Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.045908

REVIEW

A Review on the Recent Trends of Image Steganography for VANET Applications

Arshiya S. Ansari*

Department of Information Technology, College of Computer and Information Sciences, Majmaah University, Al-Majmaah, 11952, Saudi Arabia

*Corresponding Author: Arshiya S. Ansari. Email: ar.ansari@mu.edu.sa

Received: 11 August 2023 Accepted: 27 December 2023 Published: 26 March 2024

ABSTRACT

Image steganography is a technique of concealing confidential information within an image without dramatically changing its outside look. Whereas vehicular ad hoc networks (VANETs), which enable vehicles to communicate with one another and with roadside infrastructure to enhance safety and traffic flow provide a range of value-added services, as they are an essential component of modern smart transportation systems. VANETs steganography has been suggested by many authors for secure, reliable message transfer between terminal/hope to terminal/hope and also to secure it from attack for privacy protection. This paper aims to determine whether using steganography is possible to improve data security and secrecy in VANET applications and to analyze effective steganography techniques for incorporating data into images while minimizing visual quality loss. According to simulations in literature and real-world studies, Image steganography proved to be an effective method for secure communication on VANETs, even in difficult network conditions. In this research, we also explore a variety of steganography approaches for vehicular ad-hoc network transportation systems like vector embedding, statistics, spatial domain (SD), transform domain (TD), distortion, masking, and filtering. This study possibly shall help researchers to improve vehicle networks' ability to communicate securely and lay the door for innovative steganography methods.

KEYWORDS

Steganography; image steganography; image steganography techniques; information exchange; data embedding and extracting; vehicular ad hoc network (VANET); transportation system

1 Introduction

Digital image-based steganography has emerged as an essential field of study in signal processing. That partly results from the analysis of the community's intense interest. A steganography expert from Dresden University has urged researchers in the field to look at how steganography and other per-processing approaches, like cryptography, communication, etc., because all current steganography methods heavily rely on conventional cryptographic algorithms that are obviously inappropriate for steganography uses in situations requiring adaptability, robustness, and safety. Real-time transfer of information among vehicles and road equipment is made possible by the revolutionary and flexible technology for wireless communication known as the VANET. The use of ad hoc networks and

communication between vehicles study are combined in this novel technology to generate a robust and adaptable system that improves traffic flow, highway security, and the overall driving experience. They will make highways safer, quicker, and more intelligent, and they will move us nearer to the dream of self-sufficient and connected automobiles [1–4]. The process of hiding a message within the image is known as steganography. In VANET applications, image classifiers using machine learning techniques can be extremely helpful in identifying and understanding steganographic content hidden within images. Image steganography, in contrast to the use of encryption, alters the cover image (CI) to disguise the hidden data, making it appear legitimate. On the other hand, steganalysis is used to undergo/decipher secret signals and uncover hidden information [5–9].

In Fig. 1, we see the steganographic method in action in the VANET environment. After an emergency car accident, a car location message or picture can be transmitted using encryption & steganography from one terminal to another terminal.

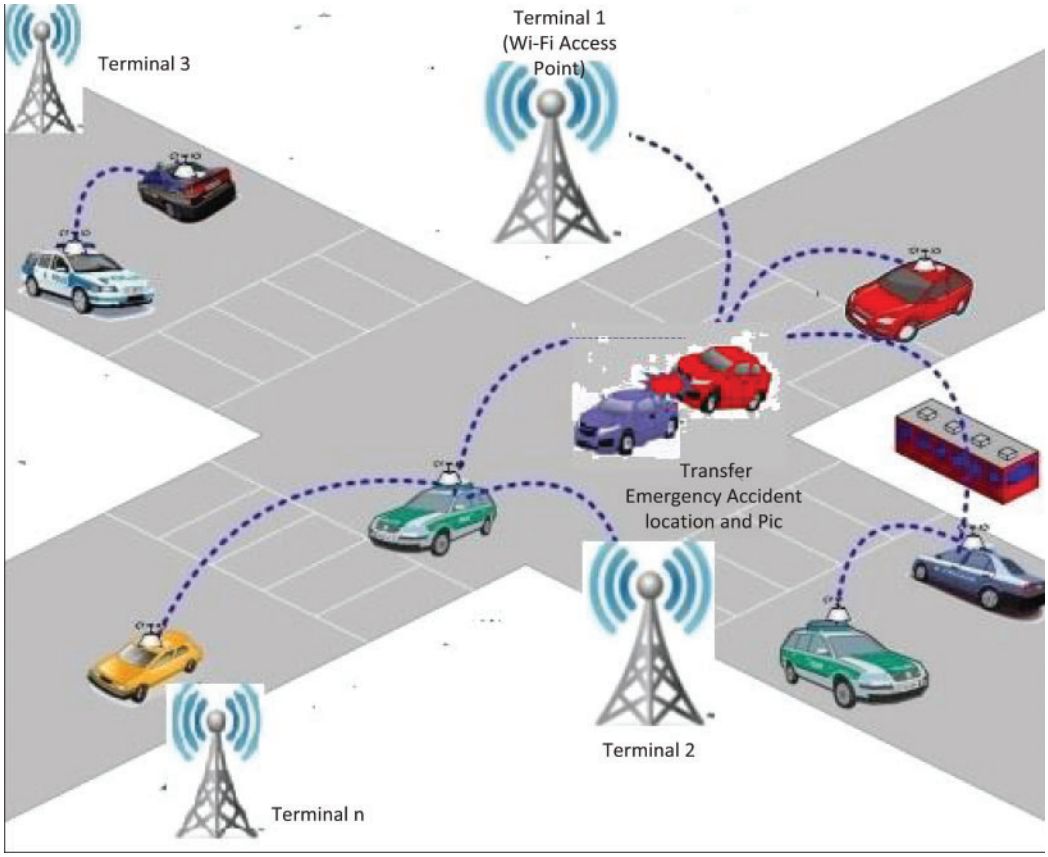

Figure 1: VANETs secure terminal to terminal transmission of accident location and picture

The practice developed throughout time as a result of the pressing necessity to write faster due to the rapid interchange of oral messages. Steganography is typically used in court proceedings and the media. The file containing the concealed information is denoted as the cover file, while the file itself is denoted as the secret data file. The new business and court hearings are typically where steganography is used most frequently [10–14]. Three fundamental building blocks for steganographic techniques are described in contemporary steganography. i) Using Cover Modifications (CMO). To include confidential information, the steganographer first creates a CI and adjusts it. The modified

version will obviously result in some embedding modifications to the cover picture. ii) Steganography using Cover Selection (CSE) is a process asking for image size according to the size of data. Using a big database of photos from which hidden messages can be created using stego images, the steganographer chooses a genuine, unaltered, normal image to use for steganography. iii) By using Cover Synthesis, steganography (CSY), a steganographer makes a stego picture with hidden messages. Building a realistic digital image was more of a theoretical concept ten years ago than a useful steganographic method [15–18]. The private data is slightly modified and designated as a CI by typical image steganography before being embedded into the carrier data. SD and TD-based steganography techniques are the two primary categories of steganography techniques [19–21].

The image cameras installed in vehicles can provide useful data for things like lane detection, distance measurement, obstacle identification, augmented reality navigation, and more. Images captured by smartphones, computers, tablets, watches, etc., carried by drivers and passengers, can also be utilized for other purposes, such as communication, accident recording and liability determination, vehicle tracking, etc. The use of numerous images in a realistic manner distributing the embedding payload among a collection of photographs and conducting theoretical security assessments on a large number of images are significant hurdles for steganography [22,23].

1.1 Outline and Types of Steganography

The term steganography originates from the Greek for hidden writing. Steganography derives from the Greek terms steganos and graphical, which mean secret writing. Steganography has its roots in the biomedical and physiological [24–26]. Image classifiers are used in VANET applications as a preventative measure against steganographic attacks. Nowadays, however, most persons use the medium to transmit information in text, photographs, videos [27–30], in VANET, and in transportation systems.

1.1.1 Steganography of Text File

Text files are used to conceal secret information. Since text steganography can only save text files, it uses less memory [31–35]. It allows for rapid file transfers or interaction between computers [36–40]. Text steganography is rarely used since there is so much redundant information in text files. Information can be concealed in text files in a variety of ways. The first method is predicated on structure, the second on statistics, and the third on language [41–45].

1.1.2 Steganography of Image

Image steganography, also known as the method of secret data concealment in an image file [46–50], is a technique for hiding information using a cover such as a photograph. Some limitations include not being able to safely incorporate a large quantity of data in an image without raising suspicions that the image itself contains data and causing distortion. The LSB embedding technique is used for traditional image steganography [51–55].

1.1.3 Steganography of Audio

Using audio steganography, one can hide sensitive information in an audio file. It also has a strong personality, yet there is only so much data that can be kept secret [56–58]. This method can be used to obfuscate data in audio formats including MP3, AU, and WAV. There are a number of different approaches to audio steganography [59].

1.1.4 Steganography of Video

Frequency domain (FD) and spatial domain (SD) techniques are the two main categories of steganographic methods. In this case, video is used as the carrier to conceal the data. Each video frame has its contents obscured using Discrete Cosine Transform (DCT), a common method for hiding sensitive information. H.264, MP4, MPEG, and AVI are the most used file types for video steganography [60].

1.1.5 Steganography for a System or Protocol

Network steganography techniques include changing just one network protocol. It requires disguising the information by passing it through a network protocol. It is really strong and safe [61].

1.2 Steganography for VANET & Transportation System

Radio transmission parameters, including low transfer speeds, mutual association, and administration remain unchanged; therefore, the standard for VANET generally follows the procedural innovation of MANET. However, VANET's primary operational challenge stems from the rapid and unpredictable mobility of the flexible hubs (vehicles) along the routes. The methods of steganography for VANETs are shown in Fig. 2. It shows how steganography is done in VANET environment.

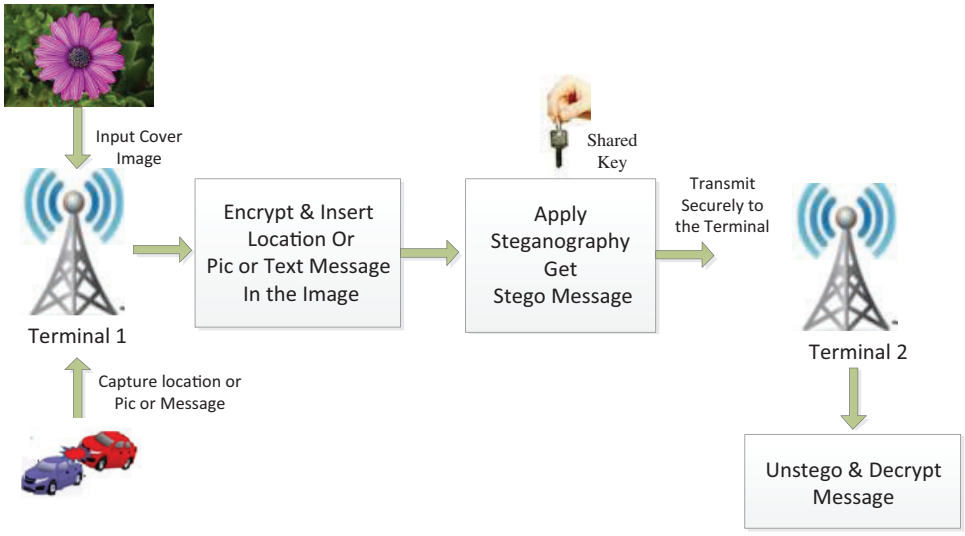

Figure 2: Process of VANETs steganography

1.3 Different Methods\|Techniques for Different Domains of Steganography

To name only a few of the many steganographic variants: Many different steganographic techniques are presented by authors, each one suited to a different kind of cover item. Fig. 3 shows different steganography methods/techniques & embedding domains.

The two main basic categories of steganography embedding domains are special domain (Example: Least significant bit insertion) and frequency domain (Example: Discrete Cosine Transform). By substituting the LSB of the CI pixels with the bits of concealed data, this method utilizes a straightforward kind of embedding. After being embedded, an image looks remarkably similar to the original, with little variation when the LSB of a pixel is altered. LSB is efficient for short messages by

quietly modifying the least significant bits of pixel values, but it is vulnerable to visual examination, The FD steganography method may balance data concealment and image quality as it operates in the frequency domain, it has a reasonable efficiency for short messages, as shown in Table 1 for efficiency for short messages. In the TD-based method coefficients of the picture, attempt to encrypt message bits. Strong watermarking frequently uses information embedding in the TD. There are several groups into which TD methods can be divided as shown in Fig. 3.

