Journal of Science and Engineering Applications Vol. 8, No. 1, pp. xx–xx, April 2026

Journal of Science and Engineering Applications

Contents are available at https://jsea.iujournals.com

Image Steganography Based on Machine Learning Algorithms: A Survey

Yousif H. Jasim[1] and Asaad N.Hashim[2]

Department of Computer Science, College of Computer Science and Mathematics, University of Kufa, Najaf, Iraq

yousifh.alsary@student.uokufa.edu.iq; asaad.alshareefi@uokufa.edu.iq

ARTICLE INFORMATION

Received date: Date Mon Year
Revised date: Date Mon Year
Accepted date: Date Mon Year

Keywords

Image steganography, Machine learning algorithms, Deep learning, Convolutional neural networks, Generative adversarial networks.

ABSTRACT

Image steganography is an important field for secure data transmission by embedding secret messages within digital images in difficult to detect. Given the limited robustness and capacity of traditional methods in the spatial and transform domains, recent research has turned to adaptive embedding strategies based on machine learning, including deep learning, to improve embedding capacity and resistance to steganalysis. This paper presents a survey of representative image steganography techniques, with a brief discussion of traditional methods and a focus on machine learning-based schemes such as convolutional neural networks (CNNs), and generative adversarial networks (GANs). The survey covers 43 research papers published in peer-reviewed journals between 2017 and 2025, and analyzes the main advantages and disadvantages of the mentioned methods from a practical point of view. Furthermore, it discusses existing challenges in imperceptibility, robustness, and security, and identifies possible future research directions for machine learning-based image steganography systems.

1. Introduction

With the rapid growth in digital communications, information security has become extremely important, especially in civilian and military applications. Large volumes of information are passed through unstable or even aggressive networks, which impose great pressure on the confidentiality and safeguarding of information. Two prerequisite data security methods in such a setting are encryption and steganography [1].

Encryption is the process of converting a plaintext message into an encrypted message using encryption keys. This renders any unauthorized user hard to get a copy of the original text. Nevertheless, the fact that the information is encrypted can be a cause of suspicion among attackers who will then decrypt it to get the original information. To address this limitation, steganography has emerged as an art of hidden communication, where the message's existence is concealed by embedding it within a digital medium in a secure, imperceptible manner [2]. The primary

objective of steganography is to secure communication by concealing the message itself, while encryption aims to ensure the confidentiality of content but raises suspicion due to the encrypted data format [3].

Steganography enables invisible communication by embedding secret messages within digital images, video, or audio files. In particular, image steganography has received widespread attention, due to the ease of obtaining digital images and their ability to embed relatively large amounts of confidential data [4]. Figure 1 shows the fundamental structure of an image steganography system.

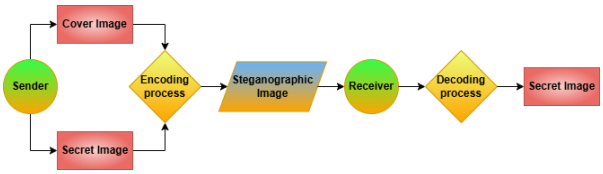

Figure 1. Fundamental structure of an image steganography system.

Despite the good performance of traditional image steganography in both spatial and transform domains, these schemes often suffer from limited robustness to common processing operations such as compression, noise, cropping, and filtering. As a result of these operations, the secret data may be lost or degraded, making it easier to detect. Recent developments in machine learning-based image steganography, particularly deep learning, have led to the emergence of new adaptive techniques that are highly resistant to steganalysis, more flexible in modeling the complex statistical features of digital images, and more efficient at embedding and retrieving confidential data. However, these methods face several challenges, including the need for large training datasets, increased computational complexity, and generalization problems when dealing with data distributions unfamiliar to the steganographic model [5].

This paper introduces the following main contributions:

- It provides a systematic review of image steganography schemes and organizes them into a unified taxonomy based on spatial-domain, transform-domain, and machine-learning-based methods.
- It presents a qualitative comparison of the strengths, weaknesses, and typical application scenarios of representative image steganography techniques within these categories.
- It provides an in-depth review of methods based on machine learning and deep learning, highlighting recent advances, key limitations, remaining research gaps, and corresponding directions for future work.

The rest of the paper is divided as follows: Section 2 describes the search strategy and the categorization method used in the literature review. Section 3 provides a literature review of the image steganography methods. Section 4 gives a qualitative comparison of the pros and cons of representative approaches and their common use. The key research gaps and the existing challenges are discussed in Section 5. Section 6 describes the future research directions. The major findings from this survey are summarized in Section 7.

2. Survey Methodology

This section presents a structured taxonomy of image steganography approaches into three main categories: spatial-domain, transform-domain, and machine-learning-based schemes. Figure 2 shows the taxonomy and representative methods for these categories.

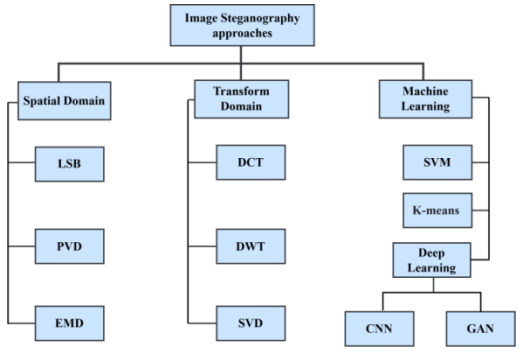

Figure 2. Taxonomy of image steganography approaches.

This paper presents a systematic literature survey, following a sequential search, screening, and inclusion process. Figure 3 also provides an overview of the methodology for selecting studies. Major databases, including IEEE Xplore, SpringerLink, Web of Science, ACM Digital Library, Scopus, and Google Scholar, were searched for peer-reviewed research papers published between 2017 and 2025 in the field of image steganography, using keyword combinations such as image steganography, machine learning, deep learning, convolutional neural networks, and generative adversarial networks. The initial search yielded a general set of studies on steganography; non-image media, such as audio and video, were excluded, research based on theoretical models without empirical verification, and duplicate articles. After examining titles, abstracts, and conclusions, 43 core articles containing empirical results were selected and categorized into three main categories, as shown in Figure 2.

* Corresponding authors: *Department of Computer Science*, *University of Kufa*, *Iraq*
E-mail addresses: yousifh.alsary@student.uokufa.edu.iq (Yousif H. Jasim)

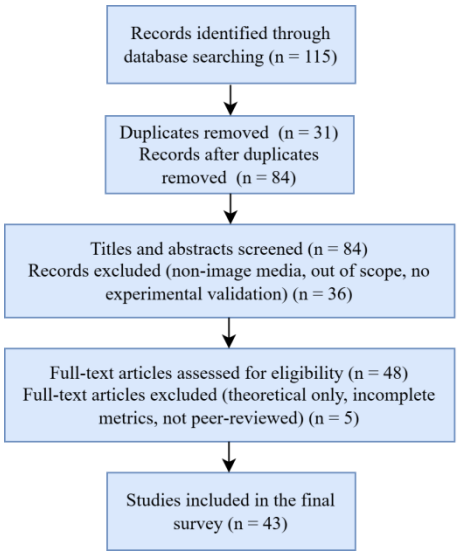

Figure 3. A simplified flow diagram of selecting studies process.

