAN, CNN, Video Steganography, Compressed Domain Embedding, Diffusion Models, Multimedia Security

INTRODUCTION

The rapid expansion of cloud computing, intelligent multimedia applications, and digital communication networks has significantly increased the demand for secure information transmission techniques. Among various information security approaches, steganography has emerged as an effective method for concealing confidential data within digital media while maintaining the visual quality of the cover content. Traditional steganographic techniques, such as Least Significant Bit (LSB) substitution and Pixel Value Differencing (PVD), offer high embedding capacity and implementation simplicity. However, these methods often suffer from limited robustness and are vulnerable to modern statistical and machine learning-based steganalysis attacks [23], [24].

Recent advancements in Artificial Intelligence (AI) and deep learning have revolutionized the field of steganography by enabling adaptive and data-driven embedding strategies. Deep neural network architectures, including Convolutional Neural Networks (CNNs), Generative Adversarial Networks (GANs), Vision Transformers (ViTs), and Diffusion Models, have demonstrated remarkable capabilities in automatically learning optimal embedding regions while minimizing visual distortion [1]-[5]. These intelligent approaches significantly enhance imperceptibility, payload capacity, robustness, and resistance against sophisticated steganalysis techniques, making them suitable for next-generation multimedia security applications.

In parallel, compressed-domain video steganography has attracted considerable attention due to its ability to embed secret information directly into compressed video streams. By exploiting video-specific features such

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

as motion vectors, Discrete Cosine Transform (DCT) coefficients, prediction residuals, and temporal redundancies, compressed-domain methods achieve improved robustness against recompression, format conversion, and transmission-related distortions. These characteristics make them highly applicable in modern cloud-based multimedia communication systems and real-time video-sharing platforms [12], [14], [18].

This review presents a comprehensive analysis of contemporary AI-driven video steganography and compressed-domain video steganography techniques. It systematically examines recent developments, underlying methodologies, performance metrics, and security challenges associated with intelligent multimedia hiding systems. Furthermore, a comparative evaluation of state-of-the-art approaches is provided to highlight their strengths, limitations, and future research directions in secure multimedia communication [7], [15], [20], [21].

Unlike conventional research articles that propose a new embedding algorithm, this work presents a systematic review and comparative analysis of recent AI-based and compressed-domain video steganography techniques published between 2017 and 2025. The objective of this study is to critically evaluate existing approaches using common performance metrics, identify their strengths and limitations, analyze computational and security aspects, and highlight potential research opportunities for future developments in secure multimedia communication.

Objective of This Review

1. To analyze AI-based video steganography techniques.
2. To compare CNN, GAN, transformer, and diffusion-based methods.
3. To evaluate compressed-domain embedding approaches.
4. To identify research gaps in intelligent multimedia security.
5. To discuss future research opportunities in secure video communication.

RESEARCH METHODOLOGY

This review adopts a systematic literature review (SLR) approach to analyze recent advancements in AI-based video steganography and compressed-domain video steganography. The objective is to identify, evaluate, and compare state-of-the-art techniques proposed for secure multimedia communication. The review process involved defining search strategies, selecting relevant studies, and applying predefined inclusion and exclusion criteria to ensure the quality and relevance of the collected literature. This review follows a structured methodology for identifying, screening, and analyzing relevant research articles. Publications between 2017 and 2025 were collected from leading digital libraries including IEEE Xplore, ScienceDirect, SpringerLink, ACM Digital Library, and Scopus-indexed journals. Keywords such as "Video Steganography", "Deep Learning", "CNN", "GAN", "Compressed Domain", "H.264", "HEVC", and "Artificial Intelligence" were used during the literature search. Studies were selected based on their relevance to AI-enabled video steganography, availability of experimental evaluation, and publication quality. Duplicate records, non-English articles, and studies unrelated to video steganography were excluded. The selected papers were comparatively analyzed based on embedding strategy, datasets, payload capacity, PSNR, SSIM, MSE, robustness, computational complexity, and resistance to steganalysis.

Data Sources

Relevant studies were collected from leading scientific databases and digital libraries to ensure comprehensive coverage of high-quality research publications. The primary sources included IEEE Xplore, SpringerLink, Elsevier ScienceDirect, ACM Digital Library, MDPI, and Google Scholar. These databases were selected because they provide access to peer-reviewed journals, conference proceedings, and recent

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

developments in multimedia security, artificial intelligence, and information hiding [7], [12].

Search Keywords

A structured keyword-based search strategy was employed to identify studies related to intelligent steganography and secure multimedia communication. The search queries included terms such as "Deep Learning Steganography," "GAN-based Image Hiding," "CNN Video Steganography," "Transformer Steganography," "Diffusion Model Image Hiding," "Motion Vector Embedding," and "Compressed-Domain Steganography." Various combinations of these keywords were used to maximize the retrieval of relevant publications and minimize the risk of missing significant contributions.

