Intelligent Automation & Soft Computing
DOI:10.32604/iasc.2021.014773
Article

Tech Science Press

Image Steganography in Spatial Domain: Current Status, Techniques, and Trends

Adeeb M. Alhomoud[*]

Department of Basic Sciences, College of Science and Theoretical Studies, Saudi Electronic University, Riyadh, 11673, Saudi Arabia
[*]Corresponding Author: Adeeb M. Alhomoud. Email: a.alhomoud@seu.edu.sa

Received: 15 October 2020; Accepted: 01 November 2020

Abstract: This research article provides an up-to-date review of spatial-domain steganography. Maintaining the communication as secure as possible when transmitting secret data through any available communication channels is the target of steganography. Currently, image steganography is the most developed field, with several techniques are provided for different image formats. Therefore, the general image steganography including the fundamental concepts, the terminology, and the applications are highlighted in this paper. Further, the paper depicts the essential characteristics between information hiding and cryptography systems. In addition, recent well-known techniques in the spatial-domain steganography, such as LSB and pixel value differencing, are discussed in detail and several comparisons are provided to show the merits and the demerits of the discussed techniques. Furthermore, to aid the steganography researchers in developing efficient spatial-domain embedding techniques, the future research of the spatial-domain steganography is discussed and a set of recommendations are suggested.

Keywords: Information hiding; steganography; spatial-domain steganography; stego-image; adaptive embedding; steganalysis

1 Introduction

Steganography is a word that is derived from the Greek word, namely, “Stegos”, which refers to the word “cover”, and the word “Grafia” refers to the word “writing”, which is defined as “covered writing” [1]. Steganography can be defined as the art and science that aims at applying an object of digital communication by hiding any secretive information [2]. Typically, secure communication is targeted based on different encryption approaches. Nonetheless, the current need for security remains increasing causing the use of steganography for information security. Fig. 1 illustrates many different majors related to the domain of information hiding. Cryptography and Steganography are highly dependent aspects to information hiding. In fact, both aspects deliver the same aim, while both are however different in some other aspects. Steganography represents a writing that is hidden, while cryptography represents a writing that is kept secret. In particular, cryptography offers security based on the message’s contents, while steganography aims at hiding the message itself [1].

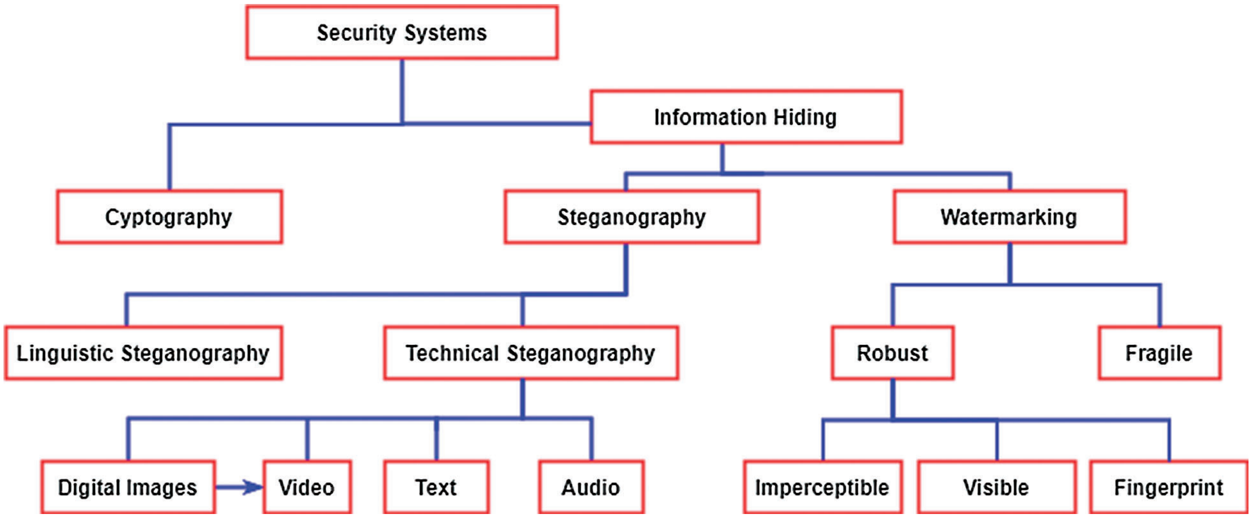

Figure 1: The different disciplines of information hiding [3]