In contrast to generic surveys that address generic concepts (e.g., Luo et al. [4]; Kombrink et al. [5]), the paper under analysis is dealing with machine learning-based image steganography techniques and quantitatively and qualitatively compares them with conventional spatial- and transform-domain methods. In order to make a comparison of the chosen schemes in each category, we noted down the steganographic domain, the algorithm employed, and the strengths and weaknesses of each study. Also, we noted the reported performance statistics, such as structural similarity index measure (SSIM), peak signal-to-noise ratio (PSNR), and payload capacity. As the outcome of the performance depends on varying conditions of evaluation and datasets, quantitative comparisons of the studies are expected to be viewed as trends but not a standard. Tables 3 and 4 give an overview of the schemes used as representatives of each category, which forms an oversimplified basis for the comparative study and the gaps, limitations, and future research directions of image steganography systems.

2.1 **Spatial Domain Techniques**

spatial-domain techniques directly modify pixel values, replacing the lowest bits of the cover image pixels with bits of the hidden data. This maintains a high degree of visual similarity between the cover and stego images. Among these schemes, least significant bit (LSB) substitution and pixel value difference (PVD) are widely used due to their simplicity and ability to provide acceptable embedding capacity. However, these methods are vulnerable to statistical steganalysis and image processing procedures, such as compression and filtering, which compromise the security of the embedded data [6].

2.1.1 ***Least Significant Bit (LSB).*** The LSB technique embeds the secret message by replacing the least significant bits in the pixels of the cover image with their corresponding bits in the secret data. Since modifications in the least significant bit plane do not produce large changes in pixel intensity, the visual quality of the stego image is usually indistinguishable from that of the cover image to the human eye. However, conventional LSB schemes are highly fragile to image-processing operations such as compression, filtering, and noise addition, and they are also vulnerable to statistical steganalysis attacks that exploit the predictable structure of the LSB plane [7][8].

2.1.2 ***Pixel Value Difference (PVD).*** In the PVD method, the secret bits are embedded in the intensity differences between pairs of neighboring pixels. The cover image is partitioned into small, disjoint pixel pairs, and the magnitude of the intensity difference in each pair determines how many secret bits are embeddable according to predetermined ranges matched to human visual sensitivity. The pixel intensities are subsequently adjusted to embed the secret information. However, PVD-based techniques are sensitive to manipulation of pixel intensity and geometry, as pixel differences can be distorted when processing a stego image with common operations such as cropping, filtering, and noise addition, which often leads to the failure of this technology to recover the secret message and makes it vulnerable to detection [9][10].

2.1.3 ***Exploiting Modification Direction (EMD).*** The EMD technique depends on the modification direction (exploiting the modification direction) of a specific number of pixels, increasing, decreasing, or leaving them unchanged, to embed secret data with minimal distortion in the cover image. This method preserves the embedded payload and improves imperceptibility and resistance to simple statistical steganalysis methods compared to LSB-based spatial-domain techniques [11].

2.2 **Transform Domain Techniques**

In transform-domain (e.g., discrete cosine transform (DCT) and discrete wavelet transform (DWT))-based methods, the cover image is transformed into the frequency domain, after which the secret data is hidden in specific transform coefficients. These approaches increase resistance to statistical steganalysis and require

* Corresponding authors: *Department of Computer Science*, *University of Kufa*, *Iraq*
E-mail addresses: yousifh.alsary@student.uokufa.edu.iq (Yousif H. Jasim)

less payload capacity and higher computation complexity than those based on the spatial domain [12].

2.2.1 ***Discrete Cosine Transform (DCT).*** The discrete cosine transform (DCT) converts the cover image from the spatial-domain to the frequency-domain, providing a direct way to embed secret data into specific transform coefficients. In a typical DCT-based scheme, the cover image is divided into a set of non-overlapping blocks (e.g., 8x8), and a two-dimensional DCT is applied to each block. The secret bits are then embedded in the selected DCT coefficients, typically in the highest-frequency coefficients. This method produces high-quality stego images and is highly resistant to compression attacks, such as JPEG [12].

2.2.2 ***Discrete Wavelet Transform (DWT)***. In DWT-based techniques, the cover image is decomposed into four non-overlapping subbands (LL, LH, HL, and HH) according to their spectral content. One or more subbands are selected to hide the secret data depending on the steganography objective. High-frequency subbands (LH, HL, HH) are used to embed information in edge and texture regions, resulting in high-quality stego images with minimal distortion. At the same time, the low-frequency LL subband can improve robustness, as it contains most of the image structural information [13].

2.2.3 ***Singular Value Decomposition (SVD).*** SVD method is used to image steganography to achieve robustness and imperceptibility, where the cover image matrix C (M×N) is analyzed into three submatrices U, S, and V^t as follows:

$$C = USV^t \quad (1)$$

where U and V are orthogonal matrices of dimensions M×M and N×N, respectively, and S is a diagonal M×N matrix whose diagonals contain most of the basic information of the image. Because small changes in secret data can be embedded in these coefficients without significantly degrading image quality. Thus, the capacity, robustness, and imperceptibility of SVD-based steganographic methods are well balanced, albeit at the cost of increased computational complexity compared with spatial-domain techniques [14].

2.3 **Machine Learning-Based Techniques**

In this paper, the standard machine learning methods,

vector machines (SVMs) and K-means clustering. It dwells on deep learning-oriented approaches like convolutional neural networks (CNNs) and generative adversarial networks (GANs) that enhance automatically the hierarchical feature representation and data-driven embedding plans. Both embedding and extraction approaches, learning process, benefits, and shortcomings associated with each chosen technique are reported so that the comparison of machine learning-based schemes could be comprehensive.

2.3.1 ***Support Vector Machine (SVM).*** SVMs are supervised learning models that have been applied to both classification and regression tasks, and have been widely used in various image steganography studies. An SVM seeks a maximum-margin separating hyperplane in an appropriate feature space and can also deal with nonlinearly separable patterns by projecting the input data into higher-dimensional spaces via kernel functions [15]. SVMs have three primary roles in image steganography. First, they can determine which regions of the image (e.g., textured or smooth) are most helpful for choosing message embedding locations in the cover image when the embedded payload is small enough to improve imperceptibility and payload efficiency. Second, steganalysis models using SVMs distinguish the presence of hidden data in an image by classifying an input image as cover or stego using a feature set and have achieved high accuracy in several works. Third, SVMs have been applied to the so-called “hybrid” methods that combine transform-domain features (such as DCT and DWT) and learning-based decision rules for noise robustness, compression tolerance, or other image-processing operations, achieving acceptable visual performance and embedding capacity [16][17].

2.3.2 ***K-means Clustering.*** K-means is an unsupervised clustering algorithm that groups data samples into a predefined number of clusters by minimizing the variance within each cluster. For image steganography, K-means is applied to partition the cover image into clusters of pixels with similar intensity or color values, enabling the identification of coherent cluster structures suitable for data embedding. The secret data are preferentially embedded in positions within these clusters, usually in textured or flat regions insensitive to fine pixel-value adjustments and far from complex or edge-like regions to avoid visual distortion and maintain compatibility between the embedding and extraction clusters. This cluster-based embedding algorithm has been combined with LSB and cryptographic transformations (such as DES) to enhance the quality and security of robust data hiding, thereby providing payload-stable yet independent stego images without requiring access to the original cover for message extraction [18][19].

* Corresponding authors: *Department of Computer Science*, *University of Kufa*, *Iraq*
E-mail addresses: yousifh.alsary@student.uokufa.edu.iq (Yousif H. Jasim)

In summary, classical machine-learning-based image steganography techniques such as SVM and K-means are able to improve adaptive embedding strategies and introduce data-driven robustness mechanisms at low computational cost; however, their reliance on manually designed features limits their ability to capture complex image statistics.