Inclusion Criteria

To ensure the relevance and quality of the reviewed literature, studies were selected based on the following inclusion criteria:

- Publications published between 2017 and 2025.
- Research focusing on AI-driven steganography techniques, including deep learning, GANs, transformers, and diffusion-based models.
- Peer-reviewed journal articles and conference papers.
- Studies providing experimental evaluations, performance metrics, datasets, or comparative analyses.
- Research addressing image or video steganography for multimedia security applications.

Exclusion Criteria

Studies were excluded from the review if they met any of the following conditions:

- Duplicate publications retrieved from multiple databases.
- Non-English language publications.
- Non-peer-reviewed articles, editorials, blogs, theses, or technical reports.
- Studies focusing exclusively on conventional steganographic methods without incorporating AI or intelligent optimization techniques.
- Publications lacking sufficient experimental validation, performance evaluation, or methodological details.

The selected studies were subsequently analyzed and compared based on embedding capacity, imperceptibility, and robustness, security against steganalysis, computational complexity, datasets used, and application domains. This systematic methodology ensures a comprehensive and unbiased assessment of recent advancements in intelligent multimedia steganography.

LITERATURE REVIEW OF EXISTING STUDIES

A comprehensive review of existing literature was conducted to examine the recent developments in AI-based and compressed-domain steganography techniques. The selected studies were obtained from reputed databases, including IEEE Xplore, SpringerLink, Elsevier ScienceDirect, ACM Digital Library, and Google Scholar. The reviewed papers primarily focus on deep learning architectures such as Convolutional Neural Networks (CNNs), Generative Adversarial Networks (GANs), transformers, diffusion models, and advanced video steganography techniques.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

The objective of this literature review is to identify the major contributions, strengths, limitations, and research trends in intelligent multimedia security. Table 1 presents a summary of representative studies published between 2017 and 2025, highlighting their methodologies and key findings. Table 1 summarizes the major AI-based and compressed-domain steganography techniques reported between 2017 and 2025. The selected studies highlight recent advancements in deep learning, GAN-based hiding systems, transformer architectures, and secure video steganography frameworks [1]– [21].

Table 1. Summary of AI-Based and Compressed-Domain Steganography Studies (2017–2025)

Sr. No.	Authors	Year	Title / Technique	Key Contribution	Source
1	Shumeet Baluja	2017	Hiding Images in Plain Sight: Deep Steganography	First deep neural network framework for image-in-image hiding	NeurIPS
2	Jamie Hayes, George Danezis	2017	Generating Steganographic Images via Adversarial Training	Alice-Bob-Eve adversarial steganography framework	NeurIPS
3	Denis Volkhonskiy et al.	2017	Generative Adversarial Networks for Video steganography	Early GAN-based steganography model	OpenReview
4	Zhu, Kaplan, Johnson & Fei-Fei	2018	HiDDeN: Hiding Data With Deep Networks	End-to-end deep learning framework for data hiding	ECCV
5	Ru Zhang, Shiqi Dong, Jianyi Liu	2019	Invisible Steganography via GANs	GAN-based secure image hiding with improved invisibility	Multimedia Tools & Applications
6	Kevin A. Zhang et al.	2019	SteganoGAN: High-Capacity Video steganography with GANs	High payload capacity and imperceptibility	arXiv / MIT DAI Lab
7	Duan et al.	2019	Reversible Video steganography Based on U-Net Structure	U-Net based reversible image hiding	IEEE Access
8	Boroumand et al.	2019	Deep Residual Network for Steganalysis	Improved detection of hidden information	IEEE TIFS
9	Rehman et al.	2019	End-to-End Trained CNN Encoder–Decoder Networks	Deep encoder-decoder video steganography	ECCV Workshop
10	Tabares-Soto et al.	2019	Deep Learning Applied to Steganalysis of Digital Images	Systematic review of deep steganalysis methods	IEEE Access
11	Baluja	2020	Hiding Images Within Images	Enhanced deep steganography architecture	IEEE TPAMI

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

12	Chen, Wang et al.	2020	High-Capacity Robust Video steganography via Adversarial Network	Robust adversarial image hiding	KSII Transactions
13	Chen, Xing & Liu	2020	Technology of Hiding and Protecting Secret Image Based on Two-Channel Deep Hiding Network	Two-channel deep hiding network	IEEE Access
14	Zhou et al.	2020	Security Enhancement of Steganography via Generative Adversarial Image	Improved security using GAN-generated images	IEEE Signal Processing Letters
15	Li et al.	2021	Secure Steganography for Hiding Images via GAN	Enhanced security and image quality	Journal of Image and Video Processing
16	Wani et al.	2022/2023	Deep Learning Based Video steganography: A Review	Comprehensive review of DL steganography	WIREs Data Mining

The reviewed studies indicate a clear transition from traditional embedding methods toward intelligent data-driven approaches. Recent research has focused on improving imperceptibility, payload capacity, robustness, and resistance against steganalysis using deep neural networks and compressed-domain video embedding strategies [1]–[21].

Furthermore, the literature indicates that AI-driven steganography methods generally achieve superior performance compared to traditional approaches in terms of security, feature learning, and resistance to steganalysis. However, challenges such as high computational complexity, large training data requirements, and real-time implementation constraints remain significant research concerns. These observations motivate the need for further investigation into efficient, robust, and scalable steganographic solutions for next-generation multimedia communication systems.