Information hiding contains two sub domains, which are watermarking and steganography [4]. The two domains are applied to make the secret message hidden from other unauthorized users. Both domains are highly dependent on each other. Nonetheless, they depend on many various objectives. Steganography aims at hiding the protective and communication tools pertaining to the secretive information. On the contrary, watermarking aims at protecting the secret data's integrity as to whether the communication derived from eavesdroppers is hidden. The applications of watermarking aim at protecting the information contents' intellectual property. Nevertheless, Tab. 1 depicts the essential basic characteristic between information hiding and cryptography systems [5].

Table 1: Brief comparison between information hiding and cryptography

	Information Hiding		Cryptography (Encryption)
	Watermarking	Steganography	
Main objective	Protect media copyrights	Conceal existence of secret data and communication	Content protection
Robustness	Against removing tampering security data	Against detecting the existence of secret data	Against breaking ciphers
Secret information	Watermark	Payload	Plain text of file
Security of communication	Depends on how confidential the embedding method is.	Depends on how confidential the embedding method is.	Depends on how confidential the key is.
Loss of security	When loss of integrity	When detecting the existence of security data	When decrypting the cipher
Result	Watermarked media	Stego-media	Cipher
Need for key	Optional	Depends on used application	Compulsory
Type of attacks	Image processing	Steganalysis	Cryptanalysis
Main challenges	Robustness	Imperceptibility, embedding payload, and robustness	complexity of encryption and key management

New review papers in the domain of image steganography are always needed to discuss the strengths and limitations of recent proposed techniques. Therefore, this review paper aims to present an up-to-date knowledge for spatial-domain image steganography. The rest of the paper is structured as follows: Section 2 presents an overview of the steganography including history, fundamental concepts, terminology, and applications. Section 3 reviews the current spatial-domain image steganography, where recent well-known techniques are analyzed and discussed in detail. The future research and recommendations, which could forward the researchers to develop efficient spatial-domain embedding schemes, are presented in Section 4. Finally, Section 5 concludes the paper.

2 Steganography: An Overview

2.1 Brief History

The notion of making any information hidden from other unauthorized users has been studied since the 440 BC and applied into various layouts through the past few years ago [6]. Based on the Greek historian Herodotus, Histaiacus, who is a Greek tyrant, applied a steganography layout in order to provide a communication along with his son-in-law 'Aristagoras'. Histaiacus shaved a trusted slave's head where a tattoo was applied on a secret message on top of his scalp. When the hair of that slave grew back again, Aristagoras received him along with the hidden message [7]. A further layout of steganography took place in the World War 2 once Germans improved the microdot method. In fact, the method aims at condensing several information, at most photographs, into a typed period's size. Information is hidden through one period of a paper (e.g., a full stop) and disseminated through an undefended channel. Edgar Hoover, an FBI detective, elaborates the way of using microdots as a form of the enemy's masterpiece of espionage [8]. Despite the fact that steganography has far been studied for several years now, its new layout formation is clarified based on the use of the prisoners' problem that is produced by Simmons [9] such that two prisoners, Alice and Bob, look forward to exchanging information in a secret manner in order to obtain an escape scheme. The whole communication between both prisoners is provided to Eve, who represents a warden of such a communication. If this warden distrusts any secretive communication, then the two prisoners are directed to a solitary confinement. The entire correspondences between the two prisoners are assessed through the warden, which can be either active or passive. If the warden considers a passive method, it will be possible for that warden to check any available secretive information through a prospective communication. If a secretive communication is revealed, then the warden provides a notification towards an external party where the information can accordingly gain access with no any obstacle. Nevertheless, if an active warden distrusts any hidden information; the communication is then modified based on changing or eliminating the hidden data [10].