2.3.3 ***Deep Learning (DL).*** Deep learning, a branch of machine learning, learns hierarchical layer-based representations, where simple concepts are combined to form more complex ones. Deep neural networks (DNNs) are the dominant models in deep learning [20]. They are typically implemented as multi-layer extensions of traditional artificial neural networks (ANNs), as illustrated in Figure 4.

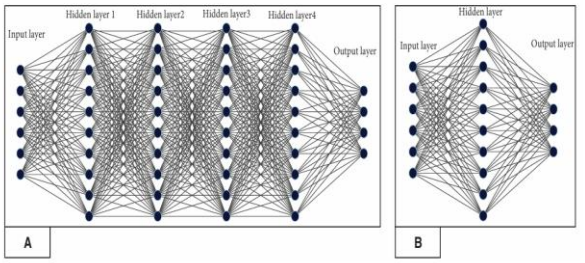

Figure 4. Deep Neural Network (A) and a Shallow Neural Network (B) [20].

Here, the depth of a neural network denotes the number of hidden layers. Greater depth allows models to extract more abstract and distinct features, as the initial signals extracted from the first layers gradually transform into more complex representations towards the output layer. However, deep models typically require large training datasets and higher computational costs due to the significantly increased number of parameters compared to shallower structures. CNN-based and GAN-based models are among the most common deep learning frameworks used in image steganography.

Convolutional Neural Network (CNN):

CNNs are among the most effective deep learning architectures, due to their ability to automatically learn visual features from data without manual feature design. Through successive convolutions and pooling operations, these networks form multi-level feature hierarchies. They gradually transform the intensity of raw pixels into more abstract and meaningful representations. It makes them perform exceptionally well in image recognition and many other computer vision tasks [21].

CNNs are generally applied in an encoder-decoder architecture for image steganography. The encoder network is trained to embed a secret message into a cover image to produce a stego image; the decoder network is trained to accurately restore the secret message contained in the stego image. By jointly training these networks, imperceptibility, embedding capacity, and resistance to steganalysis attacks are optimized simultaneously. Multiple studies claim that these models are better than traditional spatial-domain methods in the sense that they adaptively choose the locations of embedding, and they also retain the statistical characteristics of the original image. The designs of architectures like HiDDeN, SteganoCNN, and U-net-based designs are described as being robust, scalable, and flexible architecturally. Still, CNN-based methods typically need extensive training datasets and huge computing resources and may suffer from overfitting or deep learning-based steganalysis. Nevertheless, CNNs have achieved significant advances in image steganography, thus becoming a cornerstone of many current deep learning-based steganography systems [22]. This is especially true of CNN-based models, which are more popular in more complicated imaging problems, such as medical images and high-resolution landscape images, where detailed spatial patterns and subtle statistical correlations need to be well represented [23]. Nonetheless, they may perform poorly because of bias in the datasets and a restricted range of training, which, in most cases, results in overfitting and decreased resilience when the distribution of application data differs from the distribution of training data [24].

Generative Adversarial Network (GAN):

GANs are deep generative models consisting of two units, a generator and a discriminator, which are trained in a competitive environment. The generator generates fake samples from noise and possibly additional information, while the discriminator distinguishes between real and generated data, forcing the generator to produce images that are indistinguishable from real ones. As shown in Figure 5, this adversarial dynamic produces highly realistic outputs. This high generative capacity has made GANs increasingly popular for image generation, enhancement, and transformation tasks. Therefore, their superior ability to maintain complex image statistics makes adversarial generative networks (GANs) a promising basis for developing secure image steganography systems, which exhibit greater resistance to statistical detection and steganalysis. [25].

In the field of image steganography, GANs can be applied across three classical steganographic strategies. These include modifying an existing cover, selecting a

* Corresponding authors: *Department of Computer Science*, *University of Kufa*, *Iraq*
E-mail addresses: yousifh.alsary@student.uokufa.edu.iq (Yousif H. Jasim)

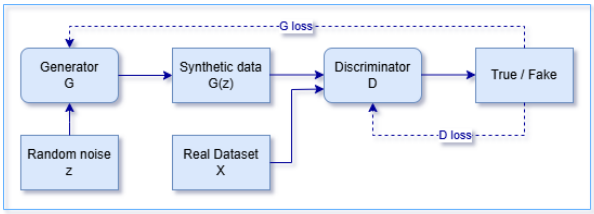

Figure 5. The general structure of a GAN [25].

suitable cover, or synthesizing a new stego cover. For the modification strategy, GAN-based models may learn adaptive distortion or probability maps that determine pixel or coefficient changes for data-driven embedding, thereby more closely preserving natural image statistics. In the case of cover selection and especially cover synthesis, several studies have shown that GAN generators can produce stego images whose distributions more closely match those of the cover images, thereby improving indistinguishability against the steganalysis tools used in those experiments. This transfers steganography design from hand-crafted distortion functions to automatically learned, data-driven embedding models [26].

GAN-based image steganography continues to suffer the same classic trade-off between imperceptibility, embedding capacity, and robustness. The latest researches have incorporated competitive training as an objective of enhancing these contradictory goals in a coherent system. The evidence that early GAN-based approaches provide is that one can achieve stego images by a generator and a specialized steganalyzer that are both statistically and perceptually similar to the cover images; this benefit is frequently associated with lower embedding capacity and reduced practical flexibility. Newer models, including SteganoGAN and U-Net-based GAN models, propose task-dependent loss functions and explicit decoders to trade off competitive loss and reconstruction error. They also clearly generate perceptual similarity between the cover images and the stego image samples at the distribution level with the induction of perceptual or feature space losses. The schemes can achieve better PSNR and SSIM values than conventional LSB- and DCT-based schemes as a baseline benchmark, although at the cost of reduced steganalysis resistance on benchmark studies [27]. Along with these outstanding achievements, GAN-based models continue to experience significant challenges, including high computational cost, high data requirements, and training instability. These models take advantage of the fact that in complex data spaces, and high-dimensional visual spaces the generator effectively approximates the underlying image distribution and synthesizes stego instances that are nearly indistinguishable in terms of cover images, and thus greatly increases their capacity to deceive in secure communication models. Nevertheless, other phenomena, including mode collapse or sensitivity to training data quality and diversity, remain continue challenges and could make generalization challenging and difficult to apply them reliably in practice [28].

3. Literature Review

This section reviews previous studies and recent developments in image steganography, within a unified classification, and focuses on representative techniques within each category. By examining basic design principles, advantages, and limitations, the review provides a structured basis for the comparative analysis in Section 4.

3.1 Traditional Image Steganography Techniques

The historical basis of steganography in images is traditional methods, which offer the conceptual basis for further development. Such methods are broadly categorized into two broad groups, including spatial-domain and transform-domain methods, with each having a trade-off between embedding capacity, imperceptibility, and resistance to steganalysis. The representative schemes of each of the two categories are discussed in the following, and are summarized in Table 1, which is used in the following section to make the qualitative comparison.

Aziz et al. (2023) compared two schemes of image steganography in grayscale and color images with the LSB technique, where 1 or 4 least significant bits per pixel are altered. The 1-LSB scheme has a good visual quality, and it has a reasonable value of peak signal-to-noise ratio (PSNR) and mean squared error (MSE), offers a simple baseline, and has a moderate embedding capacity. The 4-LSB scheme, on the contrary, attains a significantly larger payload. Nonetheless, causes apparent distortions in the stego image and serious degradation in PSNR and MSE, which supports the essential trade-off between capacity and imperceptibility in LSB image steganography [29].