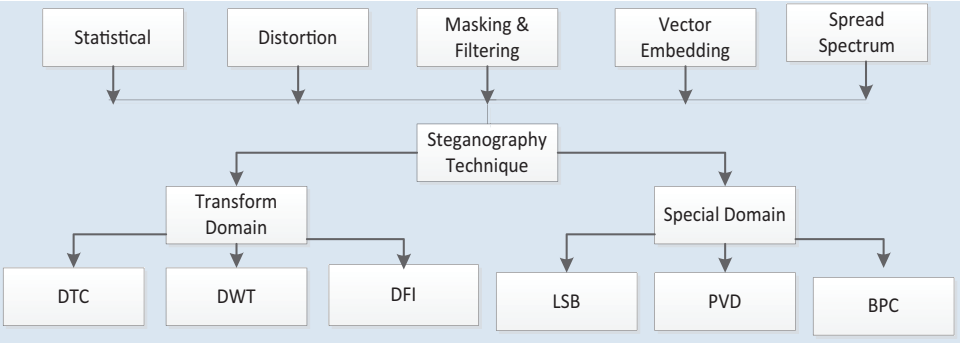

Figure 3: Steganography techniques & embedding domain

Table 1: Efficiency for short messages

Steganography domain	Short messages efficiency	Difficulty faced
Special domain (LSB)	High	Capability of visual detection
Frequency domain (DCT)	Moderate	Sensitive to compression

2 Literature Review

This study's main goal is to research and describe the different steganography methods for VNET. Deep-learning methods used to visualize steganography and VANETs. VANETs can undoubtedly support deep learning. Deep learning, a type of machine learning, uses artificial neural networks to learn from data. Because of this, it excels at jobs like intrusion detection, traffic control, and highway safety. Deep learning is a promising technology for VANETs despite many difficulties. Deep learning is anticipated to become more crucial to the creation of VANETs as technology advances and the amount of data at our disposal grows.

Study [62] enhanced the development of agent software using a steganography approach. It suggested using an agent network to conceal a secret message in a particular cover reputation, based on a support vector machine (SVM) classifier. Six statistics parameters energy, the standard deviation, the histogram, variation, mean, and entropy were essential to the development of an agent system. As a result, the SVM classifier was able to classify the features and predict which cover picture would be the best candidate for embedding. Regarding indistinctness, threat, and cover photograph prediction by quantitative issues, noteworthy results have been obtained. Study [63] improved the privacy of patients in the event of a remote diagnosis by safely and imperceptibly embedding the patient's identifiable data in their medical photos using steganography system. The average square error and PSNR were used to calculate the deformation between the cover photograph and stego-image, and normalizing cross-correlation was used to calculate the degree of proximity between the two images. Study [64] proposed multithreaded planning technique utilizing virtual realities to address the issues of narrow

orientation of objects and inadequate visual making capacity of the test system of the optical network for communication. Additionally, the exploratory system design approach for the optical network of communications with multiple channels serial line design. The outcome shown that the test setup for optical communication networks had an excellent visual modeling effect, enhanced stability and dependability, and decreased telecommunication transmissions error.

Study [65] developed a deep learning-based method for enhancing steganography in spontaneous cloud systems. There are two sections to this research implementation. The performance of the deployed ad-hoc system was superior to that of Amazon AC2, and the deep stenography technique demonstrated an outstanding assessment rate for data and picture concealment when tested against multiple attacks in a spontaneously cloud system context. Study [66] presented an image steganography process that builds the safety of the confidential information using an encrypted image method based on binary bit-plane decomposition (BBPD) and a mix of several techniques. In contrast to the latest techniques used currently, the suggested stenography method exhibits superior outcomes in terms of security, photographic quality, and capacity of payload. Study [67] proposed a key negotiation method for an instantaneous data exchange platform for vehicular ad hoc networks (VANETs), where a communication center verifies a user's identity as they declare a disaster and provides other users with a digital certificate in case of emergency. The experiment's findings demonstrate the viability and compliance of the suggested plan with security standards.

The idea of imagining steganalysis, which enables us to find the image buried inside another image, was applied in study [68]. This experiment analyzes different steganography techniques utilized in the modern world and tries to use picture stochastic analysis with visual decoding using LSB and MSB methodology.

In order to take advantage of multi-domain information in the geographical, rate, and compression areas, they provided the manipulation classification network (MCNet) in study [69]. Furthermore, they conducted experiments to demonstrate the effectiveness of the refined model, which was based on the multi-class modification job, for various forensic tasks including DeepFake detection and JPEG picture integrity verification. Study [70] addressed an evaluation of the steganographic scheme's system capacity using a 2-D Markov chains model in respect to the specification. A comparison of the analytical and computational outcomes under various network parameters is used to validate the model. According to quantitative and modeling outcomes, the steganographic channel's system performance values are dependent on data.

Study [71] proposed an image localization technique for a class of steganography involving pseudo-randomly scrambled JPEG images. According to the research findings, when the examiner has several stego pictures inserted in the identical direction, the suggested position methods can locate the stego sites in JStego and F5 steganography with accuracy. Furthermore, the location findings can be utilized to obtain the technique known as key requested to unlock the hidden messages that have been implanted.

Study [72] presented a method that combines the techniques of inversion code, encryption, and steganography. It concentrates on the LSB approach in a different way, i.e., the approach utilizes the MSB of the footage frame and the LSB of the stego image in order to accomplish the LSB stenography method opposed to inserting information at the LSB of the original frame. The combination of factors contributes to the safeguard image's improved quality and minimal distortion. The PSNR value would be used to calculate the algorithm's productivity value. B-spot was a durable and safe image transfer system that was based on cryptocurrency and steganography was proposed in study [73]. Ultimately, the distributed ledger is recovered and used to recreate the stego-image. After using the extraction

process, the recipient can then get the hidden images. The outcomes of the simulations indicate that the suggested mechanism possesses a substantial data ability, enhanced imperceptibility, a tolerable computation time, and resilience against noise. Study [74] suggested a variation of the spatial rich model feature that was based on asymmetrical channels anchoring modification probability. The experimental findings demonstrate that, particularly for smaller package sizes, the suggested features can greatly enhance identification capabilities for steganography system.

Study [75] presented the IAS-CNN, a lightweight convolutional neural network designed for image adaptable the steganalysis. They use the network's self-education filter technique to get around the drawback of manually creating remaining extractor filtering. The outcomes of the experiments demonstrate the manner in which IAS-CNN works in steganalysis. Study [76] suggested combining blockchain-based technology with two-factor authorization as a safety preventative measures to increase the use of smart electronic voting machines for election procedures. The private blockchain approach is used to guarantee records operations' integrity and dependability, prevent records manipulation, and provide immutability. The experimentation with a false accepting rate, the system's performance was demonstrated to be improved.

The three main divisions of deep learning approaches for photo steganography are traditional methods, methods based on "convolutional neural networks (CNNs), and methods based on global adversarial networks (GANs)". The paper [77] offered a thorough justification of the technique, a list of the datasets utilized, an analysis of the experimental conditions, and a list of frequently employed assessment measures. Promising research in the subject area is outlined in this publication. Before they analyze the primary uses of this research's methodology, they first give some background information about it. They also describe the information of different datasets used by the authors to analyze results. All the images of size $512 * 512$ are used to analyze results. Capacity, robustness, and security factors have been considered for observation. The remainder of the paper [78] explored projects showcasing state-of-the-art advancements in the creation of strategies and tactics to achieve information concealment in digital visuals. The focus of this study, which does not purport to be thorough, is on recent studies that show the path that information embedded in digital photographs is now taking. The primary characteristic of a review that sets it apart from reviews that have already been published is that. Finding a sensible compromise between requirements like large Hiding Capacity (HC), improved imperceptibility, and increased security is the main challenge for the bulk of these Image Steganography Techniques (ISTs). The study [79] analyzed numerous picture steganography measures across multiple ISTs, ranging from conventional to cutting-edge spatial innovations. The primary challenge in designing a steganography system is striking a good compromise between robustness, security, invisibility, and high bit embedding rates. The book [80] examined all the different types of photo steganography that are in use today, including the most current developments in each subcategory across different mediums. Additionally, the paper offers a comprehensive introduction to visual steganography system, including a discussion of its basic concepts, necessary conditions, many aspects, different types, and evaluations of its efficacy. Image detectors are trained using huge collections of covering and stego images.

The previously suggested steganography systems are divided into two primary groups in this work: the geographical domain and the frequency domain. We evaluate works based on their ability to withstand geometric and non-geometric attacks, as well as their complicity, as well as their payload, and recovered bit error rate. The most popular metrics used in the field of steganography are discussed together with their methods of assessment. Finally, steganography's difficulties and emerging trends were presented by the research [81].

The paper [82] reviewed the history of steganalysis and offers broad guidelines for utilizing digital multimedia to conceal hidden information. For better comprehension, steganalysis is categorized in this survey based on a variety of viewpoints. Additionally, it offers a thorough evaluation of current steganalysis methods and procedures for audio, video, and pictures. Finally, to provide a helpful resource for future study, the current problems and recommendations in this topic are highlighted. This study [83] gave a high-level summary and comparison of several investigations that have been undertaken in the field of object recognition and image categorization. The study was divided into three sections: machine learning methods, deep learning methods, and object recognition in low-light settings. A table was included to facilitate comparison of the various texts. They conducted a thorough literature review on "3-D mesh steganography and steganalysis" in this paper. New taxonomies for steganographic methods were proposed in the paper under the names "convert field, permutations area, LSB area, and two-state area" [84]. They separated the two categories of steganalysis techniques: general-purpose and specialized. Each section describing the current state of the art includes some background information on the development of technology. They emphasized several intriguing research topics in their conclusion, as well as the challenges of improving 3-D mesh steganography and steganalysis performance. Steganography is the process of secretly transmitting information via encoded messages that can be deciphered only by the intended recipient.

An introduction to steganography in cloud computing was provided in [85], which also serves as a comparison table for studies that differ in their technique choice, carrier format, payload capacity, and embedding algorithm. The paper provides a summary of the research that is being done in this area right now. The paper [86] began by describing the foundations and operation of text steganography. The following section explains the three categories of text steganography: linguistics, format-based techniques, and statistical and random generation. The methods used by each class are examined, with a focus on how each class offers a special method for concealing sensitive information but ignored the robustness issue.

The article [87] explored the underlying concepts, covered selection methods and security aspects of steganography along with mythologies. In addition, evaluation quality metrics for cover selection were also highlighted. Improvement direction for steganography mythologies also suggested. The paper [88] used artificial intelligence for text based linguistic steganography to improve hiding method. Natural language processing used for automatic text detection. The article also proved the robust security against attack. The traditional LSB steganography method was used in article [89]. The author experimented on natural images considering edges and smooth region of images. The gradient of edge was used to embed secret message. The data inserted in the pixel range from 0 to 255. Pixel values adjusted to positive negative value range accordingly. Steganography proved more robust while combining cryptography technique. The Filter bank cipher encryption method was used in paper [90] to provide strong security and speed. DCT domain used to embed secret data. PSNR metric is used to evaluate the result performance. High PSNR value evaluated for better perceptibility.

This section reviewed the reported work of scholars on steganography. The segment summarized the different types of steganography presented by authors along with their methodologies used. In addition, it discussed the factors considered for result assessment. The comparative analysis is described in the next section.

3 Comparative Analysis

3.1 A Survey Regarding Three Categories of Image Steganography

After surveying the various image steganography frameworks, the various approaches are essentially classified as traditional, CNN-based, or GAN-based image steganography methods. Traditional approaches are frameworks that do not employ machine learning or deep learning methods. The LSB approach is the foundation for many traditional methods. To embed and extract the hidden messages, CNN-based approaches rely on deep CNN, whereas GAN-based methods use various forms of GAN. Both CNN and GAN models may be used for deep learning techniques.

3.1.1 Traditional Steganography Methods

Traditional image steganography makes use of the LSB substitution technique [91]. Higher-resolution images often have a lower percentage of their pixels utilized. The LSB approach presupposes that changing a small number of pixel values would not be noticeable [92]. Binary code is used to store the private information. The LSBs of the CI are then modified by swapping in the binary data from the hidden image [93,94].

A variety of comparable approaches have been presented, with the LSB method serving as the benchmark for comparison. For instance, in the process of turning the hidden data into binary codes, there is a very slight modification that is carried out [95,96]. The LSB technique is then used to add the encoded bits to the CI [97]. In the study [98], the LSB method was applied in a unique way to RGB images. The CI has three channels, and each of those channels has been a bit fragmented [99]. In videos, the LSB substitution technique in its most basic version and the Huffman encoding method, in conjunction with the LSB substitution method, are used [100].