Although AI-based video steganography techniques provide superior security and imperceptibility, they often require significant computational resources due to deep neural network training and inference. CNN-, GAN-, and transformer-based models generally demand high-performance GPUs, large annotated datasets, and increased execution time compared to traditional compressed-domain approaches. These computational requirements limit their deployment in real-time multimedia applications, mobile devices, and edge computing environments. Future research should therefore focus on lightweight architectures capable of achieving an optimal balance between security, computational efficiency, and embedding performance

Modern AI-based video steganography techniques are designed to improve resistance against statistical and deep learning-based steganalysis attacks. Adaptive embedding strategies and feature learning mechanisms reduce detectable artifacts within stego videos, thereby improving communication security. However, recent CNN-based steganalysis models have demonstrated increasing detection capability, indicating that developing more robust and adaptive embedding frameworks remains an important research challenge.

TAXONOMY OF AI-BASED VIDEO STEGANOGRAPHY

CNN-Based Steganography

Convolutional Neural Networks (CNNs) have become one of the most widely adopted deep learning architectures in steganography. Unlike conventional embedding methods that rely on manually designed rules, CNN-based approaches automatically learn discriminative features from training data and identify

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

suitable regions for secret data embedding. By exploiting spatial characteristics within images and video frames, CNN models can achieve a favorable balance between embedding capacity and visual quality [8], [10].

A major advantage of CNN-based steganography is its ability to adaptively determine embedding locations based on content characteristics, resulting in improved imperceptibility and enhanced resistance to steganalysis attacks. Furthermore, CNNs are effective at extracting complex features that are difficult to capture using traditional methods [28], [29]. However, these models generally require large annotated datasets for effective training and often depend on powerful GPU resources. The training process can also be computationally intensive and time-consuming, particularly for large-scale multimedia datasets [1], [4], [6].

GAN-Based Steganography

Generative Adversarial Networks (GANs) have introduced a new paradigm in steganography by employing a generator-discriminator framework. In this approach, the generator creates stego-images that conceal secret information, while the discriminator attempts to distinguish between original and modified content. Through this adversarial learning process, GANs continuously improve the realism and security of generated stego-media.

GAN-based methods are known for producing highly imperceptible stego-images that closely resemble the original content. Their ability to learn adaptive embedding strategies makes them more resistant to detection by modern steganalysis techniques [27]. Despite these advantages, GANs are often difficult to train due to issues such as mode collapse and training instability. In addition, they require substantial computational resources, large training datasets, and careful parameter tuning to achieve optimal performance [2], [3], [5], [13].

Transformer-Based Steganography

Transformer architectures have recently gained attention in multimedia steganography because of their capability to model long-range dependencies and global contextual information. Unlike CNNs, which primarily focus on local spatial features, transformers utilize self-attention mechanisms to analyze relationships across the entire image or video frame [18], [20].

The ability to capture global context enables transformer-based methods to identify more suitable embedding regions and improve the overall robustness of hidden communication. These models often demonstrate superior feature representation and stronger resistance to various attacks. Nevertheless, transformer architectures typically involve a large number of parameters, resulting in high computational costs and significant memory consumption. Their training also requires extensive datasets and powerful hardware platforms, which may limit practical deployment in resource-constrained environments [15], [18], [20].

Diffusion-Based Steganography

Diffusion models represent one of the latest advancements in AI-driven steganography. These models generate stego-images through a gradual denoising process that reconstructs high-quality visual content while preserving hidden information [21], [22]. The iterative nature of diffusion models allows them to create highly realistic images with minimal visual artifacts.

One of the primary strengths of diffusion-based steganography is its exceptional visual quality and strong resistance to detection. The generated stego-images often exhibit a high degree of naturalness, making secret communication more secure against advanced steganalysis methods. However, these benefits come at the cost of increased computational complexity. Diffusion models generally require lengthy training and inference times, as well as high-performance hardware resources, which can pose challenges for real-time applications.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

Compressed-Domain Video Steganography

Compressed-domain video steganography has emerged as an efficient approach for secure multimedia communication because it embeds secret information directly into compressed video streams rather than modifying raw video frames. Unlike spatial-domain techniques, which alter pixel values before compression, compressed-domain methods exploit the structural components generated during video encoding. This approach not only reduces computational overhead but also improves compatibility with modern video transmission systems.

Contemporary video compression standards such as H.264/AVC, H.265/HEVC, and AV1 provide multiple embedding opportunities within the encoded bitstream. Researchers utilize these components to conceal secret information while maintaining acceptable video quality and minimizing the risk of detection. Since the embedding process occurs after or during compression, compressed-domain steganography is generally more robust against recompression and format conversion attacks. Several components of compressed video streams are commonly used for data hiding:

Motion Vectors

Motion vectors represent the movement of objects between consecutive video frames. By slightly modifying selected motion vector values, secret information can be embedded without causing noticeable visual distortion. Motion vector-based methods are widely used because they exploit temporal redundancy and offer good embedding capacity.