Vishnu et al. (2020) introduced a scheme of image steganography using the PVD technique, where the Canny edge detector algorithm was used on the image, after which the compressed data was embedded on the detected edges. It is better than simple LSB embedding in that it enhances the size of embedded data and the degree of security without reducing image quality because edge pixels are tolerant of intensity variations. Nevertheless, no other robustness measures than PSNR, MSE, and edge-based payload were given, and no performance in steganalysis was tested [30].

* Corresponding authors: *Department of Computer Science*, *University of Kufa*, *Iraq*
E-mail addresses: yousifh.alsary@student.uokufa.edu.iq (Yousif H. Jasim)

Kaur and Singh (2021) suggested a hybrid image steganography method that integrates DCT with a chaotic map. The secret data are embedded into high-frequency DCT coefficients, thereby largely preserving the visual quality of the cover image. At the same time, a novel dual chaotic map (CCM) is used to randomly select embedding positions in the DCT domain. Experimental findings show that the proposed scheme is resistant to steganalysis and yields high-quality stego images [31].

Fajih and Mahsa (2022) suggested a two-stage DWT-domain steganography scheme in which two secret bits are first embedded into adjacent DWT coefficients using an XOR operator. A genetic algorithm is then employed to optimize these modified coefficients, thereby reducing distortions in the stego image and yielding stego images with superior visual quality and enhanced robustness. Short embedding and extraction keys are further utilized in the method to provide a more secure yet simple implementation process [32].

Khandelwal et al. (2022) presented a DWT–SVD steganography system that embeds the grayscale secret and cover images using a threshold-based scrambling and encryption mechanism. The secret image is then partitioned into three sub-images using pixel thresholds and rearranged according to a code rule. It is embedded into the DWT domain via SVD and further boosted by a pixel-permutation technique. The outcomes of the digital image processing experiments demonstrate that the proposed algorithm achieves a relatively high degree of imperceptibility and accurately restores secret images for high-contrast images. It also yields higher

Table 1. Summary of representative classical image steganography methods in the spatial and transform domains.

Ref	Domain / Technique	Algorithm	Advantages	Challenges	Evaluation metrics / results
[29]	Spatial / LSB-based	1-LSB and 4-LSB substitution with XOR-based secret key stream	Very simple; supports color and grayscale images; 1-LSB yields acceptable PSNR and minimal visual distortion.	4-LSB causes noticeable distortion and low PSNR; evaluation is based mainly on MSE/PSNR and histogram analysis.	bpp: not reported; PSNR: 42.7 dB (1-LSB) and 29.3 dB (4-LSB); SSIM: not reported
[30]	Spatial / PVD-based	PVD + Canny edge detection	Higher embedding capacity than basic LSB, with improved security in edge regions.	PVD degrades image quality compared with LSB; added complexity from edge detection and block processing.	bpp: not available; PSNR: not reported (only qualitative claim of quality vs. LSB reported in text); SSIM: not reported.
[31]	Transform / DCT-based	DCT with Chaotic map	High embedding capacity; good perceptual quality; zero BER at maximum payload high security.	Higher computational complexity than simple spatial methods; focuses on grayscale test images.	bpp: not reported; PSNR: 32.99 dB (Lena), 31.20 dB (Baboon), 32.74 dB (Airplane), 32.08 dB (Boat), 33.04 dB (Pepper); SSIM: acceptable.
[32]	Transform / DWT-based	DWT + XOR	High visual quality; better than DCT-based methods at low and high payloads; shows reduced SPAM detection accuracy.	More complex than basic spatial methods; capacity–security trade-off remains (security decreases at highest payload).	bpp: not reported; PSNR: around 52–53 dB at low capacity and 51 dB at higher capacity; SSIM: 0.998 at high capacity on standard test images.
[33]	Transform / SVD-based	SVD + DWT with threshold-based scrambling of the secret image	High imperceptibility; secret and stego images visually indistinguishable from originals; security better than plain DWT/DCT methods.	Capacity depends on α (higher capacity lowers PSNR); the scheme is relatively complex.	bpp: not reported; PSNR: 37.7–54.1 dB; SSIM: up to 1.0 depending on α and image.

* Corresponding authors: *Department of Computer Science*, *University of Kufa*, *Iraq*
E-mail addresses: yousifh.alsary@student.uokufa.edu.iq (Yousif H. Jasim)

PSNR and MSE than previous DWT- and DCT-based schemes on standard grayscale test images, albeit without comparison to current deep-learning-based steganalysis [33].

The main characteristics of the reviewed traditional steganography methods are summarized in Table 1, including the technique used, the algorithm employed, their main advantages and limitations, and the evaluation metrics. However, as will be discussed in Section 5, these traditional methods in the spatial and transform domains still show notable weaknesses under realistic distortions and practical deployment constraints.

3.2 **Machine Learning-based Techniques**

In this subsection, we provide a brief review of the literature on machine-learning-based image steganography methods, including classical models such as SVMs and K-means, as well as deep architectures based on CNNs and GANs.The focus is on representative schemes that demonstrate how data-driven models can improve adaptive embedding strategies, payload-distortion trade-offs, and robustness against steganalysis. The main characteristics of these techniques are summarized in Table 2, which supports the subsequent comparative Analysis.

3.2.1 ***Classical machine-learning-based methods.*** In this subsection, conventional machine-learning-based image steganography models that rely on manually designed features and traditional classifiers are described.

As a steganography technique, Hussein et al. (2023) introduced SVM-Steg that uses SVMs to distinguish between secret and cover data and provide perceptually significant areas in which secret data can be embedded on the cover image. The suggested scheme improves the capacityquality trade off and attains PSNRs that are over 40 dB in different image classes. It is also capable of high payload and stego-image quality as opposed to classical LSB-based methods [34].

Chowdhuri et al. (2023) came up with a hybrid image steganography system, which combines support vector machines (SVMs) and the integer wavelet transform (IWT) to strengthen the robustness, security, and integrity of medical images in classification data. SVMs are utilized to differentiate between the important regions and unimportant regions in the breast magnetic resonance images, whereas IWT is utilized to transform the unimportant regions into an area that can be securely embedded. SVM has a higher predictive performance than Naive Bayes and KNN classifiers, which leads to stego images that are visually indistinguishable, and to images that are resistant to Gaussian and salt-and-pepper noise, as well as JPEG compression. The method has an average SSIM of 0.9802, PSNR of 64 dB, and a payload of 0.44 bpp at a comparatively high initial computational cost [15].

A method of embedding secret messages in a grayscale cover image using K-means clustering was proposed by the authors of Kich et al. (2017). Under this method, the cover image is divided into clusters, and these clusters are divided into smooth and complex regions. Adaptation is then done to incorporate the secret data in the smooth areas through an LSB method to make it visually undetectable. There is an adaptive threshold that regulates the number of bits per pixel. The method allows a flexible and quite high payload, without degrading the perceptual quality of the stego image [18].

Shetty et al. (2020) suggested a method of image steganography, which integrates the use of K-means clustering and DES encryption to improve the security of hidden information in color images. In which a color cover image is initially segmented into clusters by the K-means algorithm, and then the secret message is encrypted by DES before being coded using LSB into clusters. The authors cited that the approach was relatively high in payloads and acceptable quality of visualization. Nonetheless, the experimental analysis can be described as very qualitative and is not a full systematic measure of either image quality or steganalysis robustness measures [19].