Most of the current steganographic systems make use of different multimedia objects such as images, videos, audio files, and so on, as a covering media since digital images are frequently transmitted by users through emails and many different communications [11]. These systems aim at making any information hidden into digital multimedia files and at the level of a network packet. In addition, in comparison with other digital media, image-based steganography is currently the most developed field, with several techniques are provided for different image formats [12].

Modern steganographic systems apply the inventions of the networking and computers that appeared in the 20th century. There exist four major improved aspects regarding the digital steganography. These comprise network steganography, file system steganography, linguistic steganography and digital media steganography [13].

2.2 Fundamental Concepts

The term cover image indicates to the image that is used for the purpose of transporting the embedded bits [1]. The embedded data refers to the payload where the image with the embedded data refers to which is called ‘stego-image’. The “embedded technique” refers to the algorithm or process of hiding the “secret message” within the “cover image” including an optional “stego-key”. The optional “stego-key” is shared with the two ends [5]. In the same context, the “extraction technique” refers to the procedure of recovering the “secret message” from the “stego-image” including an “optional key”. Steganalysis represents the attack that usually occurs through the steganography process. In particular, steganalysis refers to the science and art of recovering or detecting the secret message that is derived from different stego images. Embedding distortion is the distortion that induced on the cover signal by embedding secret data. Imperceptibility refers to the difficulty confronted by the HVS in noticing any difference between the stego-image and the original cover image [14]. It is necessary that Stego-image would not contain any risky visual objects. A few main needs for steganography comprise embedding payload, security, and robustness. Embedding payload represents the number of information, which is hidden within a cover medium with no deterioration on the cover image’s integrity. This number is based on the number of bits per pixel (bpp). The embedding process requires maintaining the statistical features pertaining to the cover image including the perceptual quality. Robustness refers to the number of updates for which the stego medium could possibly resist before an adversary attempts to destroy any hidden information. Security refers to the incapability of an eavesdropper to reveal any hidden information [1].

2.3 The General Model of Steganography (The Terminology)

In Fig. 2, the entire structure pertaining to the steganography process is depicted. Assume that ‘C’ refers to the cover medium i.e., an image, where C' refers to the stego-image that is derived based on the data that is embedded [1]. Additionally, assume that ‘K’ refers to the optional key, where ‘SM’ refers to the secret message that is to be communicated with. Assume also that P_{emb} refers to the embedding procedure, where P_{ext} refers to the extraction procedure. The encryption and compression procedures remove the redundancy that is likely to occur within a secret message and yield to a further improved security. Therefore, the procedures of embedding and extracting the secret data is highlighted according the following formulas:

$$P_{emb} : C \times K \times SM \ \rightarrow \ C' \tag{1}$$

$$P_{ext}(C') \approx SM \tag{2}$$

where the size of the secret message |SM|, hidden in C', is known as an embedding payload.