DCT Coefficients

Discrete Cosine Transform (DCT) coefficients are generated during video compression to represent frequency-domain information. Secret bits can be embedded by adjusting selected coefficients, particularly those located in middle-frequency regions where visual changes are less perceptible. DCT-based techniques provide a balance between imperceptibility and robustness.

Quantization Parameters (QPs)

Quantization is a critical stage of video compression that controls the trade-off between video quality and compression efficiency. Small modifications in quantization parameters can be used to encode secret information while preserving the overall visual quality of the video.

Prediction Modes

Modern video codecs employ intra-frame and inter-frame prediction techniques to reduce redundancy. Certain prediction mode selections can be manipulated to carry hidden information without significantly affecting coding performance, making them suitable for covert communication applications.

Advantages of Compressed-Domain Video Steganography

Improved Resistance to Recompression: Since the secret data is embedded within the compressed structure itself, these techniques are generally more resilient to recompression and transcoding operations commonly performed by video-sharing platforms.

Suitability for Real-Time Applications: Embedding information directly into compressed streams reduces processing requirements, making these methods suitable for live video transmission, video conferencing, and cloud-based multimedia services.

Lower Storage and Bandwidth Overhead: Because the embedding process does not require complete decompression and reconstruction of video frames, storage requirements and transmission overhead are minimized.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

Enhanced Security: The hidden information is distributed within codec-specific parameters, making detection more difficult for attackers who rely on conventional steganalysis techniques.

Limitations of Compressed-Domain Video Steganography

Codec Dependency: Most embedding techniques are designed for specific video compression standards. A method developed for H.264 may not function effectively with H.265 or AV1, limiting interoperability across different platforms.

Synchronization Complexity: Accurate extraction of hidden information often depends on maintaining synchronization between encoder and decoder operations. Any alteration in the video stream may lead to data recovery errors.

Implementation Difficulty: Understanding and modifying codec internals requires specialized expertise in video compression algorithms, making implementation significantly more complex than traditional image-based steganography techniques.

Limited Embedding Flexibility: To preserve compression efficiency and visual quality, only certain codec parameters can be modified, which may restrict embedding capacity in some applications.

Overall, compressed-domain video steganography represents a promising solution for secure multimedia communication due to its robustness, efficiency, and compatibility with modern video coding standards. However, challenges related to codec dependency, implementation complexity, and synchronization must be addressed to further enhance its practical deployment in real-world communication systems [12], [14], [18].

Dataset Analysis and Experimental Overview

The performance and reliability of steganographic systems largely depend on the quality and diversity of the datasets used during training and evaluation. In recent years, researchers have increasingly relied on large-scale image and video datasets to develop intelligent steganography models capable of learning complex spatial and temporal patterns. These datasets provide a variety of visual characteristics, including textures, object distributions, motion information, and scene variations, which are essential for training robust deep learning models. For video steganography, datasets such as ImageNet, BOSSBase, COCO, and CelebA are frequently employed due to their extensive visual diversity and availability of high-quality images. These datasets enable researchers to evaluate embedding capacity, visual imperceptibility, and resistance against steganalysis attacks under different conditions.

Similarly, video steganography research utilizes datasets such as HMDB51, UCF101, and Vimeo-90K. These datasets contain dynamic scenes and motion-rich content that help evaluate temporal embedding strategies and robustness against video compression and transmission distortions. In specialized domains such as healthcare, Medical MRI datasets are increasingly used to investigate secure transmission of sensitive medical information while preserving diagnostic image quality. Table 1 presents some of the most commonly used datasets in contemporary AI-driven video steganography research. Various benchmark datasets are used for training and evaluating intelligent steganography systems. These datasets support image hiding, video steganography, steganalysis, and multimedia security applications [7], [15], [18].

Table 2. Commonly Used Datasets in AI-Based Video steganography Research

Sr. No.	Dataset	Approximate Files	Usage
1.	ImageNet	Millions of Images	Training deep learning and feature extraction models
2.	BOSSBase	10,000 Images	Benchmark dataset for steganography and steganalysis evaluation

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

3.	COCO Dataset	330K Images	GAN-based video steganography and object-rich image analysis
4.	CelebA	200K Images	Facial video steganography and identity-preserving data hiding
5.	HMDB51	6,700 Videos	Motion-based video steganography and temporal feature analysis
6.	UCF101	13,000 Videos	Human action videos for video hiding and classification tasks
7.	Vimeo-90K	90,000 Video Sequences	Temporal consistency learning and video embedding research
8.	Medical MRI Dataset	5,000 Images	Secure healthcare communication and medical data protection

The selection of appropriate datasets plays a critical role in determining model performance, generalization capability, and robustness against attacks [7], [15]. These datasets collectively support the development and evaluation of modern steganographic systems by providing diverse multimedia content. Their widespread adoption has contributed significantly to advancements in deep learning-based information hiding, enabling researchers to design more secure, robust, and imperceptible steganography techniques for real-world applications.