The comprehensive analysis of classic image steganographic techniques is shown in Table 2. PVD is another time-tested technique for concealing images [101]. The secret bits may be hidden in PVD by measuring the difference between neighboring pixels, and the method ensures that the cover image's visual coherence is preserved in the process [102,103]. Coverless steganography is another method, in which the CI is not provided but rather created depending on the hidden data [104]. Using the object detection approach, we extract the confidential data and handle the associated relationships in order to create the CI [105]. The borders of the color CI are retrieved without using LSB [106,107]. Then, after the borders of the cover images have been uncovered, the secret information may be deciphered in binary [108].

The following describes several variations of the VANET and transportation system techniques used in steganography. We analyze pixels in the same positions in both blocks and exploit the differences in their DCT coefficients to conduct embedding [109–113]. These JPEGs serve as medical documentation. In particular, the novel method known as the Pixel Density Histogram [114] works well with halftone images. To protect the privacy of the data, a histogram is created [115].

PSNR & MSE

The mean squared error (MSE) of the cover and stego images is divided by the maximum pixel value to produce the PSNR, which measures the stego image's quality. Increasing PSNR values improve the stego image's quality. The comprehensive analysis of classic image steganographic techniques is shown in Table 2.

$$PSNR = 10 * log10\left(\left(\max^2\right)/MSE\right)$$

Table 2: Steganography traditional models performance summary

Method	Metrics	Dataset	Advantages	Disadvantages
[109]	Mean square error (MSE) & peak signal-to-noise ratio (PSNR)	Lena and Baboon	Computation time is less The image is a hidden message	Security is less than deep learning
[110]	PSNR and time	RGB image	Computation time is less	Weak security
[111]	PSNR	Lena	The image is a hidden message	Security is less

The median squares differences are calculated using MSE using the values of pixels of the cover and stego pictures. If the MSE is lower, the quality is higher.

$$MSE = \Sigma\,(pixelcover - pixelstego)^2\,/N$$

where N = quantity of pixels.

3.1.2 CNN-Based Steganography Methods

The encoder-decoder structure is a major inspiration for CNN-based image steganography [116]. Using the CI and the Secret Image (SI), an encoder creates a Stego Image (SOI); the decoder then reads the SI from the SOI [117]. Though they all operate on the same underlying principle of VANET and transportation systems, many approaches have experimented with various architectural implementations [118,119]. Each technique has its own unique set of parameters. The CI and the SI must have the same dimensions for this to work; otherwise, just some of the CI's pixels will end up on the cover [120].

A proposal for encoder-decoder architecture may be found in [121,122] suggests using a CNN with 6 layers for the extraction process. The hiding process uses an encoder-decoder architecture that is based on U-Net. The U-Net's input form has been changed so that it can now accept input in 256256 and 6 channels [123]. The input is created by combining the cover and hidden images, yielding a total of six channels [124]. The steganography techniques used with CNN are reviewed in Table 3.

Table 3: CNN models summary

Method	Dataset	Architecture	Advantages	Disadvantages
[122]	ImageNet	U-Net	Simple architecture	The image size is quite modest at 64 × 64.
[125]	ImageNet	Encoder-decoder	The picture is a hidden message	Picture size is quite modest at 64 × 64.

3.1.3 Steganography Methods Based on GAN

A subclass of CNNs known as General Adversarial Networks (GANs) was initially introduced in 2014 by [125,126]. For image creation challenges, a GAN employs game theory to develop an adversarial generative model [127,128]. In GAN architecture, an ideal picture is generated by having

two networks: the generator network and the discriminator network compete with one another. Input data is provided to the generator model, and a high-quality, near-perfect approximation of the input image is produced as output [129]. The VANET and transportation system-produced images are sorted into fake and real categories by the discriminator networks [130]. Both networks are trained to minimize noise while producing an accurate representation of the input data [131]. In order to detect the phony images, a discriminator model is trained. Since then, several variants of GAN have been presented, each one improving the algorithm and making it more suited to generating synthetic images [132]. In the realm of image generation, GANs have a well-deserved reputation for excellence [133].

One example of this kind of image-generating task is image steganography, which takes two images as input (the CI and the SI), and VANET and the transportation system produce a third image (the stego image) [134,135]. The two primary parts of a GAN model are the generator and the discriminator [136]. Some of the techniques include the use of a novel network, the steganalyzer, to decipher the steganographically concealed images in VANET and transportation systems [137].

The generator network was created using the U-Net-based design, which is why the authors in [138] refer to this system as a UT-GAN. For the input value CI, C, the algorithm creates a probabilistic map, P, and U-Net is chosen because of its effective pixel-for-pixel segmented capability. Convolutional layers in the U-Net utilized here grow in size for the convolutional layers and shrink in size for the deconvolutional layers [139,140]. The authors in [141] used a WGAN as their generative model. It is suggested to use a generative model to create a CI with textural content. Once the CI and SI have been prepared, they are sent to a concealing network [142]. Because of this, the final output is a textured output with hidden information inside it. The authors in [143,144] offered an adversarial learning, VANET, and transportation system-based approach.

3.1.4 Patchwork

A steganography approach called the Patchwork Algorithm involves breaking an image up into smaller patches or blocks and altering these patches to conceal data. By limiting the visual impact on the entire image and embedding information inside it, this method reduces the likelihood of discovery. The information we are concealing is given redundancy by this steganography method, which then distributes it throughout the image. In this, two areas of the image are chosen, and if one area is lightened, the other area is made darker. In order to conceal data, this method breaks the image into smaller patches and modifies the colors or textures of the patches. Due to the fact that it does not alter the full image, it may be more resistant to detection. Table 4 reviews the patchwork steganography methods.

Table 4: Patchwork model summary

Methods	Advantages	Disadvantages
Patchwork	1. Unwillingness to accept tone and gama corrections 2. Utilizing distinct patches prevents interference between them, which results in disruption in one patch but not the other	Smaller bit rate

3.2 Pixel Value Differencing Steganography (PVDS)

There are smooth and textured areas in a picture. The image's texture areas of VANET have the ability to hold more hidden information than its smooth regions. The transportation system has rough

and smooth parts of a picture that cannot be distinguished using LSB-based approaches, though. The foundation of PVDS is the idea of pixel difference, sometimes referred to as Fluctuation Value (FV). The image is then divided into several blocks, each of which has two CPs. The CPs of the various blocks is then used to locate FVs. Then, these FVs are used to perform the embedding procedure in each individual block. Fig. 4 shows an example of the PVDS technology and describes how the embedding and extraction processes work. Overflow and Underflow Problem (OUP) status, Attack Resistance Ability (ARA) to Regular and Singular (RS) analysis, average "Bits per Pixel (BPP), Peak Signal-to-Noise Ratio (PSNR)", Pixel Difference Histogram (PDH), or any other steganalysis attacks, are shown in Table 5.

3.2.1 Merits and Issues of PVDS Technique

The smooth and textural parts of the picture are effectively used by VANET, the transportation system, and the PVDS approach in a sufficient manner for hidden bit embedding. As a result, it defies the RS analysis. The PVDS technique's RS-plot of the Lena picture is displayed in Figs. 4 and 5. It is evident that the circumstances.

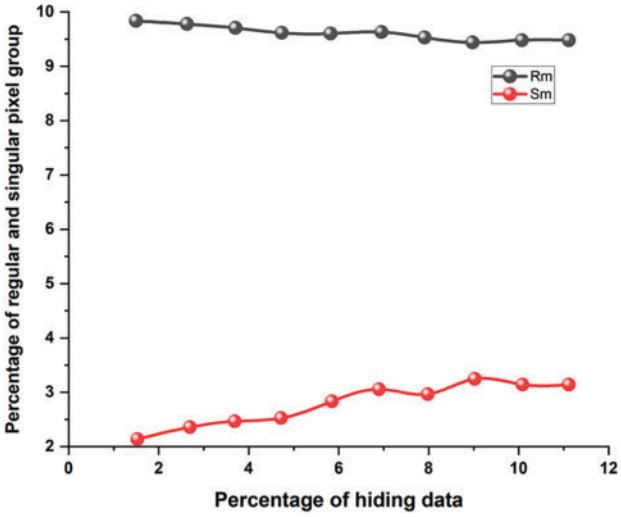

Figure 4: RS-plot of Lena image

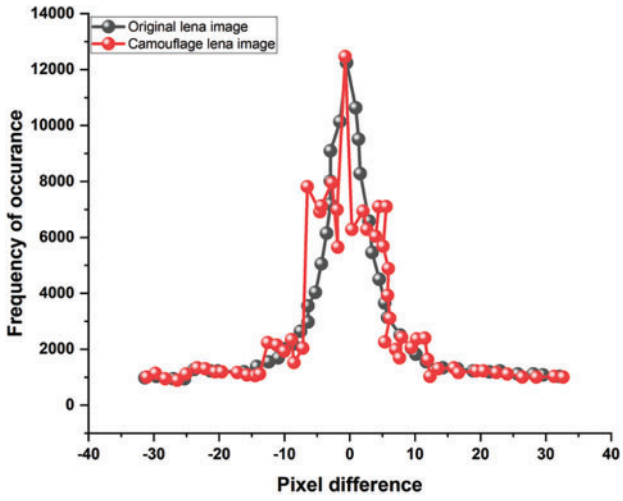

Figure 5: PDH-plot of Lena image for PVDS

Table 5: Evaluation of a PVDS-based method

Ref.	Methodologies	BPP	Standard PSNR (in dB)	ARA to RS	OUP avoided	ARA to PDH
Hussain et al. (2017) [145]	Parity-bit PVDS (with RT 2)	2.17	39.09	✓	✓	✓
	PVDS parity-bit PVDS	2.07	40.45	✓	✓	✓
	(PBPVD) + Improved rightmost digit replacement (IRMDR)	3.00	38.47	✓	✓	✓

(Continued)

Table 5 (continued)

Ref.	Methodologies	BPP	Standard PSNR (in dB)	ARA to RS	OUP avoided	ARA to PDH
Swain (2018) [146]	RT PVDS-non-adaptive	3.16	36.88			
	RT PVDS-adaptive	2.96	42.97	✓	✓	✓
Hameed et al. (2018) [147]	Adaptive PVDS in a block with a color image in the diagonal, vertical, and horizontal directions	1.65	45.49	–	–	✓
Liu et al. (2019) [148]	PVDS + Side match technique	2.79	35.17		–	–
Grajeda-Marín et al. (2018) [149]	Optimization strategy + PVDS	2.41	38.33	–	–	–
Kim et al. (2019) [150]	Adaptive steganography + Modified PVDS	1.58	40.67	–	✓	–
Wu et al. (2005) [151]	Modified PVDS	1.55	43.35	✓	✓	✓
		0.11	47.23			

Furthermore, almost all of the VANET, transportation system, and PVD-based steganography methods that have recently been created by various researchers were built on PVDS technology. One of the biggest problems with the PVDS approach in a PDH analysis is resistance. After hidden bits have been embedded, the PDH plot of the Lena image is shown in Fig. 6. The fact that the CI's histogram is zigzag in shape, as opposed to smooth, shows that the CI contains some information. Next, OUP affects the majority of PVDS procedures. The OUP pixel employed in the PVDS technique is shown in Fig. 6. These methods are also taken into consideration for the evaluation since they put the VANET, transportation system, and PVDS idea into practice. By including some random data in the obtained images, as shown in Fig. 7, the proportion of pixels that experience OUP is seen in Table 6.

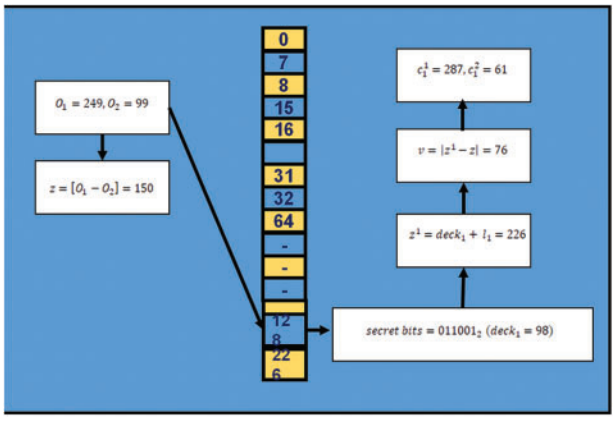

Figure 6: An illustration of OUP in the PVDS process

Figure 7: Test images in 512 × 512

Table 6: OUP affected pixel count for various PVDS-based techniques

Dark image (512 × 512)	Wu et al. (2005) [151]	Wu et al. (2003) [152]	Jung (2018) [153]	Khodaei et al. (2012) [154]
Aerial	46	259	329	194
Baboon	3	22	4566	11
Lena	0	0	0	2
Baby	30	472	1576	207
Barbara	746	673	492	1
House	1	0	0	0
Zelda	0	5	631	5
Couple	74	173	631	64
Boat	81	99	256	4
Houses	1545	3165	3707	2267
Girl's face	172	4283	11383	2065
Peppers	228	391	4138	58
Crowd	64	980	1458	967
Airfield	734	4001	4566	3813
Clown	140	146	15909	2

3.3 Least Significant Bit Steganography (LSBS)

The LSBS methodology, which includes swapping out the least significant bits (LSBs) of the original picture OI pixels with secret bits, is by far the most traditional and basic method of image steganography. The LSBs of the OI's pixels could be changed to hidden bits to further enhance the HC. In Fig. 8, we can observe the 1 LSBS approach. Different LSBS-based strategies have been developed by the literature, some of which enhanced HC quality and others, CI quality, and transportation systems.