3.2.2 ***Deep learning-based techniques.*** This subsection reviews image steganography schemes based on CNNs and GANs.

The paper by Subramanian et al. (2021) presents a lightweight end-to-end image steganography system based on a deep convolutional auto-encoder. It conceals a complete secret image inside a cover image and then recovers it from the corresponding stego image. The system architecture includes preprocessing, embedding, and extraction networks and is trained and assessed using ImageNet, CelebA, and COCO datasets. As per experimental outcomes, this technique yields better PSNR, embedding capacity (up to 24 bits per pixel), and imperceptibility than conventional LSB-based and DCT-based methods, and some baseline deep learning schemes [35].

Xintao et al. (2020) constructed a convolutional neural network, SteganoCNN, that can embed two secret images into one cover image and retrieve them from the stego image through extensive training. The network design is the dual branching of an encoder-decoder and separate extraction networks that are developed to extract and conceal two secrets of the cover image automatically. Their work reported experimental results of high quality stego images with a payload of up to 47.92 bits per pixel and very low detection rates by the steganalyzers taken into account in their study. Generalization was also promising in the

model when evaluated on other datasets, including remote sensing and aerial images [36].

Sriram and Havaldar (2023) developed a CNN-based system to hide a secret image within a cover image and to extract it via a steganalysis-based processing path, thereby reconstructing the secret image. The two processes are performed simultaneously through training, resulting in improved information concealment and extraction. The system was evaluated using PSNR and the structural correlation coefficient (SCC). The results showed significant improvements in security, greater flexibility, and interpretability over the baseline traditional and deep-learning-based image steganography techniques considered in their experiments, providing improvements in both visual quality and robustness [37].

Shahnawaz et al. (2024) suggested a hybrid method combining a CNN and a DCT to hide confidential data in a cloud-stored image. First, a CNN is used to learn features of optimal embedding sites. This is followed by DCT-based embedding of the confidential data to achieve imperceptibility. The experimental evaluation indicates that the proposed technique is highly robust against steganalysis attacks, has a low retrieval error (0.028), an MSE of 112, and an execution time of 2.3 seconds, thus meeting the requirements of cloud computing [38].

Schner and Gunay (2024) proposed an improved U-Net-based model for hiding a color secret image inside a cover image, with both images having a resolution of 256×256 pixels. Batch normalization and residual blocks were incorporated into the model, and the network is trained with the AdamW optimizer using a one-cycle learning rate schedule. Test results on ImageNet, LFW, and Linnaeus 5 datasets showed that the model has higher stego quality and embedding capacity than traditional and deep-learning-based methods, thus enhancing information security [39].

Kubusame et al. (2020) proposed an enhanced image steganography scheme that employs adversarial training with a CycleGAN to generate high-quality stego images. The generator is trained to hide the secret message in a form that is difficult for the discriminator to distinguish, thereby improving both concealment quality and retrieval accuracy. Experiments on the USC-SIPI dataset showed that the proposed method achieves high PSNR and SSIM values and lower detection rates than the traditional baselines for image steganography considered in their study, indicating an improvement in robustness under the assessment conditions used there [40].

Zhao et al. (2022) introduced AFHS-GAN, a deep frequency-domain steganography network that builds on SteganoGAN and augments it with an adaptive frequency-domain channel attention network (AFcaNet) and a low-frequency loss function. Tests were conducted on the DIV2K dataset, and the results showed improvements in embedding capacity, steganography quality, and generalization compared with the SteganoGAN baseline under the authors' experimental settings [41].

Ramandi et al. (2024) proposed a deep spatial steganography framework, VidaGAN (Variable Adaptive GAN), that uses an encoder–decoder–critic GAN for embedding binary data into images. The system learns richer feature maps to balance embedding capacity and transparency, thus enhancing both PSNR and SSIM for the stego images. Testing on the DIV2K dataset showed that the 4 bits per pixel configuration outperformed the comparison methods in terms of distortion and visual quality. Moreover, the proposed model achieved a peak hiding capacity of 3.9 bpp on DIV2K and, by StegExpose analysis, an AUC of approximately 0.6, which the authors regard as an acceptable trade-off for transparency and robustness [42].

Polisity and Rizvi (2025) designed a GAN-based image steganography model that enhances the embedded data payload, stego-image visual quality, and resistance to steganalysis. The architecture follows an encoder–decoder–discriminator design and incorporates a custom loss that jointly optimizes competitive learning, imperceptibility, and embedding efficiency. Tests were conducted on both the COCO and ImageNet datasets, and the results showed high PSNR and SSIM values, as well as greater robustness against compression, distortion, and clipping, compared with traditional LSB- and DCT-based methods [43].

4. Comparative Analysis

Table 3 provides an overview of the main strengths and weaknesses, as well as typical application domains, of the image steganography schemes reviewed in this paper, which include spatial-domain, transform-domain, and machine-learning-based techniques. The table thus extends the information in Tables 1 and 2 by summarising the characteristics of each method into higher-level design trade-offs to consider when selecting appropriate techniques for specific applications and adversarial environments. Therefore, the quantitative indicators in Tables 1 and 2, such as PSNR, SSIM, and payload, should be interpreted as indicators of general trends in the traditional trade-offs between capacity, imperceptibility, and robustness within each category of methods, rather than as strict rankings between research papers, because the underlying studies rely on heterogeneous datasets and

* Corresponding authors: *Department of Computer Science*, *University of Kufa*, *Iraq*
E-mail addresses: yousifh.alsary@student.uokufa.edu.iq (Yousif H. Jasim)

Table 2. Comparative summary of ML- and DL-based image steganography methods.