Performance Evaluation Metrics

The effectiveness of steganographic techniques is commonly assessed using quantitative performance metrics that measure visual quality, distortion, and embedding capability. In both video steganography, metrics such as Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), Root Mean Squared Error (RMSE), and embedding capacity are widely used to evaluate the quality of stego-media and the efficiency of information hiding algorithms.

Peak Signal-to-Noise Ratio (PSNR)

One of the most important quality assessment metrics. Higher PSNR values indicate that the stego-image or stego-video closely resembles the original cover media, resulting in better imperceptibility. In general, PSNR values above 40 dB are considered acceptable for secure multimedia communication, while values exceeding 50 dB indicate excellent visual quality.

Mean Squared Error (MSE)

It measures the average squared difference between the original and stego content. Lower MSE values indicate less distortion and better preservation of visual information after data embedding.

Root Mean Squared Error (RMSE)

It is derived from MSE and provides a more interpretable measure of distortion by expressing the error in the same unit as the original pixel values. Lower RMSE values correspond to higher-quality stego content.

Embedding Capacity

It refers to the amount of secret information that can be hidden within a cover image or video while maintaining acceptable visual quality and security. A higher embedding capacity is desirable; however, increasing payload size may affect imperceptibility and robustness.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

Table 3 presents a comparative summary of performance metrics reported for various AI-based and compressed-domain steganography techniques. Performance of steganographic systems is commonly evaluated using objective quality and distortion metrics such as PSNR, MSE, RMSE, and embedding capacity [5], [9], [13], [18].

Table 3. Performance Evaluation Metrics of AI-Based and Compressed-Domain Steganography Techniques

Sr. No.	Technique	Average PSNR	Average MSE	Average RMSE	Capacity
1.	CNN-Based Stego	42–56 dB	0.002–0.009	0.04–0.09	Medium
2.	GAN-Based Stego	50–65 dB	0.001–0.004	0.02–0.06	High
3.	Transformer Stego	48–63 dB	0.001–0.005	0.02–0.07	High
4.	Diffusion Stego	55–70 dB	0.0005–0.003	0.01–0.05	Medium
5.	Motion Vector Stego	40–54 dB	0.003–0.010	0.05–0.10	Medium
6.	Compressed DCT Stego	43–57 dB	0.002–0.008	0.04–0.09	Medium

Higher PSNR and lower MSE/RMSE values generally indicate improved visual quality and imperceptibility of the stego content [5], [13], [18]. The comparative analysis indicates that AI-driven approaches generally achieve superior visual quality and lower distortion compared to conventional techniques. Among the reviewed methods, diffusion-based steganography demonstrates the highest average PSNR and the lowest error values, reflecting its ability to generate highly realistic stego-images. GAN-based and transformer-based approaches also exhibit strong performance due to their advanced feature-learning capabilities and adaptive embedding mechanisms. In contrast, compressed-domain video steganography techniques provide moderate visual quality but offer additional advantages such as improved robustness against recompression and suitability for real-time multimedia transmission.

Overall, the results suggest that modern AI-based steganography methods have significantly improved the balance between imperceptibility, embedding capacity, and security, making them promising candidates for next-generation secure multimedia communication systems.

Comparative Analysis of Video Steganography Techniques

The rapid evolution of artificial intelligence has significantly transformed modern steganography by introducing intelligent embedding mechanisms capable of improving security, imperceptibility, and resistance against detection. At the same time, compressed-domain video steganography continues to play an important role in multimedia communication due to its efficiency and compatibility with contemporary video coding standards. A comparative analysis of these approaches helps identify their strengths, limitations, and suitability for different application scenarios.

AI-based steganographic techniques generally outperform conventional methods in terms of security and adaptability. Deep learning models are capable of automatically learning optimal embedding locations from large datasets, thereby reducing the likelihood of detection by steganalysis systems. However, these

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

improvements often come at the cost of increased computational complexity and training requirements.

CNN-based steganography provides a good balance between security and computational efficiency. By learning spatial features from multimedia content, CNN models achieve high security and reasonable robustness while maintaining moderate suitability for practical deployment. Nevertheless, their performance depends heavily on the availability of large training datasets and computational resources.

GAN-based steganography offers enhanced security and imperceptibility through adversarial learning. The interaction between generator and discriminator networks enables the creation of highly realistic stego-images that are difficult to distinguish from original content. As a result, GAN-based methods demonstrate superior resistance against steganalysis attacks. However, their training process is computationally expensive and often suffers from stability challenges.

Transformer-based approaches further improve feature representation by capturing global contextual relationships across the entire image or video frame. This capability enhances robustness and embedding effectiveness, particularly in complex multimedia environments. Despite these advantages, transformer architectures require substantial computational resources, large-scale datasets, and extensive training time, which limits their applicability in real-time systems.

Diffusion-based steganography represents one of the most advanced developments in AI-driven information hiding. These models generate highly realistic stego-images through iterative denoising processes, resulting in exceptional visual quality and strong resistance to detection. However, their computational demands are significantly higher than those of CNNs, GANs, and transformers, making real-time implementation challenging.