Without embedded data, the RS plots for the Lena picture are shown in Figs. 9 and 10. However, statistical analysis methods including RS research, bit plane analysis, and chi-square analysis are made available to the traditional LSBS procedures. RS plots for the Lena picture using the 1 LSBS approach are shown in Fig. 11. For the 1 LSBS, 2 LSBS, and 3 LSBS approaches, the PDH indicators are revealed in Figs. 11a–11c, correspondingly.

Additionally, LSB plane analysis can be used to quickly spot the CI planes' visual defects, which are different from the OI planes. Bit planes of the related plane images in the original Lena image. The first-bit plane images match the original Lena image (1 LSBS, 2 LSBM, and 3 LSBS). Please note that the other two methods under consideration here both use randomized embedding, whereas the 1 LSBS method uses sequential embedding. The obtained images demonstrate that the 1 LSBS approach is unique from the OI's original bit plane and smooth. Anyone can therefore assume that information about VANET and transportation systems exists. However, randomized embedding can be used in place of sequential embedding to avoid this analysis.

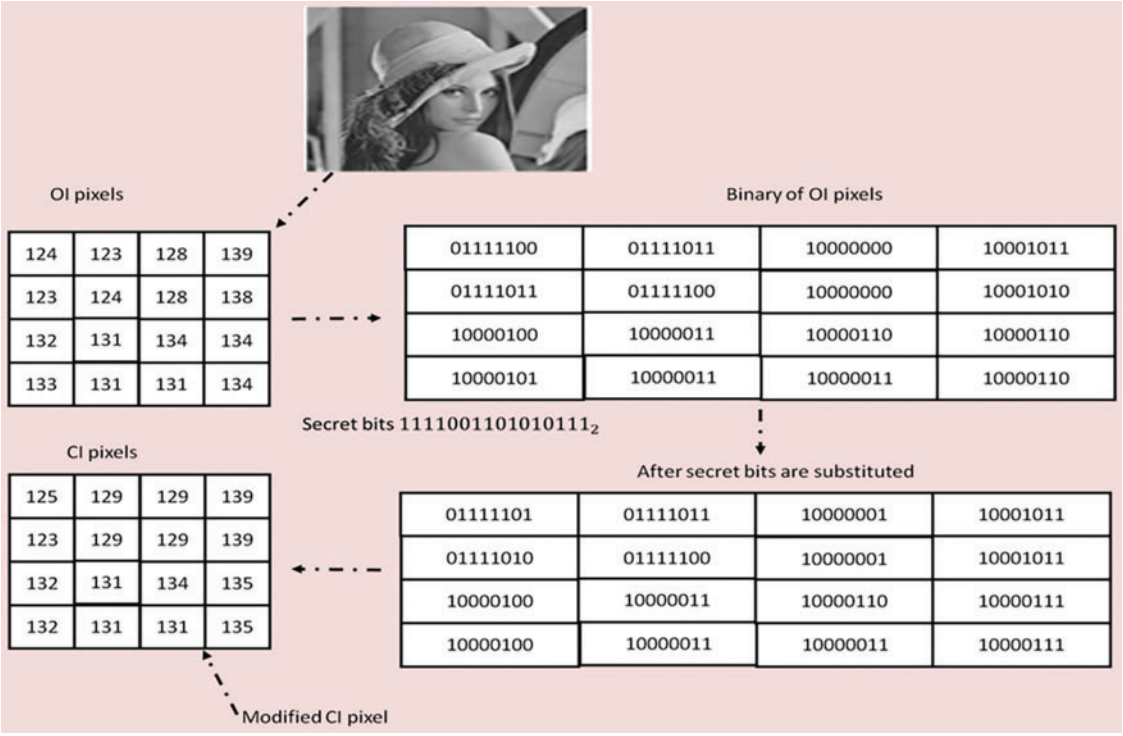

Figure 8: An example of the LSBS approach

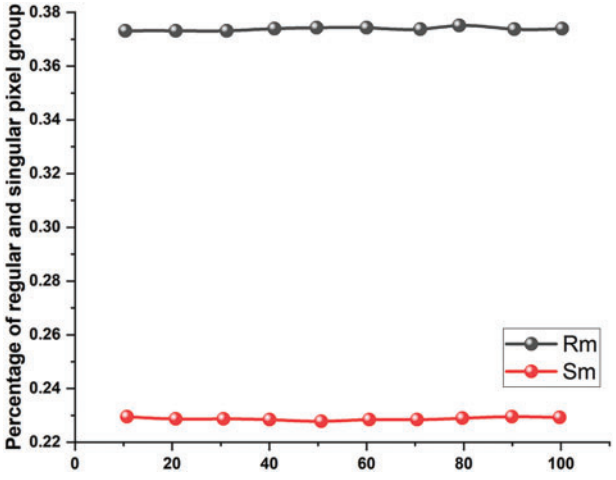

Figure 9: Lena images RS plots without embedded

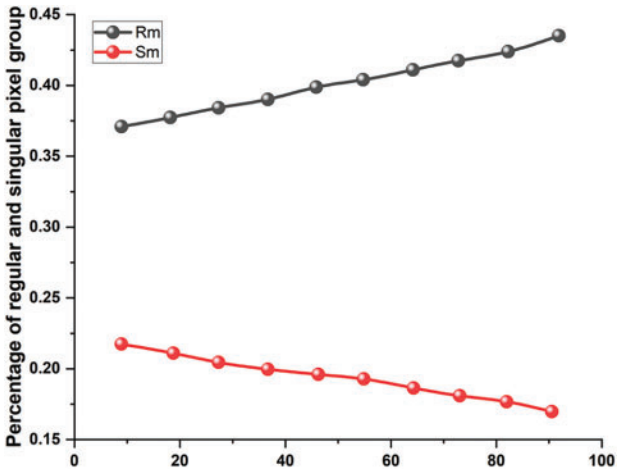

Figure 10: Lena images RS plot after embedded

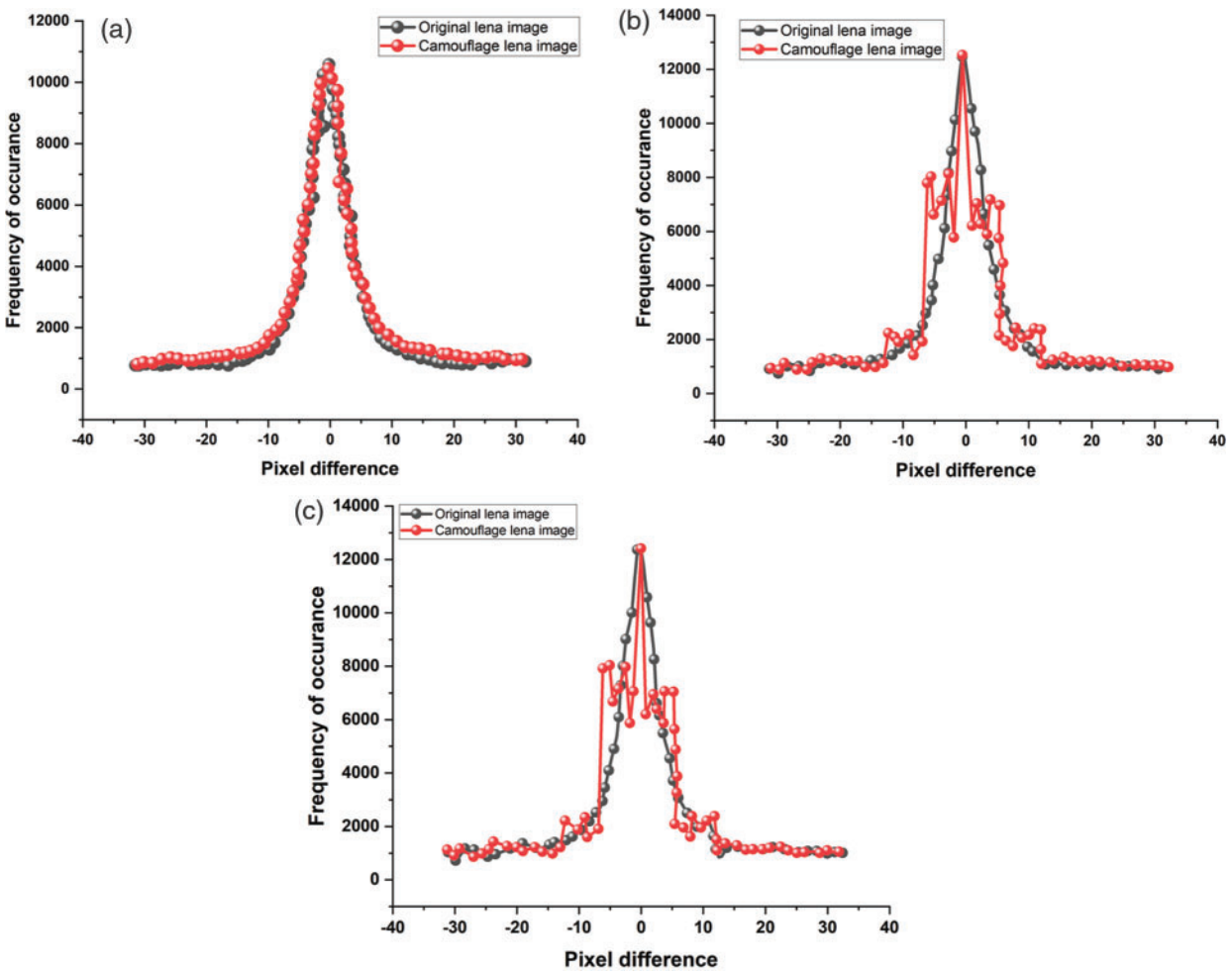

Figure 11: (a) RS plots for the Lena picture using the 1 LSBS approach. (b) RS plots for the Lena picture using the 2 LSBS approach. (c) RS plots for the Lena picture using the 3 LSBS approach

3.3.1 Advantages and Disadvantages of the LSBS-Based Strategy

The simplicity of the LSBS approach is one of the transportation system's most important benefits. The HC can also be expanded by extra LSBs in order to embed the hidden bits. When the secret bits are embedded using MSBs, the CI quality suffers. Another significant flaw is the poor ARA it has with respect to certain statistical studies. With the LSBS method, secret bits are used in place of the LSBs directly. As a result, RS analysis is applied to these procedures. The OI pixels in a unique embedding technique are altered at random by 1. The LSBM method is the name of this methodology. However, the LSBM's real implementation. However, algorithm 3 discusses how to use LSBM in practice.

In an array, the LSB bits are gathered and stored. The secret bits are then mapped with this array, which is given the label LSBA. For the retrieval, the index of the sites where the greatest numbers of bits match has been kept. Since just a small portion of the OI is affected by VANET and the transportation system, this method observes high imperceptibility. Table 7 displays standard BPP, PSNR, and ARA to RS analyses as well as alternative steganographic assaults for various LSBM, LSBS, and LSBA-based methods. Agent-based steganography for VANET is proposed by authors in mounted the agents

on terminals and used steganography for secure transfer of data. The successful experimental results are based on an RGB color scheme using a multi-agent technique.