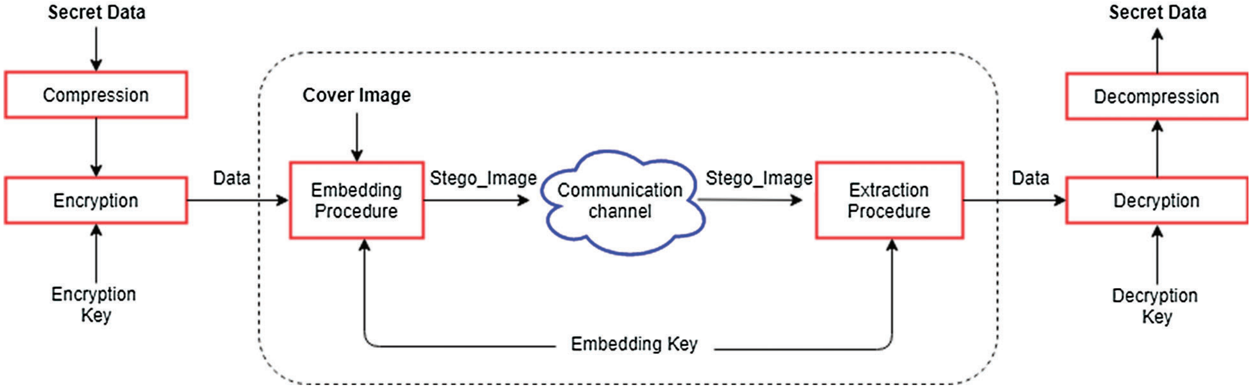

Figure 2: General model of image steganography

An image is a frequently applied file format in steganography since a secret message is entirely embedded within a cover image. Image steganography is categorized into transform and spatial domains. In the spatial domain, a secret message is efficiently embedded within a pixel value in a direct manner. In the transform domain, different approaches perform the embedding procedure based on initially transforming an image from a spatial domain along to a frequency domain based on the use of any available transforms. In the next step, the embedding procedure is applied according to appropriate transformed coefficients.

The measures of an image quality are applied in order to assess the quality of the stego-image that is acquired following the embedding procedure. Various approached aim to attack the steganographic algorithm. Several techniques related to steganography are existing where such techniques involve StegHide, Hide4PGP, S-tools, OutGuess, Stegnos, Ezstego, Hide and Seek, F5, Mp3Stego, and so on. Many different methods of steganalysis comprise the efficient selection of any available secret message and detecting its estimated length or a way of retrieving it. Many different stego attacks involve the filter attack, image resizing attack, J. Fridrich's RS steganalysis, JPEG compression attack, Chi Square attack, Jeremiah J. Harmsena's Histogram attack, image tampering attack, AWGN attack, and so on. The algorithm that is applied to embed the secret data must endure the whole attacking types by preventing an eavesdropper from obtaining the hidden message [1].

2.4 Steganography Applications

Steganography is applied into many different suitable applications [1,3]. For instance, such examples comprise materials' copyright control, improving the strength of several image search engines including smart IDs (identity cards) when all details of individuals are embedded through their photos. Many more applications comprise TV broadcasting, checksum embedding [15], the safe circulation of companies' secret data, video–audio synchronization, TCP/IP packets (e.g., a unique ID is embedded into an image for analyzing the network traffic of particular users) [2]. Another example involves Petitcolas [16], which highlights a few current applications. One of these applications involve medical imaging systems where a separation is significant for achieving privacy among the data images of prospective patients or DNA sequences including their captions, such as physician's name, patient's name, address and some other related and personal details. Nonetheless, a link is kept between the two. Consequently, a patient's information that is embedded based on an image is beneficial for safety measures purposes, which assist in tackling any emerging issues related to the secrecy of a patient's information. Steganography offers a final assurance of authentication in which no further security techniques can provide a reliable assurance. Miaou et al. [17] propose the LSB embedding method for recording patients' information electronically according to the bi-polar multiple-base data hiding method. The difference of a pixel value between the JPEG version of an original image and the image itself represents a number of a conversion base. Nirinjan et al. [18] and Li et al. [19] also discussed hiding patient data in cover images.