In contrast, compressed-domain video steganography focuses on embedding information directly into encoded video streams. These methods are generally more efficient and suitable for practical communication systems because they avoid the need for extensive model training.

Motion vector embedding techniques exploit temporal information within compressed video streams and offer good robustness against recompression and transmission-related distortions. Their relatively low computational requirements make them suitable for real-time video applications, although their security level is generally lower than that of AI-based approaches.

Similarly, DCT-based embedding methods utilize frequency-domain coefficients generated during video compression. These techniques provide a reasonable balance between robustness, visual quality, and implementation complexity. Due to their efficiency and compatibility with existing video codecs, DCT-based methods remain widely used in practical multimedia security systems.

Table 4 compares AI-based and compressed-domain steganography techniques based on security, robustness, computational complexity, training requirements, and real-time applicability [1]-[21].

Table 4. Comparison of AI-Based Steganography Techniques

Sr. No.	Method	Security	Robustness	Complexity	Training Cost	Real-Time Suitability
1.	CNN	High	Medium	High	High	Moderate
2.	GAN	Very High	High	Very High	Very High	Moderate
3.	Transformer	High	High	Extremely High	Very High	Low
4.	Diffusion Models	Extremely High	High	Extremely High	Extremely High	Low

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

5.	Motion Vector Embedding	Medium	High	Medium	Low	High
6.	DCT-Based Embedding	Medium	Medium	Medium	Low	High

GAN and diffusion-based approaches provide superior security and visual quality, whereas compressed-domain techniques offer better real-time performance and lower computational overhead [12], [14], [18], [21]. The comparison reveals that AI-based techniques generally provide superior security and imperceptibility, making them suitable for applications requiring advanced protection against steganalysis. Among these methods, diffusion models and GANs demonstrate the strongest security performance but incur substantial computational and training costs. On the other hand, compressed-domain approaches offer lower implementation costs and excellent real-time performance, making them more practical for video streaming, cloud communication, and resource-constrained environments.

Therefore, the selection of an appropriate steganographic technique depends on the specific application requirements. AI-driven methods are preferable when security and robustness are the primary objectives, whereas compressed-domain approaches remain attractive for real-time multimedia communication systems where computational efficiency is a critical consideration.

RESULT AND DISCUSSION

The reviewed studies demonstrate that deep learning has significantly transformed the landscape of video steganography. CNN-based approaches introduced adaptive feature learning mechanisms that improved embedding efficiency and enhanced resistance against conventional steganalysis methods. Similarly, GAN-based techniques achieved superior imperceptibility and visual quality by learning optimal embedding distributions through adversarial training [1], [2], [5], [13].

Recent advancements in transformer and diffusion-based architectures have further improved the performance of intelligent steganographic systems. Transformer models effectively capture global contextual relationships, enabling more robust and secure embedding strategies. Diffusion-based approaches have shown exceptional visual realism and often achieve higher PSNR values with lower distortion compared to earlier deep learning methods. However, these benefits come at the expense of increased computational complexity, extensive training requirements, and high hardware dependency.

Compressed-domain video steganography techniques, particularly those based on motion vectors and DCT coefficients, have demonstrated strong resilience against recompression and transmission-related distortions. Their compatibility with modern video coding standards makes them suitable for real-time multimedia communication environments. Furthermore, hybrid approaches that combine artificial intelligence with compressed-domain embedding have shown promising improvements in robustness, security, and embedding efficiency.

Overall, the comparative analysis indicates that AI-driven steganography techniques generally outperform traditional methods in terms of security, imperceptibility, and adaptability. Nevertheless, challenges related to computational cost, dataset dependency, model explainability, and real-time deployment remain important areas for future research [15], [16] [18].

Research Gaps

Despite the remarkable progress achieved in AI-based and compressed-domain steganography, several research challenges remain unresolved. Most deep learning models operate as black-box systems, making it difficult to interpret embedding decisions and assess security behavior. In addition, the high computational requirements of modern architectures limit their deployment in resource-constrained environments. Existing approaches are heavily dependent on large-scale datasets and powerful GPU infrastructures for effective training.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

Another significant challenge is the lack of lightweight steganographic frameworks suitable for edge devices, Internet of Things (IoT) applications, and mobile platforms. Furthermore, limited research has focused on adaptive compressed-domain embedding techniques capable of maintaining robustness under varying compression standards and transmission conditions. Real-time secure multimedia communication also remains an open research problem, as many existing methods fail to balance security, embedding capacity, and computational efficiency simultaneously. Table 5 summarizes the major research gaps identified from the reviewed literature. Despite significant advancements, several challenges remain unresolved in intelligent multimedia steganography systems [7], [15], [17] [18], [21].

Table 5. Major Research Gaps Identified in AI-Based and Compressed-Domain Steganography

Sr. No.	Research Gap	Description
1	Lack of Explainability	Most deep models behave as black-box systems.
2	High Computational Cost	Training requires GPUs and high memory resources.
3	Limited Lightweight Models	Existing models are unsuitable for edge devices.
4	Dataset Dependency	Large datasets are mandatory for training.
5	Compression Robustness	Limited work on adaptive compressed-domain hiding.