Table 7: Comparative study of LS-based methods

Ref.	Approaches used	BPP	PSNR on average (in dB)	Any other steganalysis to ARA	Analysis from ARA to RS
[155]	LSB-based data mapping strategy	3.24	42.15	Histogram analysis	–
[156]	n-rightmost bit replacement	1.00, 2.00	51.21, 44.08	S&P noise	–
		3.00, 4.00	40.72, 34.83		
[157]	Multi-Stego-image-based LSBM	4.00	36.06, 37.88	–	–
			39.60, 41.00		
[158]	Inverse Transitions + LSBS	1.50	50.04	–	–
[159]	Quantum IS + LSBS	0.50	50.22	–	–

4 Observations

Traditional steganography uses common techniques for data concealment, usually on text, audio, or image files. Traditional methods of image steganography frequently make use of simple algorithms, including Least Significant Bit (LSB) insertion, in which hidden data is inserted into the image's pixels' least significant bits. Convolutional neural networks are used in CNN-based steganography to increase data capacity and imperceptibility in comparison to straightforward conventional approaches [160,161]. To further increase security and robustness, deep learning steganography, on the other hand, uses sophisticated architecture like GANs and RNNs in addition to CNNs. By offering additional methods to embed and extract data, CNN and deep learning techniques also significantly increase steganography. This ensures secure communication in a variety of applications, including VANETs [162,163]. The work experiments used standard steganography methods to produce the stego images for the desired steganalysis demanding practicality assessment for this issue to overcome the proposed solution. The author has used machine learning RBF (radial-based function) and Nave Bayes formula to improve accuracy [164]. Traditional steganography, CNN-based techniques, and Deep Learning steganography were compared in this paper. Traditional steganography is simple but unreliable, whereas CNN-based techniques increase capacity and imperceptibility but may still be detectable. The performance of deep learning-based steganography is superior to the other two methods in many ways, including security, capacity, and visual appeal. Deep learning algorithms, however, might need more computing power and training data. The best approach to use for a given VANET application will rely on the intended level of privacy, information capacity, and computing complexity.

The different types of steganography were reviewed including audio and video steganography. Compared to image steganography, audio steganography can handle more data, and it is challenging to spot without specialized equipment. Data embedding may cause a little decrease in audio quality. Some audio steganography approaches can be broken by steganalysis tools including the durability of hidden data can be impacted by audio recordings with high compression rates. Video steganography provides more data storage than steganography in images or audio. Video frames conceal data, making it more difficult to identify, and temporal redundancy can be exploited for improved security.

Higher complexity levels for embedding and data extraction. Possibly requires a specialized detection apparatus. Additionally, video editing or compression may have an impact on data extraction.

5 Conclusion

Image steganography is a method of hiding data in digital photos that has attracted a lot of interest in the field of vehicular ad hoc networks (VANETs). This study contributes to a holistic review of image steganography methods for improving data security and secrecy inside vehicular ad hoc networks (VANETs) without jeopardizing the exterior look of images. This study may aid researchers in investigating and increasing the secure communication capabilities of vehicle networks and open the way for new steganography approaches. VANETs provide safety and value-added services and are essential components of contemporary smart transportation systems. The study explores multiple steganography methods, including Spatial and Transform Domains steganography, distortion-based, masking, and filtering-based steganography, to improve safety in transportation systems. Steganography in VNAT reliably secures the trustworthy and confidential transmission of messages between terminals, thereby safeguarding privacy within VANETs. The literature review reveals that transform domain methods are more secure but embed a smaller number of data bits whereas special domain methods or bit insertion methods can insert more numbers of data bits but are less secure. The frequency domain loses more data bits during compression than special domain methods do. Many steganography algorithms have been proven applicable in ensuring secure and reliable message transfer between terminals while also protecting privacy in VANETs. We can still improve data security in VANET systems, with an emphasis on reducing visual quality loss. Image steganography has been shown in simulations and real-world research to succeed in maintaining secure communication even in difficult network settings.

5.1 Challenges

The following are some issues with image steganography:

- Data Availability-Despite the fact that unsupervised learning is used and image reconstruction is the primary aim, there is currently no suitable benchmark dataset for image steganography [165]. It might be difficult to find a useful dataset. The large image sizes in ImageNet, the most used dataset, are a big issue [166]. There is 64×64 in each image, which is really small.
- Convergence of GAN-One of the main problems with GAN is that the system does not converge regardless of the parameters used [167]. Given the interdependence of the generator and the discriminator, mode collapse occurs often.
- Compared to other approaches-Because different approaches use various evaluation metrics, it is challenging to compare the proposed method to the existing methodology.
- Real-time steganography-Large volumes of data are used to teach steganography models [168]. The situation becomes more challenging, however, when authentic steganography is required [169–171]. The stego image must be sent across an unsecured channel in order to utilize the trained model for conducting steganography and steganalysis [172–174]. The VANET and transportation system trained model's ability to handle live, in-the-moment images that may include sounds, skew, and blur remains unproven. The viability of using the concept in real-time steganography is still up for debate.

5.2 Future Works

The following are a few things to consider while planning future programs:

- Popular networks like U-Net and cycleGAN, as well as DCT and DWT, have been considered, and more research into additional specialized designs may be done. For instance, alternative methods to conventional CNNs such as RNNs might be investigated. Different types of GAN may stand in for a personalized WGAN [175].
- Most image steganography techniques rely on text or a grayscale image to conceal data, and there is a pressing need for studies that investigate the hiding of images inside other images [176,177].
- Using different datasets, further experiments may be run to optimize the parameters and reduce the storage capacity.
- Since the quantum computing era is on the horizon, more research may be done into designing quantum images.
- An ensemble of both classic and modern machine learning techniques may be investigated further for their synergistic effects on VANET and transportation systems.
- A benchmark dataset made up of images from different source cameras and image formats may be created. The algorithms for making steganographic images may be compiled as well [178–180].

Acknowledgement: Dr. Arshiya Sajid Ansari would like to thank the Deanship of Scientific Research at Majmaah University for supporting this work under Project No. R-2023-910.

Funding Statement: The author received no specific funding for this study.

Author Contributions: All work was done by a single author Arshiya S. Ansari.

Availability of Data and Materials: Not applicable. All references are from Google Scholar.

Conflicts of Interest: The author declares that they have no conflicts of interest to report regarding the present study.

References

[1] K. Saraswati and P. S. Sharma, "A literature survey on stenography approach based on different LSB technique," Master thesis, German Univ., Cairo, Egypt, 2003.

[2] A. S. Ansari, M. S. Mohammadi, and M. T. Parvez, "A comparative study of recent steganography techniques for multiple image formats," *Int. J. Comput. Netw. Inf. Secur.*, vol. 11, no. 1, pp. 11–25, 2019. doi: 10.5815/ijcnis.2019.01.02.

[3] A. M. Alhomoud, "Image steganography in spatial domain: Current status, techniques, and trends," *Intell. Autom. Soft. Comput.*, vol. 27, no. 1, pp. 2213–2224, 2021. doi: 10.32604/iasc.2021.014773.

[4] W. Su, J. Ni, X. Hu, and J. Fridrich, "Image steganography with symmetric embedding using Gaussian Markov random field model," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 31, no. 3, pp. 1001–1015, 2020. doi: 10.1109/TCSVT.2020.3001122.

[5] N. Subramanian, O. Elharrouss, S. Al-Maadeed, and A. Bouridane, "Image steganography: A review of the recent advances," *IEEE Access*, vol. 9, no. 9, pp. 23409–23423, 2021. doi: 10.1109/ACCESS.2021.3053998.

[6] S. Almutairi, A. Gutub, and M. Al-Ghamdi, "Image steganography to facilitate online students account system," *Rev. Bus Technol. Res.*, vol. 16, no. 2, pp. 43–49, 2019. doi: 10.13140/RG.2.2.32048.30727.

[7] S. Matted, G. Shankar, and B. Jain, "Enhanced image security using stenography and cryptography," in *Proc. 3rd ICCNCT*, Singapore, 2020, pp. 1171–1182.

[8] O. F. Abdelwahab, A. I. Hussein, H. F. Hamed, H. M. Kelash, A. A. Khalaf and H. M. Ali, "Hiding data in images using steganography techniques with compression algorithms," *J. Telecommun. Comput. Electron. Control*, vol. 17, no. 3, pp. 1168–1175, 2019. doi: 10.12928/telkomnika.v17i3.12230.

[9] A. A. AbdelRaouf, "New data hiding approach for image steganography based on visual color sensitivity," *Multimed Tools Appl.*, vol. 80, no. 15, pp. 23393–23417, 2021. doi: 10.1007/s11042-020-10224-w.

[10] F. J. P. Montalbo and D. P. Y. Barfeh, "Classification of stenography using convolutional neural networks and canny edge detection algorithm," in *Proc. ICCIKE*, Dubai, United Arab Emirates, 2019, pp. 305–310.

[11] D. R. I. M. Setiadi, "PSNR vs SSIM: Imperceptibility quality assessment for image steganography," *Multimed Tools Appl.*, vol. 80, no. 6, pp. 8423–8444, 2021. doi: 10.1007/s11042-020-10035-z.

[12] X. T. Duan *et al.*, "High-capacity image steganography based on improved FC-DenseNet," *IEEE Access*, vol. 8, pp. 170174–170182, 2020. doi: 10.1109/ACCESS.2020.3024193.

[13] N. Ayub and A. Selwal, "An improved image steganography technique using edge based data hiding in DCT domain," *J. Interdiscip. Math.*, vol. 23, no. 2, pp. 357–366, 2020. doi: 10.1080/09720502.2020.1731949.

[14] G. Xie, J. Ren, S. Marshall, H. Zhao, and H. Li, "A new cost function for spatial image steganography based on 2D-SSA and WMF," *IEEE Access*, vol. 9, pp. 30604–30614, 2021. doi: 10.1109/ACCESS.2021.3059690.

[15] J. Liu *et al.*, "Recent advances of image steganography with generative adversarial networks," *IEEE Access*, vol. 8, pp. 60575–60597, 2020. doi: 10.1109/ACCESS.2020.2983175.

[16] M. Sharifzadeh, M. Aloraini, and D. Schonfeld, "Adaptive batch size image merging steganography and quantized Gaussian image steganography," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 867–879, 2020. doi: 10.1109/TIFS.2019.2929441.

[17] R. Wazirali, W. Alasmary, M. Mahmoud, and A. Alhindi, "An optimized steganography hiding capacity and imperceptibly using genetic algorithms," *IEEE Access*, vol. 7, pp. 133496–133508, 2019. doi: 10.1109/ACCESS.2019.2941440.

[18] A. I. Basuki and D. Rosiyadi, "Joint transaction-image steganography for high capacity covert communication," in *Proc. IEEE IC3INA*, Tangerang, Indonesia, 2019, pp. 41–46.

[19] J. H. Qin, Y. J. Luo, X. Y. Xiang, Y. Tan, and H. J. Huang, "Coverless image steganography: A survey," *IEEE Access*, vol. 7, pp. 171372–171394, 2019. doi: 10.1109/ACCESS.2019.2955452.

[20] A. Darbani, A. Nezhadi, and M. Forghani, "A new steganography method for embedding message in JPEG images," in *Proc. 2019 5th KBEI*, Tehran, Iran, 2019, pp. 617–621.

[21] S. Pramanik, D. Samanta, S. K. Bandyopadhyay, and R. Ghosh, "A new combinational technique in image steganography," *Int. J. Inf. Secur. Priv.*, vol. 15, no. 3, pp. 48–64, 2021. doi: 10.4018/IJISP.2021070104.

[22] X. Liao, J. Yin, M. Chen, and Z. Qin, "Adaptive payload distribution in multiple images steganography based on image texture features," *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 2, pp. 897–911, 2020. doi: 10.1109/TDSC.2020.3004708.

[23] S. Dhawan and R. Gupta, "Analysis of various data security techniques of steganography: A survey," *Inf. Secur. J. Glob. Prspect.*, vol. 30, no. 2, pp. 63–87, 2021. doi: 10.1080/19393555.2020.1801911.

[24] C. Zhang, P. Benz, A. Karjauv, G. Sun, and I. S. Kweon, "Universal deep hiding for steganography, watermarking, and light field messaging," *Adv. Neural. Inf. Process*, vol. 33, pp. 10223–10234, 2020.

[25] M. Kumar, S. Kumar, and H. Nagar, "Comparative analysis of different steganography technique for image or data security," *Int. J. Adv. Sc. & Technol.*, vol. 29, no. 4, pp. 11246–11253, 2020.

[26] D. Laishram and T. Tuithung, "A novel minimal distortion-based edge adaptive image steganography scheme using local complexity," *Multimed. Tools Appl.*, vol. 80, no. 1, pp. 831–854, 2021. doi: 10.1007/s11042-020-09519-9.

[27] B. K. Pandey *et al.*, "Secure text extraction from complex degraded images by applying steganography and deep learning," in *Proc. Multidiscip. Approach Mod. Digit. Steganography*, Chennai, India, 2021, pp. 146–163.

[28] B. L. Sirisha and M. B. Chandra, "Review on spatial domain image steganography techniques," *J. Discret Math. Sci. Cryptogr.*, vol. 24, no. 6, pp. 1873–1883, 2021. doi: 10.1080/09720529.2021.1962025.

[29] A. Zenati, W. Ouarda, and A. M. Alimi, "SSDIS-BEM: A new signature steganography document image system based on beta elliptic modeling," *Eng. Sci. Technol. Int.*, vol. 23, no. 3, pp. 470–482, 2020. doi: 10.1016/j.jestch.2019.09.002.