3 Image Steganography

The indispensable characteristic of steganography is based on maintaining the communication as secure as possible when transmitting the stego-image through any available communication or networking channels [20]. Many different kinds of image steganographic techniques are produced where a distinct method is applied for each of these techniques in order to conduct the embedding process of a secret data [5]. However, since it is not possible to categorize the techniques entirely, they are split based on various categories (see Fig. 3). The only way is to split them based on the embedding domain (transform and spatial domains) that is derived from [2]. Additionally, the adaptive (statistical aware) embedding technique is also based on the indicated division as it is engaged in the transform and spatial domains. Fig. 3 illustrates the categorization of such techniques along with the objectives.

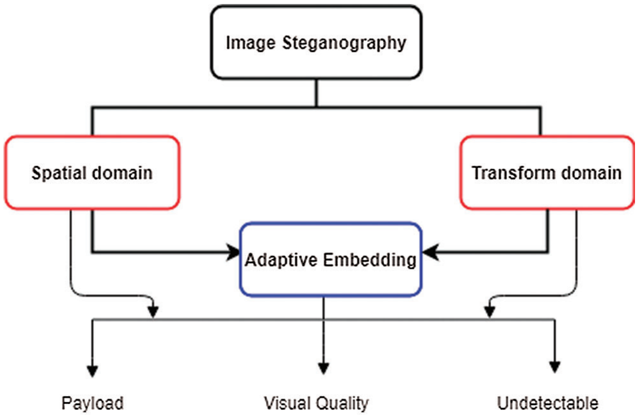

Figure 3: Image steganography domains with aimed objectives

The spatial domain can utilize the cover image pixels for concealing the secret information, such as the replacement of secret bits within a pixel value [5]. In the transform domain, the data that is contained in the cover image is initially transformed into different signals prior to the use of the embedding procedure. Take an example of the Discrete Cosine Transformation (DCT), which is applied to the pixels of the host image, and then the secret information is embedded into the DCT coefficients.

Moreover, the adaptive embedding represents a statistical or model-based approach that manages different methods related to information hiding. In fact, this approach is interwoven to the transform and spatial domains. This embedding method's type is based on considering the statistical characteristics of an image prior to applying the embedding procedure. This set of the statistical characteristics dictates where the modifications take place in the cover image [21].

3.1 Spatial Domain Image Steganography

The spatial-domain embedding techniques are more common in comparison with the transform domain due to its simplicity in the embedding and extraction procedures, but with less strength [5]. Nonetheless, the transform domain techniques are considered immune to the operations of image processing and are also considered less vulnerable to steganalysis attacks [1]. Tab. 2 highlights detailed comparisons for the transform and spatial domains.

Table 2: Detailed comparisons of the spatial and transform domains with adaptive embedding techniques

Characteristics	Spatial Domain	Transform Domain	Adaptive Embedding
Embedding Capacity (Payload)	High	Low	Vary, method dependent
Embedding place	Direct manipulating of pixel values	Transform coefficients	Method dependent
Cover format dependency	Format Dependent	Format independent	Method dependent
Complexity	Low	High	Method dependent
Robustness against noise, compression, cropping, etc.	Not robust	Less prone	Method dependent
Visual Quality (Imperceptibility)	High	Low	Low
Geometric attacks	Not robust (vulnerable)	Less prone (resistant)	Less prone (resistant)
Statistical detection attacks (e.g., Histogram, RS-attack)	Easy to detect	Hard to detect	Hard to detect
Well-known techniques	LSB, PVD, MBNS steganography	DCT based, DWT based, CWT based steganography	Region based, HVS, Machine Learning and AI based steganography

The simplest method of conducting the process of data embedding through digital images is based on updating the values of cover pixels within the spatial domain [20]. The image or spatial-domain methods apply different bit-wise techniques, which implement the noise manipulation and bit insertion by applying different simple techniques. This section discusses the well-known image steganography schemes under the umbrella of spatial domain that evolved in recent time. Various methods that aim at performing the embedding procedure within a spatial domain are illustrated in Fig. 4. Additionally, a detailed analysis of such methods is given in Tab. 3.