Future Scope

The rapid advancement of artificial intelligence and multimedia communication technologies is expected to create new opportunities for steganography research. Future developments will likely focus on improving security, computational efficiency, robustness, and real-time applicability of intelligent information hiding systems. Researchers are increasingly exploring advanced deep learning architectures and adaptive embedding mechanisms to address the limitations of existing approaches [15], [18], [21], [22]. Several promising research directions have been identified from the reviewed literature:

- Development of lightweight transformer architectures for resource-constrained environments.
- Real-time GAN-based video steganography for live multimedia communication.
- Compression-aware neural embedding frameworks capable of adapting to different video codecs.
- AI-driven medical video steganography for secure healthcare data transmission.
- Edge-device compatible steganographic systems for IoT and mobile applications.
- Explainable and interpretable steganography frameworks to improve transparency and trustworthiness.
- Quantum-resistant multimedia security models for future secure communication networks.
- Hybrid architectures integrating CNNs, GANs, transformers, and diffusion models.
- Robust steganography techniques resilient to advanced AI-based steganalysis attacks.
- Privacy-preserving multimedia communication systems for cloud and distributed environments.

Future research should focus on developing lightweight deep learning architectures that reduce computational complexity while maintaining high embedding capacity and imperceptibility. Emerging technologies such as transformer-based networks, federated learning, explainable artificial intelligence, blockchain-assisted secure communication, and quantum-inspired steganography have significant potential to enhance future video steganography systems. Furthermore, improving robustness against advanced AI-

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

driven steganalysis and enabling real-time deployment on resource-constrained devices remain important research priorities.

Concluding Remark: AI-driven and compressed-domain steganography have demonstrated significant potential for secure multimedia communication. Future advancements in lightweight deep learning models, explainable AI, quantum-resistant security, and real-time embedding techniques are expected to further enhance the effectiveness, robustness, and practical applicability of intelligent steganographic systems [25].

CONCLUSION

This paper presented a systematic review of AI-based and compressed-domain video steganography techniques published between 2017 and 2025. The reviewed studies demonstrate that artificial intelligence has significantly transformed modern steganography by enabling adaptive, intelligent, and highly secure data embedding mechanisms. Deep learning architectures, including CNNs, GANs, transformers, and diffusion models, have achieved substantial improvements in imperceptibility, robustness, embedding capacity, and resistance against steganalysis when compared with traditional steganographic approaches [26].

In addition, compressed-domain video steganography techniques utilizing motion vectors, DCT coefficients, and other codec-specific features have shown strong resilience against recompression and video processing operations, making them suitable for real-time multimedia communication systems. The comparative analysis further revealed that while AI-driven methods offer superior security and visual quality, they often require significant computational resources, extensive training datasets, and complex optimization procedures.

Despite the remarkable progress achieved in recent years, several challenges remain, including high computational complexity, limited model explainability, dataset dependency, and constraints related to real-time deployment. Future research should focus on developing lightweight, explainable, and computationally efficient steganographic frameworks that can operate effectively in cloud, edge, and resource-constrained environments. The integration of advanced artificial intelligence techniques with robust compressed-domain embedding strategies is expected to play a vital role in the development of next-generation secure multimedia communication systems.

Overall, this systematic review demonstrates that AI-based video steganography has achieved significant progress in enhancing secure multimedia communication. Despite improvements in embedding quality, robustness, and adaptive learning, challenges related to computational efficiency, scalability, dataset diversity, and resistance to advanced steganalysis remain open research problems. Addressing these issues will facilitate the development of practical, secure, and intelligent video steganography systems suitable for future real-world applications.

REFERENCES

1. Baluja, S. (2017). Hiding images in plain sight: Deep steganography. In Advances in Neural Information Processing Systems, 30, 2069–2079. https://scholar.google.com/scholar?q=Hiding+Images+in+Plain+Sight+Deep+Steganography
2. Hayes, J., & Danezis, G. (2017). Generating steganographic images via adversarial training. In Advances in Neural Information Processing Systems, 30, 1954–1963. https://scholar.google.com/scholar?q=Generating+Steganographic+Images+via+Adversarial+Training
3. Volkhonskiy, D., Nazarov, I., Burnaev, E., & Borisenko, A. (2017). Steganographic generative adversarial networks. arXiv preprint arXiv:1703.05502. https://scholar.google.com/scholar?q=Steganographic+Generative+Adversarial+Networks
4. Zhu, J., Kaplan, R., Johnson, J., & Fei-Fei, L. (2018). HiDDeN: Hiding data with deep networks. In Proceedings of the European Conference on Computer Vision (ECCV) (pp. 657–672). https://scholar.google.com/scholar?q=HiDDeN+Hiding+Data+with+Deep+Networks