[30] T. AlKhodaidi and A. Gutub, "Refining image steganography distribution for higher security multimedia counting-based secret-sharing," *Multimed. Tools Appl.*, vol. 80, no. 1, pp. 1143–1173, 2021. doi: 10.1007/s11042-020-09720-w.

[31] A. G. Benedict, "Improved file security system using multiple image steganography," in *Proc. ICDSC*, Ghaziabad, India, 2019, pp. 1–5.

[32] O. Rachael, S. Misra, R. Ahuja, A. Adewumi, F. Ayeni and R. Mmaskeliunas, "Image steganography and steganalysis based on least significant bit (LSB)," in *Proc. ETIT*, Chennai, India, 2019, pp. 1100–1111.

[33] Y. Yigit and M. Karabatak, "A stenography application for hiding student information into an image," in *Proc. 7th ISDFS*, Barcelos, Portugal, 2019, pp. 1–4.

[34] S. Farrag and W. Alexan, "A high capacity geometrical domain based 3D image steganography scheme," in *Proc. IEEE ICACTN*, Rabat, Morocco, 2019, pp. 1–7.

[35] O. C. Abikoye, U. A. Ojo, J. B. Awotunde, and R. Ogundokun, "A safe and secured iris template using steganography and cryptography," *Multimed. Tools Appl.*, vol. 79, no. 8, pp. 23483–23506, 2020. doi: 10.1007/s11042-020-08971-x.

[36] M. S. Subhedar and V. H. Mankar, "Image steganography using contourlet transform and matrix decomposition techniques," *Multimed. Tools Appl.*, vol. 78, no. 7, pp. 22155–22181, 2019. doi: 10.1007/s11042-019-7512-9.

[37] L. Zhang, W. Qin, K. Chen, W. Zhou, and N. Yu, "Adversarial batch image steganography against CNN-based pooled steganalysis," *Signal Process.*, vol. 181, no. 7, pp. 107–120, 2021. doi: 10.1016/j.sigpro.2020.107920.

[38] Z. A. Alwan, H. M. Farhan, and S. Q. Mahdi, "Color image steganography in YCbCr space," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 1, pp. 202–209, 2020. doi: 10.11591/ijece.v10i1.pp202-209.

[39] M. S. Taha, M. S. Rahim, S. A. Lafta, M. M. Hashim, and H. M. Alzuabidi, "Combination of steganography and cryptography: A short survey," *IOP Conf. Ser.: Mater. Sci. Eng.*, vol. 518, no. 5, pp. 309–313, 2019. doi: 10.1088/1757-899X/518/5/052003.

[40] Y. Wang, W. Zhang, W. Li, X. Yu, and N. Yu, "Non-additive cost functions for color image steganography based on inter-channel correlations and differences," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, no. 2, pp. 2081–2095, 2019. doi: 10.1109/TIFS.2019.2956590.

[41] X. Liao, Y. Yu, Z. Li, and Z. Qin, "A new payload partition strategy in color image steganography," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 30, no. 3, pp. 685–696, 2019. doi: 10.1109/TCSVT.2019.2896270.

[42] D. Watni and S. Chawla, "A comparative evaluation of JPEG steganography," in *Proc. 5th ISPCC*, Solan, India, 2019, pp. 36–40.

[43] Y. Luo, J. Qin, X. Xiang, and Y. Tan, "Coverless image steganography based on multi-object recognition," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 31, no. 7, pp. 2779–2791, 2020. doi: 10.1109/TCSVT.2020.3033945.

[44] M. T. Elkandoz, W. Alexan, and H. Hussein, "3D image steganography using sine logistic map and 2D hyperchaotic map," in *Proc. ICECTA*, Ras Al Khaimah, United Arab Emirates, 2019, pp. 1–6.

[45] S. A. Nie, G. Sulong, R. Ali, and A. Abel, "The use of least significant bit (LSB) and knight tour algorithm for image steganography of cover image," *Int. J. Electr. Comput. Eng.*, vol. 9, no. 6, pp. 5218–5226, 2019. doi: 10.11591/ijece.v9i6.pp5218-5226.

[46] M. K. Shyla, K. S. Kumar, and R. K. Das, "Image steganography using genetic algorithm for cover image selection and embedding," *Soft. Comput.*, vol. 3, no. 2, pp. 110–121, 2021. doi: 10.1016/j.socl.2021.100021.

[47] I. Aqeel and M. B. Suleman, "A survey on digital image steganography approaches," in *Proc. ITAC*, Bahawalpur, Pakistan, 2019, pp. 769–778.

[48] S. Rustad, A. Syukur, and P. N. Andono, "Inverted LSB image steganography using adaptive pattern to improve imperceptibility," *J. King Saud. Univ. Comput. Inf. Sci.*, vol. 34, no. 6, pp. 3559–3568, 2022. doi: 10.1016/j.jksuci.2020.12.017.

[49] A. A. Eyssa, F. E. Abdelsamie, and A. E. Abdelnaiem, "An efficient image steganography approach over wireless communication system," *Wirel. Pers. Commun.*, vol. 111, no. 1, pp. 321–337, 2023. doi: 10.1007/s11277-019-06730-2.

[50] A. ALabaichi, M. A. Al-Dabbas, and A. Salih, "Image steganography using least significant bit and secret map techniques," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 1, pp. 2088–8708, 2020. doi: 10.11591/ijece.v10i1.pp935-946.

[51] A. Al-Ahmad, O. S. Almousa, and Q. Abuein, "Enhancing steganography by image segmentation and multi-level deep hiding," *Int. J. Commun. Netw. Inf. Secur.*, vol. 13, no. 1, pp. 143–150, 2021.

[52] G. F. Siddiqui *et al.*, "A dynamic three-bit image steganography algorithm for medical and e-healthcare systems," *IEEE Access*, vol. 8, no. 18, pp. 181893–181903, 2020. doi: 10.1109/ACCESS.2020.3028315.

[53] A. Samir, W. Alexan, R. R. Eddin, and A. El-Rafei, "Steganography by random shuffling of image contents using residue model," in *Proc. IEEE 4th ICECA*, Coimbatore, India, 2020, pp. 912–918.

[54] W. She, L. Huo, Z. Tian, Y. Zhuang, C. Niu and W. Liu, "A double steganography model combining blockchain and interplanetary file system," *Peer Peer Netw. Appl.*, vol. 14, no. 5, pp. 3029–3042, 2021. doi: 10.1007/s12083-021-01143-0.

[55] E. S. Hureib and A. Gutub, "Enhancing medical data security via combining elliptic curve cryptography and image steganography," *Int. J. Comput. Netw. Secur.*, vol. 20, no. 8, pp. 1–8, 2020.

[56] D. Darwis and N. B. Pamungkas, "Comparison of least significant bit, pixel value differencing, and modulus function on steganography to measure image quality, storage capacity, and robustness," *J. Phys.*, vol. 1751, no. 1, pp. 12039–12048, 2021. doi: 10.1088/1742-6596/1751/1/012039.

[57] X. Duan, W. Wang, N. Liu, D. Yue, Z. Xie and C. Qin, "StegoPNet: Image steganography with generalization ability based on pyramid pooling module," *IEEE Access*, vol. 8, pp. 195253–195262, 2020. doi: 10.1109/ACCESS.2020.3033895.

[58] A. Gutub and H. Al-Shaarani, "Efficient implementation of multi-image secret hiding based on LSB and DWT steganography comparisons," *Arab. J. Sci. Eng.*, vol. 45, no. 4, pp. 2631–2644, 2020. doi: 10.1007/s13369-020-04413-w.

[59] O. Elharrouss, N. Almaadeed, and S. Al-Maadeed, "An image steganography approach based on k-least significant bits (k-LSB)," in *Proc. IEEE ICIoT*, Doha, Qatar, 2020, pp. 131–135.

[60] S. S. Yadahalli, S. Rege, and R. Sonkusare, "Implementation and analysis of image steganography using least significant bit and discrete wavelet transform techniques," in *Proc. 5th ICCES*, Coimbatore, India, 2020, pp. 1325–1330.

[61] A. Tiwari, G. Shankar, and B. B. Jain, "Comparative analysis of different steganography technique for image security," *Int. J. Eng. Trends. Appl.*, vol. 8, no. 2, pp. 6–9, 2021.

[62] E. H. J. Halboos and A. M. Albakry, "Improve steganography system using agents software based on statistical and classification technique," *Bull. Electr. Eng. Inform.*, vol. 12, no. 3, pp. 1595–1606, 2023. doi: 10.11591/eei.v12i3.4540.

[63] H. N. AlEisa, "Data confidentiality in healthcare monitoring systems based on image steganography to improve the exchange of patient information using the Internet of Things," *J. Healthc. Eng.*, vol. 45, no. 3, pp. 11–234, 2022. doi: 10.1155/2022/7528583.

[64] Z. Wang, W. Li, and G. Wang, "Information steganography technology of optical communication sensor network based on virtual reality technology," *J. Sensors*, vol. 12, no. 3, pp. 34–134, 2022. doi: 10.1155/2022/4827306.

[65] A. A. Mawgoud, M. H. N. Taha, A. Abu-Talleb, and A. Kotb, "A deep learning based steganography integration framework for ad-hoc cloud computing data security augmentation using the V-BOINC system," *J. Cloud Comput.*, vol. 11, no. 1, pp. 97–115, 2022. doi: 10.1186/s13677-022-00339-w.

[66] S. Dhawan, C. Chakraborty, J. Frnda, R. Gupta, A. K. Rana and S. K. Pani, "SSII: Secured and high-quality steganography using intelligent hybrid optimization algorithms for IoT," *IEEE Access*, vol. 9, pp. 87563–87578, 2021. doi: 10.1109/ACCESS.2021.3089357.

[67] C. L. Chen, Y. X. Chen, C. F. Lee, Y. Y. Deng, and C. H. Chen, "An efficient and secure key agreement protocol for sharing emergency events in VANET systems," *IEEE Access*, vol. 7, pp. 148472–148484, 2019. doi: 10.1109/ACCESS.2019.2946969.

[68] A. Chhabra, T. Woeden, D. Singh, M. Rakhra, O. Dahiya and A. Gupta, "Image steganalysis with image decoder using LSB and MSB technique," in *Proc. 2022 3rd ICIEM*, Bangulor, India, 2022, pp. 900–905.

[69] I. J. Yu, S. H. Nam, W. Ahn, M. J. Kwon, and H. K. Lee, "Manipulation classification for JPEG images using multi-domain features," *IEEE Access*, vol. 8, pp. 210837–210854, 2020. doi: 10.1109/ACCESS.2020.3037735.

[70] A. A. Almohammedi, and V. Shepelev, "Saturation throughput analysis of steganography in the IEEE 802.11p protocol in the presence of non-ideal transmission channel," *IEEE Access*, vol. 9, pp. 14459–14469, 2021. doi: 10.1109/ACCESS.2021.3052464.

[71] J. Wang, C. Yang, P. Wang, X. Song, and J. Lu, "Payload location for JPEG image steganography based on co-frequency sub-image filtering," *Int. J. Distrib. Sens. Netw.*, vol. 16, no. 1, pp. 1– 16, 2020. doi: 10.1177/1550147719899569.

[72] V. Kumar, H. Kaur, and S. Paul, "CryptMe: A cryptographic framework with steganography for securing data," in *Proc. IEEE 2nd ICIEM*, London, UK, 2021, pp. 294–299.

[73] D. Li and P. Kar, "B-spot: Blockchain and steganography based robust and secure photo transmission mechanism," *J. Mob. Multimed.*, vol. 23, no. 4, pp. 1677–1708, 2022. doi: 10.13052/jmm1550-4646.18610.

[74] C. Yang, Y. Kang, F. Liu, X. Song, J. Wang and X. Luo, "Color image steganalysis based on embedding change probabilities in differential channels," *Int. J. Distrib. Sens. Netw.*, vol. 16, no. 5, pp. 1–10, 2020. doi: 10.1177/1550147720917826.

[75] Z. Jin, Y. Yang, Y. Chen, and Y. Chen, "IAS-CNN: Image adaptive steganalysis via convolutional neural network combined with selection channel," *Int. J. Distrib. Sens. Netw.*, vol. 16, no. 3, pp. 1–9, 2020. doi: 10.1177/1550147720911002.

[76] L. A. Ajao, B. U. Umar, D. O. Olajide, and S. Misra, "Application of crypto-blockchain technology for securing electronic voting systems," in *Blockchain Applications in the Smart Era*, Roorkee, India, Cham: Springer International Publishing, 2022, vol. 34, pp. 85–105.

[77] K. Manchanda and A. Sing, "Covert communication in VANETS using Internet protocol header bit," *Int. J. Comp. Appl.*, vol. 123, no. 17, pp. 10–14, 2015.