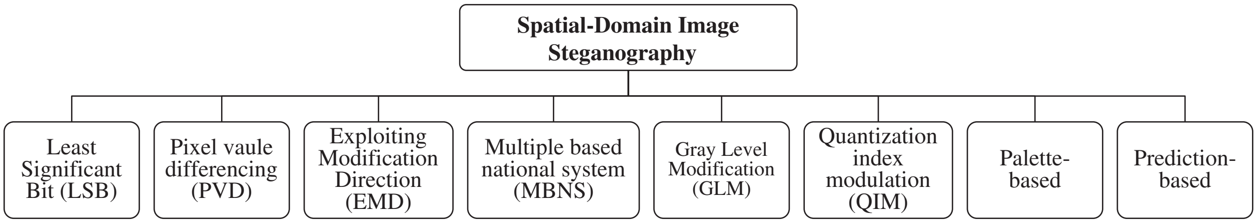
Spatial-Domain Image Steganography
Least Significant Bit (LSB)
Pixel vaule differencing (PVD)
Exploiting Modification Direction (EMD)
Multiple based national system (MBNS)
Gray Level Modification (GLM)
Quantization index modulation (QIM)
Palette-based
Prediction-based

Figure 4: Spatial-domain image steganography

Table 3: Performance analysis of recent spatial-domain steganographic methods

Approach	Reference	Method Name	Merits	Challenges	Payload (bpp)	Visual Quality (PSNR)	Resistance against Steganalysis
LSB	Sarreshtedari et al. [22]	±1 LSB	High imperceptibility & simple implementation.	Lower payload & Key dependent	1 bpp (gray-image)	~53 dB	HCF-COM
	Qazanfari et al. [23]	GLSB++	Secure against Histogram analysis & improved visual quality.	Not robust & key dependent	0.8 bpp (gray-image)	>50 dB	Chi-Square & Histogram
	Nguyen et al. [24]	MPBDH	Adaptive embedding & reduce visual attacks.	Not robust against compression & cropping & key dependent	~1.5 bpp (gray-image)	~46 dB	SPAM at low embedding
	Muhammad et al. [25]	MLEA	Keeps balance between imperceptibility and security, & applies multi-level of encryption for secret data.	Lower payload	~1 bpp	>45 dB	Salt & pepper noise, & Histogram
	Rajendran and Doraipandian [26]	logistic map-LSB	High visual quality & & simple implementation.	Lower payload	2 bpp	>44.5 dB	Histogram
	Vyas and Dudul [27]	OO-LSB	Encrypts the secret data before embedding starts & embeds in skin areas.	Uses multiple covers	~40KB	>47 dB	N/A
PVD	Balasubramanian et al. [28]	Octonary-PVD	Adaptive embedding & resistance against various statistical steganalysis.	Modern steganalysis evaluation is missing	~ 3.6 bpp (gray-image)	~40 dB	PVD analysis & RS analysis
	Shen et al. [29]	MF-PVD	Resolves the PVD underflow/ overflow problem & simple implementation.	Limited payload & modern steganalysis evaluation is missing	~1 bpp (color-image)	~36 dB	Pixel Difference Histogram & RS analysis.
	Swain [30]	Ad-PVD	Adaptive embedding.	Lower payload		~46.7 dB	

(Continued)

Table 3 (continued).