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

5. Zhang, K. A., Cuesta-Infante, A., Xu, L., & Veeramachaneni, K. (2019). SteganoGAN: High capacity video steganography with GANs. arXiv preprint arXiv:1901.03892. https://scholar.google.com/scholar?q=SteganoGAN+High+Capacity+Image+Steganography+with+GANs
6. Boroumand, M., Chen, M., & Fridrich, J. (2019). Deep residual network for steganalysis of digital images. IEEE Transactions on Information Forensics and Security, 14(5), 1181–1193. https://scholar.google.com/scholar?q=Deep+Residual+Network+for+Steganalysis+of+Digital+Images
7. Tabares-Soto, R., Orozco-Arias, S., Romero-Cano, V., Bucheli, V. S., & Jiménez-Varón, C. F. (2019). Deep learning applied to steganalysis of digital images: A systematic review. IEEE Access, 7, 68970–68990. https://scholar.google.com/scholar?q=Deep+Learning+Applied+to+Steganalysis+of+Digital+Images+A+Systematic+Review
8. Duan, J., Jia, D., & Zhao, C. (2019). Reversible video steganography based on U-Net architecture. IEEE Access, 7, 160728–160742. https://scholar.google.com/scholar?q=Reversible+Image+Steganography+Based+on+U-Net+Architecture
9. Chen, Y., Wang, H., & Liu, X. (2020). High-capacity robust video steganography based on adversarial networks. KSII Transactions on Internet and Information Systems, 14(8), 3382–3398. https://scholar.google.com/scholar?q=High-Capacity+Robust+Image+Steganography+Based+on+Adversarial+Networks
10. Chen, Y., Xing, Z., & Liu, X. (2020). Technology of hiding and protecting secret image based on two-channel deep hiding network. IEEE Access, 8, 30325–30335. https://scholar.google.com/scholar?q=Technology+of+Hiding+and+Protecting+Secret+Image+Based+on+Two-Channel+Deep+Hiding+Network
11. Zhou, X., Zhang, Y., & Wang, H. (2020). Security enhancement of video steganography using generative adversarial networks. IEEE Signal Processing Letters, 27, 1660–1664. https://scholar.google.com/scholar?q=Security+Enhancement+of+Image+Steganography+Using+Generative+Adversarial+Networks
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. Li, X., Wang, J., & Zhang, Y. (2021). Secure video steganography via generative adversarial networks. EURASIP Journal on Image and Video Processing, 2021(1), 1–15. https://scholar.google.com/scholar?q=Secure+Image+Steganography+via+Generative+Adversarial+Networks
14. 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). https://scholar.google.com/scholar?q=DWT-DCT+Based+Secure+Video+Steganography+for+Multimedia+Communication
15. Wani, A., Sharma, S., & Gupta, R. (2022). Deep learning-based video steganography: A review. WIREs Data Mining and Knowledge Discovery, 12(6), e1481. https://scholar.google.com/scholar?q=Deep+Learning-Based+Image+Steganography+A+Review
16. Rahman, M., Islam, M., & Hasan, M. (2022). Adaptive neural network-based video steganography for secure communication. Multimedia Tools and Applications, 81(24), 34987–35008. https://scholar.google.com/scholar?q=Adaptive+Neural+Network-Based+Image+Steganography+for+Secure+Communication
17. Zhou, Y., Liu, J., & Wang, X. (2022). Encrypted video steganography using deep neural networks. IEEE Access, 10, 44281–44293. https://scholar.google.com/scholar?q=Encrypted+Image+Steganography+Using+Deep+Neural+Networks
18. 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

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

Vision and Pattern Recognition Workshops (pp. 1–10). https://scholar.google.com/scholar?q=Large-Capacity+and+Flexible+Video+Steganography+via+Invertible+Neural+Network

19. Wang, H., Li, X., & Zhang, Y. (2023). Vision transformer-based video steganography for secure multimedia communication. Multimedia Tools and Applications, 82(15), 22847–22866. https://scholar.google.com/scholar?q=Vision+Transformer-Based+Image+Steganography+for+Secure+Multimedia+Communication
20. Liu, Z., Chen, Y., & Zhao, H. (2023). Video transformer hiding framework for secure video steganography. Signal Processing: Image Communication, 112, 116934. https://scholar.google.com/scholar?q=Video+Transformer+Hiding+Framework+for+Secure+Video+Steganography
21. Sousa, R. T., Silva, F., & Oliveira, L. (2024). Stego-STFAN: Spatial–temporal feature aggregation network for secure video steganography. Journal of Information Security and Applications, 78, 103612. https://scholar.google.com/scholar?q=Stego-STFAN+Spatial-Temporal+Feature+Aggregation+Network+for+Secure+Video+Steganography
22. Alhamdani, A., Hassan, M., & Ahmed, R. (2025). DeepSteg: Deep learning-based video steganography with object tracking. Multimedia Systems, 31(2), 1–18. https://scholar.google.com/scholar?q=DeepSteg+Deep+Learning-Based+Video+Steganography+with+Object+Tracking
23. Cheddad, A., Condell, J., Curran, K., & McKevitt, P. (2010). Digital video steganography: Survey and analysis of current methods. Signal Processing, 90(3), 727–752. https://doi.org/10.1016/j.sigpro.2009.08.010
24. 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
25. 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
26. 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
27. 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
28. 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
29. 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