[78] O. Evsutin, A. Melman, and R. Meshcheryakov, "Digital steganography and watermarking for digital images: A review of current research directions," *IEEE Access*, vol. 8, pp. 166589–166611, 2020. doi: 10.1109/ACCESS.2020.3022779.

[79] A. K. Sahu, and M. Sahu, "Digital image steganography and steganalysis: A journey of the past three decades," *Open Computer Science*, vol. 10, no. 1, pp. 296–342, 2020. doi: 10.1515/comp-2020-0136.

[80] 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, no. 1, pp. 299–326, 2019. doi: 10.1016/j.neucom.2018.06.075.

[81] B. F. Alatiyyat and C. Narmatha, "Survey on image steganography techniques," in *Proc. 2nd ICCIT*, Tabuk, Saudi Arabia, 2022, pp. 57–64.

[82] D. A. Shehab and M. J. Alhaddad, "Comprehensive survey of multimedia steganalysis: Techniques, evaluations, and trends in future research," *Symmetry*, vol. 14, no. 1, pp. 117–125, 2022. doi: 10.3390/sym14010117.

[83] M. V. Athira and D. M. Khan, "Recent trends on object detection and image classification: A review," in *Proc. ICComPE*, Chennai, India, 2020, pp. 427–435.

[84] H. Zhou, W. Zhang, K. Chen, W. Li, and N. Yu, "Three-dimensional mesh steganography and steganalysis: A review," *IEEE Trans. Vis Comput. Graph.*, vol. 28, no. 12, pp. 5006–5025, 2021. doi: 10.1109/TVCG.2021.3075136.

[85] W. A. Awadh, A. S. Hashim, and A. Hamoud, "A review of various steganography techniques in cloud computing," *Univ. Thi-Qar J. Sci.*, vol. 7, no. 1, pp. 113–119, 2019.

[86] M. A. Majeed, R. Sulaiman, Z. Shukur, and M. K. Hasan, "A review on text steganography techniques," *Math.*, vol. 9, no. 21, pp. 2829–2837, 2021. doi: 10.3390/math9212829.
[87] M. S. Subhedar and V. H. Mankar, "Current status and key issues in image steganography: A survey," *Comput. Sci. Rev.*, vol. 13, no. 1, pp. 95–113, 2014. doi: 10.1016/j.cosrev.2014.09.001.
[88] R. Gurunath, A. H. Alahmadi, D. Samanta, M. Z. Khan, and A. Alahmadi, "A novel approach for linguistic steganography evaluation based on artificial neural networks," *IEEE Access*, vol. 9, pp. 120869–120879, 2021. doi: 10.1109/ACCESS.2021.3108183.
[89] W. Luo, F. Huang, and J. Huang, "Edge adaptive image steganography based on LSB matching revisited," *IEEE Trans. Inf. Forensics Secur.*, vol. 5, no. 2, pp. 201–214, 2010. doi: 10.1109/TIFS.2010.2041812.
[90] S. Saraireh, "A secure data communication system using cryptography and steganography," *Int. J. Comput. Netw. Commun.*, vol. 5, no. 3, pp. 125–137, 2013. doi: 10.5121/ijcnc.2013.5310.
[91] J. R. Jayapandiyan, C. Kavitha, and K. Sakthivel, "Enhanced least significant bit replacement algorithm in spatial domain of steganography using character sequence optimization," *IEEE Access*, vol. 8, pp. 136537–136545, 2020. doi: 10.1109/ACCESS.2020.3009234.
[92] M. Fakhredanesh, M. Rahmati, and R. Safabakhsh, "Steganography in discrete wavelet transform based on human visual system and cover model," *Multimed. Tools Appl.*, vol. 78, no. 2, pp. 18475–18502, 2019. doi: 10.1007/s11042-019-7238-8.
[93] D. Pandey *et al.*, "Secret data transmission using advanced steganography and image compression," *Int. J. Nonlinear Anal. Appl.*, vol. 12, no. 1, pp. 1243–1257, 2021. doi: 10.22075/IJNAA.2021.5635.
[94] P. D. Shah and R. S. Bichkar, "Secret data modification based image steganography technique using genetic algorithm having a flexible chromosome structure," *Eng. Sci. Technol. Int. J.*, vol. 24, no. 3, pp. 782–794, 2021. doi: 10.1016/j.jestch.2020.11.008.
[95] R. Das and T. Tuithung, "A novel steganography method for image based on Huffman encoding," in *Proc. 3rd NCETACS*, Bangalore, India, 2012, pp. 14–18.
[96] A. Nag, S. Biswas, D. Sarkar, and P. P. Sarkar, "A novel technique for image steganography based on block-DCT and Huffman encoding," *Int. J. Comput. Sci. Inf. Technol.*, vol. 5, no. 1, pp. 1006–1186, 2010.
[97] S. Atawneh, A. Almomani, H. Al Bazar, P. Sumari, and B. Gupta, "Secure and imperceptible digital image steganographic algorithm based on diamond encoding in DWT domain," *Multimed. Tools Appl.*, vol. 76, no. 1, pp. 18451–18472, 2017. doi: 10.1007/s11042-016-3930-0.
[98] A. Singh and H. Singh, "An improved LSB based image steganography technique for RGB images," in *Proc. ICECCT*, Coimbatore, India, 2015, pp. 1–4.
[99] Y. Qiu, Z. Qian, H. Zeng, X. Lin, and X. Zhang, "Reversible data hiding in encrypted images using adaptive reversible integer transformation," *Signal Process.*, vol. 167, no. 1, pp. 107288–10729301, 2020. doi: 10.1016/j.sigpro.2019.107288.
[100] D. R. Sridevi, P. Vijaya, and K. S. Rao, "Image steganography combined with cryptography," *Council. Innov. Res. Peer. Rev. Res. Publi. Sys. J.*, vol. 9, no. 1, pp. 1231–1239, 2013.
[101] L. Riley, J. K. Mandal, and D. Das, "Colour image steganography based on pixel value differencing in spatial domain," *Int. J. Inf. Sci. Tech.*, vol. 2, no. 1, pp. 112–119, 2012.
[102] W. Luo, F. Huang, and J. Huang, "A more secure steganography based on adaptive pixel-value differencing scheme," *Multimed. Tools Appl.*, vol. 52, no. 2, pp. 407–430, 2011. doi: 10.1007/s11042-009-0440-3.
[103] G. Swain and S. K. Lenka, "Classification of image steganography techniques in spatial domain: A study," *Int. J. Comput. Sci. Eng. Technol.*, vol. 5, no. 3, pp. 219–232, 2014.
[104] Z. Zhou, H. Sun, R. Harit, X. Chen, and X. Sun, "Coverless image steganography without embedding," in *Proc. ICCCS*, Nanjing, China, 2015, pp. 13–15.
[105] S. Arora and S. Anand, "A new approach for image steganography using edge detection method," *Int. J. Innov. Res. Comput. Comms. Eng.*, vol. 1, no. 3, pp. 626–629, 2013. doi: 10.32628/IJSRSET1732217.
[106] R. D. Rashid, "Robust steganographic techniques for secure biometric-based remote authentication," Ph.D. dissertation, Univ. of Buckingham, London, UK, 2015.
[107] G. Swain, "Adaptive pixel value differencing steganography using both vertical and horizontal edges," *Multimed. Tools Appl.*, vol. 75, no. 21, pp. 13541–13556, 2016. doi: 10.1007/s11042-015-2937-2.

[108] B. Feng, W. Lu, and W. Sun, "Secure binary image steganography based on minimizing the distortion on the texture," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 2, pp. 243–255, 2014. doi: 10.1109/TIFS.2014.2368364.
[109] A. Arya and S. Soni, "Performance evaluation of secrete image steganography techniques using least significant bit (LSB) method," *Int. J. Comput. Sci. Trends. Technol.*, vol. 6, no. 2, pp. 160–165, 2018.
[110] K. Al-Afandy, O. S. Faragallah, A. ELmhalawy, E. S. M. El-Rabaie, and G. M. El-Banby, "High security data hiding using image cropping and LSB least significant bit steganography," in *Proc. 4th IEEE CiSt*, Tangier, Morocco, 2016, pp. 400–404.
[111] N. Patel and S. Meena, "LSB based image steganography using dynamic key cryptography," in *Proc. ICETCT*, Dehradun, India, 2016, pp. 1–5.
[112] H. W. Tseng and H. Leng, "A steganographic method based on pixel-value differencing and the perfect square number," *J. Appl. Math.*, vol. 13, no. 4, pp. 1613–1626, 2013. doi: 10.1155/2013/189706.
[113] J. F. Liu, Y. G. Tian, T. Han, C. F. Yang, and W. B. Liu, "LSB steganographic payload location for JPEG-decompressed images," *Digit. Signal Process.*, vol. 38, no. 1, pp. 66–76, 2015. doi: 10.1016/j.dsp.2014.12.004.
[114] A. Cheddad, J. Condell, K. Curran, and P. Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Process.*, vol. 90, no. 3, pp. 727–752, 2010. doi: 10.1016/j.sigpro.2009.08.010.
[115] K. Zaidoon, A. A. Zaidan, B. B. Zaidan, and H. O. Alanazi, "Overview: Main fundamentals for steganography," *J. Comput.*, vol. 2, no. 3, pp. 158–165, 2010.
[116] Q. Wang, X. Gong, G. T. Nguyen, A. Houmansadr, and N. Borisov, "CensorSpoofer: Asymmetric communication using IP spoofing for censorship-resistant web browsing," in *Proc. ACM Conf. Comput. Commun. Secur.*, Urbana, USA, 2012, pp. 121–132.
[117] S. Ashwin, J. Ramesh, S. A. Kumar, and K. Gunavathi, "Novel and secure encoding and hiding techniques using image steganography: A survey," in *Proc. ICETEEEM*, Bangalore, India, 2012, pp. 171–177.
[118] Y. Qian, J. Dong, W. Wang, and T. Tan, "Deep learning for steganalysis via convolutional neural networks," *Med. Watermarking, Secur. Forensic.*, vol. 94, no. 9, pp. 171–180, 2015. doi: 10.1117/12.2083479.
[119] S. Agarwal and K. H. Jung, "Identification of content-adaptive image steganography using convolutional neural network guided by high-pass kernel," *Appl. Sci.*, vol. 12, no. 22, pp. 11869–11880, 2022. doi: 10.3390/app122211869.
[120] Y. L. Lee and W. H. Tsai, "A new secure image transmission technique via secret-fragment-visible mosaic images by nearly reversible color transformations," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 24, no. 4, pp. 695–703, 2013. doi: 10.1109/TCSVT.2013.2283431.
[121] Y. Benlcouiri, M. Ismaili, A. Azizi, and M. Benabdellah, "Securing images by secret key steganography," *Appl. Math. Sci.*, vol. 6, no. 11, pp. 5513–5523, 2012.
[122] X. Duan, K. Jia, B. Li, D. Guo, E. Zhang and C. Qin, "Reversible image steganography scheme based on a U-Net structure," *IEEE Access*, vol. 7, pp. 9314–9323, 2019. doi: 10.1109/ACCESS.2019.2891247.
[123] Z. Fu, F. Wang, and X. Cheng, "The secure steganography for hiding images via GAN," *EURASIP J. Image Video Process.*, vol. 1, pp. 46–53, 2020. doi: 10.1186/s13640-020-00534-2.
[124] A. A. Abdulla, "Exploiting similarities between secret and cover images for improved embedding efficiency and security in digital steganography," Ph.D. dissertation, Univ. of Buckingham, UK, 2015.
[125] Z. Wang, N. Gao, X. Wang, J. Xiang, and G. Liu, "A style transformation network for deep image steganography," in *Proc. ICONP*, Sydney, NSW, Australia, 2019, pp. 1120–1132.
[126] I. Goodfellow *et al.*, "Generative adversarial nets," *Adv. Neural Inf. Process.*, vol. 27, no. 1, pp. 1–9, 2014.
[127] J. Gauthier, "Conditional generative adversarial nets for convolutional face generation," *Class Project for Stanford CS231N Convolutional Neural Netw. for Vis. Recognit. Winter Semester*, vol. 2014, no. 5, 2014.
[128] R. Zhang, S. Dong, and J. Liu, "Invisible steganography via generative adversarial networks," *Multimed. Tools Appl.*, vol. 78, no. 1, pp. 8559–8575, 2019. doi: 10.1007/s11042-018-6951-z.
[129] A. Radford, L. Metz, and S. Chintala, "Unsupervised representation learning with deep convolutional generative adversarial networks," arXiv:1511.06434, 2015.