Ref	Domain / Technique	Algorithm	Advantages	Challenges	Evaluation metrics / results
[34]	ML / SVM-based	SVM + DCT + RGB LSB	High imperceptibility, good payload capacity, and reasonable hiding speed.	Depends on classical SVM and hand-crafted DCT features; limited testing on diverse images and attacks.	bpp: not reported; PSNR: 44.31 dB; SSIM: not reported.
[15]	ML / SVM-based	SVM + KNN + IWT	High imperceptibility and robustness against noise and JPEG compression; better prediction performance.	High computational complexity; evaluated only on MR images.	bpp: 0.44; PSNR: 64 dB; SSIM: 0.9802.
[18]	ML / K-means clustering-based	K-means clustering + LSB	High stego-image quality with imperceptible distortion and good embedding capacity.	Limited to grayscale images and K-means clustering.	bpp: 3; PSNR: 38.68 dB; SSIM: not reported.
[19]	ML / K-means clustering-based	K-means clustering + DES-based data hiding in RGB segments	Supports a wide range of image formats without prior conversion; maximizes embedding capacity; enhances security.	Potential complexity due to clustering and encryption and possible sensitivity to image content.	bpp: not reported; PSNR: not reported; SSIM: not reported.
[35]	DL / CNN-based	Deep convolutional autoencoder with preprocessing, embedding, and extraction networks	High embedding capacity, strong security and robustness, and high imperceptibility with stego images visually close to covers.	Requires training on large datasets and depends on deep model complexity and parameter tuning.	bpp: not reported; PSNR: not reported; SSIM: not reported.
[36]	DL / CNN-based	SteganoCNN	Very high payload (two images; up to 47.92 bpp), low visual distortion, resistance to steganalysis, and good generalization to remote-sensing and aerial images.	Model complexity and large number of parameters; need for pruning and optimization for faster hiding/extraction and deployment on mobile devices.	bpp: 47.92; average PSNR: 28.56 dB; SSIM: 0.921.
[37]	DL / CNN-based	CNN with hiding network and extraction network	Compact and simple end-to-end design; high payload with strong confidentiality and robustness; high imperceptibility.	Requires CNN training and computational resources; evaluation limited to PSNR, UQI, and SCC without broader robustness analysis.	PSNR: 65.67 dB; SSIM: not reported.
[38]	DL / CNN-based	CNN + DCT	High embedding capacity; good visual fidelity; high security; accurate data retrieval; robustness to common transforms.	Increased complexity; robustness and performance depend on model and parameter choices.	bpp: 0.45; PSNR: not reported; SSIM: not reported.
[39]	DL / CNN-based	Enhanced U-Net with batch normalization and residual blocks	High imperceptibility and reconstruction quality across datasets, with robust performance and good generalization to complex backgrounds.	High computational and hardware requirements, with performance limitations on low-end systems and a need for further optimization.	bpp: 24; PSNR: 44.46 dB; SSIM: 0.9827.
[40]	DL / GAN-based	Modified CycleGAN with discriminator-guided embedding	Improved PSNR and visual quality over prior methods; higher robustness and payload capacity.	Risk of overtraining and need for further optimization to enhance capacity and robustness.	bpp: not reported; average PSNR: 61.03 dB; SSIM: not reported.
[41]	DL / GAN-based	AFHS-GAN: SteganoGAN enhanced with AFcaNet and a low-frequency loss in the DCT domain	Increases maximum payload by about 1.8 bpp over SteganoGAN while improving stego-image quality and generalization on DIV2K.	More complex architecture and reliance on frequency-domain processing and specialized loss design.	bpp: 24; PSNR: 36.64 dB; SSIM: not reported.
[42]	DL / GAN-based	VidaGAN with encoder–decoder–critic architecture	High visual quality (PSNR/SSIM) with high resistance to steganalysis (StegExpose AUC of about 0.6).	Limited robustness to JPEG, cropping, and noise; extraction phase less efficient.	bpp: 3.9 on DIV2K; PSNR: 38.56 dB; SSIM: 0.884.
[43]	DL / GAN-based	GAN encoder–decoder–discriminator with custom loss	Balances payload, visual imperceptibility, and robustness, while enabling realistic stego images with reliable recovery under compression, noise, and cropping.	Increased model and training complexity; requires large-scale datasets and careful loss tuning; computationally demanding for high-resolution images.	bpp: 24; PSNR: 40 dB; SSIM: 0.98.

Table 3. Summary of advantages, limitations, and typical applications of spatial-, transform-, and ML/DL-based image steganography techniques.

Ref	Domain / Techniques	Pros	Cons	Typical Application
[29, 30]	Spatial – LSB, PVD	Simple implementation, fast execution, and relatively high embedding capacity with acceptable quality.	Highly vulnerable to compression, noise, and statistical steganalysis, especially in high-threat settings.	Simple, low-risk scenarios and general-purpose image data hiding.
[31–33]	Transform – DCT, DWT, SVD	Better robustness to compression and noise, good visual quality, and support for compressed imagery.	Lower payload than spatial methods and higher computational complexity; may be sensitive to some post-processing.	Photographic and compressed images, satellite and medical imaging, and robust image hiding.
[34,15, 18,19]	Classical ML – SVM, K-means-based	Exploit manually designed features to adaptively select embedding regions or clusters; work reasonably well with limited training data.	Depend on manual feature design and may generalize poorly beyond the training distribution; added complexity from clustering and classifiers.	Region-based embedding and medical or structured-image steganography.
[35–39]	Deep learning – CNN-based	Automatic feature learning and, in many reported studies, high embedding capacity with strong visual imperceptibility under end-to-end training.	Require large datasets, high computational resources, and careful hyperparameter tuning.	High-capacity image hiding, cloud and multimedia security applications.
[40–43]	Deep learning – GAN-based	Content-adaptive embedding and visually realistic stego images, with reported improvements in resistance to recent steganalysis methods under specific settings.	Architecturally complex, difficult to train, and computationally expensive to deploy at scale.	Multimedia communication and advanced anti-detection image steganography.

evaluation protocols. Therefore, the comparative analysis in this section is primarily qualitative.

In summary, the entries in Table 3 confirm the common trade-offs between spatial-domain and transform-domain methods. Spatial approaches provide higher payload capacity with simpler implementation, whereas transform-domain methods prioritize robustness and visual image quality at the cost of higher complexity and lower payload.

Table 2 summarizes the machine-learning-based approaches discussed in detail, whereas Table 3 provides a domain-level overview that contrasts traditional methods with classical ML and deep learning models. Classical ML methods, such as SVM- or K-means-based schemes that rely on manually designed features and use clustering or classification to adaptively select embedding regions or clusters in structured contexts (e.g., medical imaging), often achieve good performance but still offer limited imperceptibility and payload capacity and remain sensitive to feature design and domain shift.

In structured medical imaging scenarios, for example, machine-learning-based steganography has been applied to breast MR images, achieving relatively high payloads and strong imperceptibility while maintaining diagnostic image quality. Deep-learning-based techniques, such as CNN- and GAN-based architectures, learn hierarchical feature representations directly from data and, in many reported studies, support high-capacity end-to-end embedding with strong visual imperceptibility and competitive robustness to common attacks on the evaluated datasets. However, these methods typically depend on large and diverse training datasets, involve complex hyperparameter tuning, and incur substantial computational cost. Accordingly, no universally best technique, and the choice of a suitable steganographic method should be driven by the requirements of the target application and its threat model, taking into account embedding capacity, perceptual quality, robustness, and implementation complexity.

5. Research Gaps and Challenges

As discussed in Sections 3 and 4, spatial-, transform-, and machine-learning-based image steganography methods have achieved notable progress; however, several gaps still remain that hinder their practical deployment in adversarial environments. Current widely available techniques, particularly spatial- domain schemes such as LSB and PVD, still exhibit poor robustness against modern steganalysis, especially in the presence of realistic distortions such as lossy compression, noise, filtering, and platform-dependent post-processing. In addition, the inherent trade-off among capacity, security, and imperceptibility has not yet been optimally addressed for a wide variety of application scenarios.

Approaches based on machine learning are still subject to generalization issues. Although such methods can reach high PSNR and SSIM values and high

* Corresponding authors: *Department of Computer Science*, *University of Kufa*, *Iraq*
E-mail addresses: yousifh.alsary@student.uokufa.edu.iq (Yousif H. Jasim)

detection-resistance scores on selected test (benchmark) datasets, they tend to fail when used on real-world images, not seen during training. In addition, GAN- and CNN-based architectures often require large annotated datasets, time-intensive training, and large computing resources; they are thus less applicable to resource-constrained systems like the Internet of Things (IoT) and edge devices. The heterogeneity of datasets and evaluation protocols adds further complexity to a fair comparison by the standardized benchmarks. Also, the widespread use of unified performance metrics remains limited, which makes it difficult to make a fair comparison between different studies. Moreover, practical aspects of deployment are not well covered by most of the applied work, such as end-to-end latency, energy consumption, platform-specific constraints (e.g., social networks and cloud services), and privacy and ethical concerns. All these are essential in changing the progress in algorithms to strong, reliable, and practically implementable image steganography systems.