[130] E. L. Denton, S. Chintala, and R. Fergus, "Deep generative image models using Laplacian pyramid of adversarial networks," *Adv. Neural Inf. Process*, vol. 28, no. 1, pp. 1–9, 2015.
[131] S. Bhattacharyya, "A survey of steganography and steganalysis technique in image, text, audio and video as cover carrier," *J. Glob. Res. Comput. Sci.*, vol. 2, no. 4, pp. 1– 16, 2011.
[132] W. Mazurczyk and L. Caviglione, "Steganography in modern smartphones and mitigation techniques," *IEEE Commun. Surv. Tutor.*, vol. 17, no. 1, pp. 334–357, 2014. doi: 10.1109/COMST.2014.2350994.
[133] V. Sedighi, R. Cogranne, and J. Fridrich, "Content-adaptive steganography by minimizing statistical detectability," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 2, pp. 221–234, 2015. doi: 10.1109/TIFS.2015.2486744.
[134] Z. Eslami, S. H. Razzaghi, and J. Z. Ahmadabadi, "Secret image sharing based on cellular automata and steganography," *Pattern Recognit.*, vol. 43, no. 1, pp. 397–404, 2010. doi: 10.1016/j.patcog.2009.06.007.
[135] D. Volkhonskiy, B. Borisenko, and E. Burnaev, "Generative adversarial networks for image steganography," in *Proc. ICLR*, Kigali, Rawanda, 2017, pp. 1–8.
[136] X. Liu and H. Cho-Jui, "Rob-GAN: Generator, discriminator, and adversarial attacker," in *Proc. of the IEEE/CVF*, Long Beach CA, USA, 2019, pp. 11234–11243.
[137] N. Meghanathan and L. Nayak, "Steganalysis algorithms for detecting the hidden information in image, audio and video cover media," *Int. J. Netw. Secur. Appl*, vol. 2, no. 1, pp. 43–55, 2010.
[138] G. Chen, Q. Chen, and D. Zhang, "Discriminative multimodal for steganalysis," in *Proc. 8th CISP*, Shenyang, China, 2015, pp. 809–813.
[139] S. Tan and B. Li, "Stacked convolutional auto-encoders for steganalysis of digital images," in *Proc. APSIPA*, Siem Reap, Cambodia, 2014, pp. 1–4.
[140] A. Cheddad, J. Condell, K. Curran, and P. McKevitt, "A hash-based image encryption algorithm," *Opt. Commun.*, vol. 283, no. 6, pp. 879–893, 2010. doi: 10.1016/j.optcom.2009.10.106.
[141] C. Li, Y. Jiang, and M. Cheslyar, "Embedding image through generated intermediate medium using deep convolutional generative adversarial network," *Comput. Mater. Contin.*, vol. 56, no. 2, pp. 313–324, 2018.
[142] A. D. Ker *et al.*, "Moving steganography and steganalysis from the laboratory into the real world," in *Proc. 1st ACM Workshop Inf. Hiding Multimed. secur.*, Wellington, New Zealand, 2013, pp. 45–58.
[143] J. Hayes and G. Danezis, "Generating steganographic images via adversarial training," *Adv. Neural Inf. Process*, vol. 30, no. 2, pp. 1–10, 2017.
[144] J. Yang, D. Ruan, J. Huang, X. Kang, and Y. Q. Shi, "An embedding cost learning framework using GAN," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 839–851, 2019. doi: 10.1109/TIFS.2019.2922229.
[145] M. Hussain, A. W. A. Wahab, A. T. Ho, N. Javed, and K. H. Jung, "A data hiding scheme using parity-bit pixel value differencing and improved rightmost digit replacement," *Signal Process. Image Commun.*, vol. 50, no. 2, pp. 44–57, 2017. doi: 10.1016/j.image.2016.10.005.
[146] G. Swain, "Adaptive and non-adaptive PVD steganography using overlapped pixel blocks," *Arab. J. Sci. Eng.*, vol. 43, no. 12, pp. 7549–7562, 2018. doi: 10.1007/s13369-018-3163-9.
[147] A. M. Hameed, S. Aly, and M. Hassaballah, "An efficient data hiding method based on adaptive directional pixel value differencing (ADPVD)," *Multimed. Tools Appl.*, vol. 77, no. 7, pp. 14705–14723, 2018. doi: 10.1007/s11042-017-5056-4.
[148] H. H. Liu, Y. C. Lin, and C. M. Lee, "A digital data hiding scheme based on pixel-value differencing and side match method," *Multimed. Tools Appl.*, vol. 78, no. 9, pp. 12157–12181, 2019. doi: 10.1007/s11042-018-6766-y.
[149] I. R. Grajeda-Marín, M. Venegas, H. A. Marcial-Romero, J. R. Hernández-Servín, J. A. Muñoz-Jiménez and G. De Ita, "A new optimization strategy for solving the fall-off boundary value problem in pixel-value differencing steganography," *Int. J. Pattern Recognit. Artif. Intell.*, vol. 32, no. 1, pp. 1860010:1–1860010:17, 2017. doi: 10.1142/S0218001418600108.
[150] P. H. Kim, E. J. Yoon, K. W. Ryu, and K. H. Jung, "Data-hiding scheme using multidirectional pixel-value differencing on colour images," *Secur. Commun. Netw.*, vol. 2019, no. 8, pp. 1–11, 2019. doi: 10.1155/2019/5323578.

[151] H. C. Wu, N. I. Wu, C. S. Tsai, and M. S. Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods," *IEEE Proc.–Vision, Image Signal Process.*, vol. 152, no. 5, pp. 611–615, 2005. doi: 10.1049/ip-vis:20059022.
[152] D. C. Wu and W. H. Tsai, "A steganographic method for images by pixel-value differencing," *Pattern Recogn. Lett.*, vol. 24, no. 9, pp. 1613–1626, 2003. doi: 10.1016/S0167-8655(02)00402-6.
[153] K. H. Jung, "Data hiding scheme improving embedding capacity using mixed PVD and LSB on bit plane," *J. Real. Time Image Process.*, vol. 14, no. 2, pp. 127–136, 2018. doi: 10.1007/s11554-017-0719-y.
[154] M. Khodaei and K. Faez, "New adaptive steganographic method using least-significant-bit substitution and pixel-value differencing," *IET Image Process.*, vol. 6, no. 6, pp. 677–686, 2012. doi: 10.1049/iet-ipr.2011.0059.
[155] A. A. Zakaria, M. Hussain, A. W. Wahab, M. Y. Idris, N. A. Abdullah and K. H. Jung, "High-capacity image steganography with minimum modified bits based on data mapping and LSB substitution," *Appl. Sci.*, vol. 8, no. 11, pp. 2199–2217, 2018. doi: 10.3390/app8112199.
[156] A. K. Sahu and G. Swain, "A novel n-rightmost bit replacement image steganography technique," *3D Res.*, vol. 10, no. 1, pp. 1–18, 2019. doi: 10.1007/s13319-018-0211-x.
[157] A. K. Sahu and G. Swain, "A novel multi stego-image based data hiding method for gray scale image," *Pertanika J. Sci. & Technol.*, vol. 27, no. 2, pp. 753–768, 2019.
[158] R. Shreelekshmi, M. Wilscy, and C. V. Madhavan, "Undetectable least significant bit replacement steganography," *Multimed. Tools Appl.*, vol. 78, no. 8, pp. 10565–10582, 2019. doi: 10.1007/s11042-018-6541-0.
[159] Z. Qu, Z. Cheng, W. Liu, and X. Wang, "A novel quantum image steganography algorithm based on exploiting modification direction," *Multimed. Tools Appl.*, vol. 78, no. 1, pp. 7981–8001, 2019. doi: 10.1007/s11042-018-6476-5.
[160] M. Asad, J. Gilani, and A. Khalid, "An enhanced least significant bit modification technique for audio steganography," in *Proc. IEEE ICCNIT*, Abbottabad, Pakistan, 2011, pp. 143–147.
[161] C. Yuan, H. Wang, P. He, J. Luo, and B. Li, "GAN-based image steganography for enhancing security via adversarial attack and pixel-wise deep fusion," *Multimed. Tools Appl.*, vol. 81, no. 5, pp. 6681–6701, 2022. doi: 10.1007/s11042-021-11778-z.
[162] K. Muhammad, J. Ahmad, S. Rho, and S. W. Baik, "Image steganography for authenticity of visual contents in social networks," *Multimed. Tools Appl.*, vol. 76, no. 18, pp. 18985–19004, 2017. doi: 10.1007/s11042-017-4420-8.
[163] Y. Luo, C. Yao, Y. Mo, B. Xie, G. Yang and H. Gui, "A creative approach to understanding the hidden information within the business data using deep learning," *Inform Process Manag.*, vol. 58, no. 5, pp. 102615, 2021. doi: 10.1016/j.ipm.2021.102615.
[164] A. Aljarf, H. Zamzami, and A. Gutub, "Integrating machine learning and features extraction for practical reliable color images steganalysis classification," *Soft. Comput.*, vol. 1, no. 19, pp. 1–12, 2023. doi: 10.1007/s00500-023-09042-7.
[165] R. Cogranne, Q. Giboulot, and P. Bas, "Challenging academic research on steganalysis with realistic images," in *Proc. IEEE WIFS*, New York, NY, USA, 2020, pp. 1–5.
[166] M. Garg, J. S. Ubhi, and A. K. Aggarwal, "Neural style transfers for image steganography and destylization with supervised image to image translation," *Multimed. Tools Appl.*, vol. 82, no. 19–20, pp. 6271–6288, 2023. doi: 10.1007/s11042-022-13596-3.
[167] K. Cheng, R. Tahir, L. K. Eric, and M. Li, "An analysis of generative adversarial networks and variants for image synthesis on MNIST dataset," *Multimed. Tools Appl.*, vol. 79, no. 19–20, pp. 13725–13752, 2020. doi: 10.1007/s11042-019-08600-2.
[168] S. Islam, M. R. Modi, and P. Gupta, "Edge-based image steganography," *EURASIP J. Inf. Secur.*, vol. 1, no. 4, pp. 1–14, 2014. doi: 10.1186/1687-417X-2014-8.
[169] A. D. Ker *et al.*, "Moving steganography and steganalysis from the laboratory into the real world," in *Proc. 1st ACM Workshop Inf. Hiding Multimed. Secur.*, New York, USA, 2013, pp. 45–58.

[170] R. Cogranne and J. Fridrich, "Modeling and extending the ensemble classifier for steganalysis of digital images using hypothesis testing theory," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 12, pp. 2627–2642, 2015. doi: 10.1109/TIFS.2015.2470220.
[171] J. Kour and D. Verma, "Steganography techniques: A review paper," *Int. J. Emerg. Res. Manag. Ttechnol.*, vol. 3, no. 5, pp. 133–135, 2014.
[172] A. Nissar and A. H. Mir, "Classification of steganalysis techniques: A study," *Digit. Signal Process.*, vol. 20, no. 6, pp. 1758–1770, 2010. doi: 10.1016/j.dsp.2010.02.003.
[173] Y. Bassil, "An image steganography scheme using randomized algorithm and context-free grammar," *J. Adv. Comput. Sci. Technol.*, vol. 1, no. 4, pp. 291–305, 2012. doi: 10.14419/jacst.v1i4.512.
[174] U. D. Acharya, P. R. Kamath, R. Adige, and P. Kamath, "A secure and high capacity image steganography technique," *Signal Image Process. Int. J.*, vol. 4, no. 1, pp. 1304–3629, 2013.
[175] P. Wu, Y. Yang, and X. Li, "Image-into-image steganography using deep convolutional network," in *Proc. Adv. Multimed. Inf. Process-PCM 2018: 19th Pacific-Rim Conf. Multimed.*, Hefei, China, vol. 19, 2018, pp. 792–882.
[176] A. A. J. Altaay, S. B. Sahib, and M. Zamani, "An introduction to image steganography techniques," in *Proc. IEEE ACSA*, Kuala Lumpur, Malaysia, 2012, pp. 122–212.
[177] A. Al-Mohammad, "Steganography-based secret and reliable communications: Improving steganographic capacity and imperceptibility," Ph.D. dissertation, School of Inf. Syst., Comp. and Mat., Univ. of Brunel Univ., UK, 2010.
[178] M. Yedroudj, F. Comby, and M. Chaumont, "Yedroudj-Net: An efficient CNN for spatial steganalysis," in *Proc. IEEE ICASSP*, Calgary, AB, Canada, 2018, pp. 2092–2096.
[179] B. Li, J. He, J. Huang, and Y. Q. Shi, "A survey on image steganography and steganalysis," *J. Inf. Hiding Multim. Signal Process.*, vol. 2, no. 2, pp. 142–217, 2011.
[180] V. Gautam, "MASSS—Multi-agent-based steganography security system for VANET," in *Proc. 3rd ICCIN*, Singapore, Springer, 2021, pp. 159–172.