The effects of such restrictions are magnified in complicated data surroundings, e.g., medical or surveillance imagery, an assortment of photographs, and social-media streams, which are typified by a strong variability in the practices of acquiring data, display resolution, and statistical characteristics. In this case, CNN- and GAN-based image steganography models that are competitive on benchmark realities can have diminished security or reduced payload capacity when subjected to unseen data distributions, domain shifts, or adversarial steganalysis, indicating the necessity of more robust and generalizable designs.

From a method-specific perspective, traditional spatial-domain techniques, such as LSB and PVD, remain highly sensitive to standard image processing operations, including lossy compression, noise addition, and filtering, which can severely impair data recovery and render them impractical in hostile or high-risk environments [29,30]. DCT-, DWT-, or SVD-based transform domain schemes achieve improved robustness and visual quality, but at the cost of reduced capacity and increased computational complexity, limiting their suitability for high-throughput systems or real-time applications [31-33]. Traditional machine learning models, such as SVM- and K-means-based techniques, rely on manually designed features, making them susceptible to domain shift when applied to images whose statistical properties are not sufficiently covered during training [15,18,19,34]. Some of these limitations can be mitigated by using deep CNNs and GANs, which learn features in a data-driven manner and support adaptive content embedding. However, new challenges emerge, including the need for large amounts of data, instability in training, limited interpretability, and deployment complexities on platforms with limited computational capabilities [35-43].

6. Future Directions

In light of the gaps and research challenges outlined in the previous section, several important research directions should be focused on to develop machine learning-based image steganography systems, especially deep learning, as follows:

One of the most important priorities is to develop more robust and adaptable embedding strategies that remain secure even when confronted with advanced machine-learning-based steganalysis across complex, diverse real-world environments. In this context, robustness-oriented design should be linked to realistic deployment scenarios by integrating secure embedding into tangible infrastructures, such as medical picture archiving and communication systems (PACS), smart monitoring systems, and content delivery platforms, and measuring their impact on diagnostic accuracy, response speed, and communication cost.

The second priority is to create lightweight efficient architectures using methods(e.g, pruning, quantization, and knowledge distillation) to make them deployable on the IoT devices, on mobile platforms, and in other resource-constrained environments. Such designs are needed to facilitate CNN- and GAN-based image steganography on cameras, embedded sensors, and edge gateways with a limited wall power to execute a full deep learning model.

Among the necessary trends is the standardisation of evaluation criteria, such as multi-domain datasets and a single set of performance measures (such as PSNR, SSIM, payload capacity, computational complexity, and area under the curve in steganalysis), so that comparisons can be made across studies under different domains.

Furthermore, the generalizability of image steganography schemes on a variety of datasets could be enhanced with the help of domain adaptation, transfer learning, self-supervised learning, and semi-supervised learning in order to make these models more resistant to image statistics variations. As an illustration, an encoder-decoder technique of image steganography can be pre-trained on high-volume natural image data sets, and then re-trained or fine-tuned to more specific datasets like medical images or surveillance images, which mitigates the effects of dataset bias and improves their capacity to adjust to domain changes.

Lastly, more studies are necessary on the real-life integration of the security, legal, and ethical looks, to aid the social media, smart environments, surveillance

* Corresponding authors: *Department of Computer Science*, *University of Kufa*, *Iraq*
E-mail addresses: yousifh.alsary@student.uokufa.edu.iq (Yousif H. Jasim)

systems, and cloud services, and to translate the advances of algorithms into secure, practical, and flexible image steganography plans. The early research on ML-based image steganography of clinical images (e.g., breast magnetic resonance imaging datasets) in a setting with strict security, legal, and ethical protocols suggests that secure embedding can be integrated into the diagnostic process. Nonetheless, more systematic studies are required to enhance resilience to attacks and to solve the regulatory and ethical limitations of patient data.

7. Conclusion

This paper presents a systematic survey of image steganography, based on a unified classification that includes spatial, transform, and machine-learning-based techniques. It also conducts a qualitative analysis of these methods, supported by quantitative comparisons. Traditional spatial and transform-based methods, such as LSB, PVD, DCT, DWT, and SVD, are characterized by their simplicity and ease of implementation, but their performance is mediocre when tuned to specific conditions and environments. However, these techniques are not robust enough to counter modern steganalysis techniques, nor do they achieve an optimal balance between imperceptibility, payload, and robustness in practical applications.

By contrast, machine-learned schemes, such as SVM and K-means, and deep-learned techniques based on CNNs and GANs provide more flexible data-driven embedding schemes that trade-offs imperceptibility, payload capacity, and robustness. Nevertheless, they have other issues that include the computational cost, data requirements, model generalization, and unstandardized evaluation measures. Through a systematic review of the literature, unified classification, summary tables, and a discussion of the strengths, weaknesses, and the general field of application, the survey paper revealed the significant open issues, gaps, and directions to follow in future research. The solutions to these problems using enhanced learning methods, typical standard criteria, and deployment-conscious design will play an important role in building security, imperceptible, and high-capacity image steganography systems, compatible enough to deploy through the use of current communication infrastructure.

References

[1] A. Arya and S. Soni, "A literature review on various recent steganography techniques," International Journal on Future Revolution in Computer Science & Communication Engineering, vol. 4, no. 1, pp. 143-149, 2018.

[2] S. K. Powar, H. T. Dinde, and R. M. Patil, "A study and literature review on various image steganography techniques," 2020.

[3] W. Luo, K. Wei, Q. Li, M. Ye, S. Tan, W. Tang, and J. Huang, "A Comprehensive Survey of Digital Image Steganography and Steganalysis," APSIPA Transactions on Signal and Information Processing, vol. 13, no. 1, 2024.

[4] S. Rahman, J. Uddin, M. Zakarya, H. Hussain, A. A. Khan, A. Ahmed, and M. Haleem, "A comprehensive study of digital image steganographic techniques," IEEE Access, vol. 11, pp. 6770-6791, 2023.

[5] M. H. Kombrink, Z. J. M. H. Geradts, and M. Worring, "Image steganography approaches and their detection strategies: A survey," ACM Computing Surveys, vol. 57, no. 2, pp. 1-40, 2024.

[6] R. Selvamani and Y. Yusoff, "Effectiveness of the Spatial Domain Techniques in Digital Image Steganography," Qubahan Academic Journal, vol. 4, no. 1, pp. 341-350, 2024.

[7] R. Selvamani, Y. Yusoff, R. Alwee, S. M. Yusuf, Z. M. Yunos, M. S. Talib, and H. Hasan, "Comparative analysis of the spatial domain in digital image steganography," 2023.

[8] A. Ahmed and A. Ahmed, "A secure image steganography using LSB and double XOR operations," International Journal of Computer Science and Network Security, vol. 20, no. 5, pp. 139-144, 2020.

[9] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, "Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research," Neurocomputing, vol. 335, pp. 299-326, 2019.

[10] O. Alade, E. Amusan, O. Adedeji, and O. Alo, "Image Steganography Using Pixel Value Differencing (PVD) Technique Based on Firefly Algorithm," Journal of Scientific Research & Reports, vol. 27, no. 7, pp. 80-86, 2021.

[11] M. Hussain, A. W. A. Wahab, Y. I. B. Idris, A. T. Ho, and K. H. Jung, "Image steganography in spatial domain: A survey," Signal Processing: Image Communication, vol. 65, pp. 46-66, 2018.

[12] D. Laishram and T. Tuithung, "A survey on digital image steganography: current trends and challenges," Proceedings of 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT), pp. 26-27, May 2018.

[13] M. K. Oudah, A. N. Abed, R. S. Khudhair, and S. M. Kaleefah, "Improvement of image steganography using discrete wavelet transform," Engineering and Technology Journal, vol. 38, no. 1A, pp. 83-87, 2020.

[14] B. Lakshmi Sirisha, "Image steganography based on SVD and DWT techniques," Journal of Discrete Mathematical Sciences and Cryptography, vol. 23, no. 3, pp. 779-786, 2020.

[15] P. Chowdhuri, P. Pal, and T. Si, "A novel steganographic technique for medical image using SVM and IWT," Multimedia Tools and Applications, vol. 82, no. 13, pp. 20497-20516, 2023.

* Corresponding authors: *Department of Computer Science*, *University of Kufa*, *Iraq*
E-mail addresses: yousifh.alsary@student.uokufa.edu.iq (Yousif H. Jasim)

[16] S. Deepa and R. Umarani, "Steganalysis on Images using SVM with Selected Hybrid Features of Gini Index Feature Selection Algorithm," International Journal of Advanced Research in Computer Science, vol. 8, no. 5, 2017.

[17] A. AbdelQader, "A novel image steganography approach using multi-layers DCT features based on support vector machine classifier," The International Journal of Multimedia & Its Applications (IJMA), vol. 9, 2017.

[18] I. Kich, E. B. Ameur, and A. Souhar, "New Image Steganography Method Based on K-means Clustering," Proceedings of the 2nd International Conference on Big Data, Cloud and Applications, pp. 1-6, March 2017.

[19] S. S. Shetty, K. Athmaranjan, S. D. R. Shambhavi, and S. R. Shetty, "Image Steganography Using K-Means and DES Algorithm," IJRESM International Journal of Research in Engineering, Science and Management, vol. 3, 2020.

[20] M. Yedroudj, "Steganalysis and steganography by deep learning," Doctoral dissertation, Université Montpellier, 2019.

[21] J. Gu, Z. Wang, J. Kuen, L. Ma, A. Shahroudy, B. Shuai, T. Chen, "Recent advances in convolutional neural networks," Pattern Recognition, vol. 77, pp. 354-377, 2018.

[22] L. Alzubaidi, J. Zhang, A. J. Humaidi, A. Al-Dujaili, Y. Duan, O. Al-Shamma, L. Farhan, "Review of deep learning: concepts, CNN architectures, challenges, applications, future directions," Journal of Big Data, vol. 8, pp. 1-74, 2021.

[23] H. Saidi, O. Tibermacine, and A. Elhadad, "High-capacity data hiding for medical images based on the mask-RCNN model," Scientific Reports, vol. 14, no. 1, p. 7166, 2024.

[24] O. A. Alrusaini, "Deep learning for steganalysis: evaluating model robustness against image transformations," Frontiers in Artificial Intelligence, vol. 8, p. 1532895, 2025.

[25] J. Liu, Y. Ke, Z. Zhang, Y. Lei, J. Li, M. Zhang, and X. Yang, "Recent advances of image steganography with generative adversarial networks," IEEE Access, vol. 8, pp. 60575-60597, 2020.

[26] B. Sun, "Methodology and application of GAN algorithms," International Conference on Computer Graphics, Artificial Intelligence, and Data Processing (ICCAID 2021), vol. 12168, pp. 663-668, SPIE, March 2022.

[27] W. Rehman, "A novel approach to image steganography using generative adversarial networks," arXiv preprint arXiv:2412.00094, 2024.

[28] J. Zhao and S. Wang, "A stable GAN for image steganography with multi-order feature fusion," Neural Computing and Applications, vol. 34, no. 18, pp. 16073-16088, 2022.

[29] S. A. Jebur, A. K. Nawar, L. E. Kadhim, and M. M. Jahefer, "Hiding Information in Digital Images Using LSB Steganography Technique," International Journal of Interactive Mobile Technologies, vol. 17, no. 7, 2023.

[30] B. Vishnu, L. V. Namboothiri, and S. R. Sajeesh, "Enhanced image steganography with PVD and edge detection," Fourth International Conference on Computing Methodologies and Communication (ICCMC), pp. 827-832, IEEE, March 2020.

[31] R. Kaur and B. Singh, "A hybrid algorithm for robust image steganography," Multidimensional Systems and Signal Processing, vol. 32, pp. 1-23, 2021.

[32] V. Sabeti and M. Amerehei, "Secure and Imperceptible Image Steganography in Discrete Wavelet Transform Using the XOR Logical Function and Genetic Algorithm," ISeCure, vol. 14, no. 2, 2022.

[33] J. Khandelwal, V. K. Sharma, D. Singh, and A. Zaguia, "Dwt-svd based image steganography using threshold value encryption method," Computers, Materials & Continua, vol. 72, no. 2, 2022.

[34] H. S. Hussain, F. Ghazali, H. M. Ali, A. Sangodiah, and K. K. Oumar, "A New SVM-STEG Embedding Model in Steganography," IEEE 8th International Conference On Software Engineering and Computer Systems (ICSECS), pp. 336-341, IEEE, August 2023.

[35] N. Subramanian, I. Cheheb, O. Elharrouss, S. Al-Maadeed, and A. Bouridane, "End-to-end image steganography using deep convolutional autoencoders," IEEE Access, vol. 9, pp. 135585-135593, 2021.

[36] X. Duan, N. Liu, M. Gou, W. Wang, and C. Qin, "SteganoCNN: Image steganography with generalization ability based on convolutional neural network," Entropy, vol. 22, no. 10, p. 1140, 2020.

[37] Sriram K. V and R. H. Havaldar, "Convolutional Neural Network Based Data Security in Image Steganography," SSRG International Journal of Electrical and Electronics Engineering, vol. 10, no. 7, pp. 102-109, 2023.

[38] S. Ahmad, J. O. Ogala, F. Ikpotokin, M. Arif, J. Ahmad, and S. Mehfuz, "Enhanced CNN-DCT Steganography: Deep Learning-Based Image Steganography Over Cloud," SN Computer Science, vol. 5, no. 4, p. 408, 2024.

[39] D. Şener and S. Güney, "Enhancing Steganography in 256×256 Colored Images with U-Net: A Study on PSNR and SSIM Metrics with Variable-Sized Hidden Images," Review of Computer Engineering Studies, vol. 11, no. 2, 2024.

[40] P. G. Kuppusamy, K. C. Ramya, S. S. Rani, M. Sivaram, and V. Dhasarathan, "A novel approach based on modified cycle generative adversarial networks for image steganography," Scalable Computing: Practice and Experience, vol. 21, no. 1, pp. 63-72, 2020.

[41] S. Zhang, H. Li, L. Li, J. Lu, and Z. Zuo, "A high-capacity steganography algorithm based on adaptive frequency channel attention networks," Sensors, vol. 22, no. 20, p. 7844, 2022.

[42] V. Y. Ramandi, M. Fateh, and M. Rezvani, "VidaGAN: Adaptive GAN for image steganography," IET Image Processing, vol. 18, no. 12, pp. 3329-3342, 2024.

[43] D. Polisetty and S. W. A. Rizvi, "GAN-Based Adaptive Image Steganography," International Journal of Computer Applications, vol. 187, no. 6, pp. 45-50, 2025.

* Corresponding authors: *Department of Computer Science*, *University of Kufa*, *Iraq*
E-mail addresses: yousifh.alsary@student.uokufa.edu.iq (Yousif H. Jasim)