Approach	Reference	Method Name	Merits	Challenges	Payload (bpp)	Visual Quality (PSNR)	Resistance against Steganalysis
					~1.74 bpp (color-image)		Pixel Difference Histogram & RS analysis.
	GrajedaMarín et al. [31]	PVD-TPVD	Resolves the PVD underflow/overflow & embedding done by full utilization of pixels.	Security evaluation by steganalysis is missing	~2.14 bpp (gray-image)	~38.3 dB	N/A
	Swain [32]	Ad-PVD	Adaptive embedding & High visual quality	Complex algorithms for embedding & extracting	~3 bits per byte	~43 dB	Pixel Difference Histogram & RS analysis.
EMD	Kuo et al. [33]	GEMD	Uses dynamic modulus table to resolve the extraction function fixed weighting problem.	Modification of all pixels to embed the secret data	1.5 bpp	~50.2 dB	N/A
	Kuo, Wang, et al. [34]	MSD	Maintains the bpp with increasing of n pixels & reduces the pixel modification ratio (only n/2 of pixels modification).	Limited payload	Only 1 bpp	>52 dB	RS analysis
	Kuo et al. [35]	MBEF	Adaptive embedding & resolves the PVD underflow/overflow.	Low visual quality when high payload is embedded	Bet. 1.25 & 4.5 bpp	Bet. 51 to 30 dB based on the payload	Bit plane & RS analysis
MBNS	Geetha et al. [36]	VRNS	Good visual quality.	Not robust against compression, filtering & cropping, limited payload	Only 1 bpp	~41 dB	RS analysis
	Chen et al. [37]	GMB	Adaptive technique & increases security by coefficient mapping	SPAM analysis detection when payload is > 1 bpp	Bet. 1.46 to 3.8 bpp	Bet. 50 to 35 dB	SPAM analysis, Histogram, RS analysis
	Nyeem [38]	Bit Plan Sclicing	high payload with high imperceptibility	Not robust against attacks	Bet. ~2.5 to ~7.3 bpp	~57 dB at 2.5 bpp	Histogram
GLM	Muhammad et al. [39]	GLM-MLE	High imperceptibility & robust against salt & pepper.	Limited payload	8 KB	~57 dB	N/A
Palette	Imaizumi et al. [40]	k-bit palette	Higher payload with higher visual quality	Location map is required to extract the embedded bits	Bet. 1 to 3 bpp	~40 dB at 3 bpp	N/A
Prediction	Jafar et al. [41]	MPE	Improved the prediction accuracy by using multiple predictors.	Limited payload & security evaluation by steganalysis is missing	Only 90574 bits	~46 dB	N/A
	Benhfid et. al. [42]	MLBS	Good imperceptibility level	Limited payload	1.8 bpp	~40 dB	Chi-Square
	Baluja [43]	CNN	Higher payload		1:1 ratio	N/A	N/A

Table 3 (continued).

Approach	Reference	Method Name	Merits	Challenges	Payload (bpp)	Visual Quality (PSNR)	Resistance against Steganalysis
Deep learning				Takes more time to embed the secret image and requires much more memory			
	Zhu et al. [44]	GAN	High extracting accuracy	Limited payload and requires excessive memory	0.203 bpp	<40 dB for Combined model	ATS analysis
	Shang et al. [45]	GANste	Better security	Limited payload	0.4 bpp	<30 dB	FGSM & Onepixelattack

3.1.1 Least Significant Bit (LSB) Steganography

The LSB technique is considered an extremely simple technique in its performance, and therefore, it represents one of those common spatial image steganographic techniques [20]. The least significant bits within an image only introduces weak information and small modifications in these bits are not detectable through the eyes of humans. The secret bits are directly embedded into the cover image based on applying an LSB-based spatial-domain technique by modifying the cover's least significant bits with no any distortion for the visual quality of the cover image. However, the embedding procedure generates a noise of 50% derived from the average bit embedding rate (i.e., embedded bits per pixel). Previous studies in the LSB steganography approach [46,47] have only focused on designing a method for increasing the capacity of the payload based on the use of the cover pixels. Further, the domain of steganalysis turns to be more effective in breaking such methods when statistical analysis is applied.

To achieve effectiveness of this technique, several developed LSB based image steganography versions are taken into account. The most significant versions apply different LSB matching algorithms [48], Adaptive LSB embedding based on image features such as texture contents or nature of edge pixels [49,50], Optimized LSB substitution based on learning methods [51,52] and so on. Additionally, the LSB technique is expanded to a maximum of 4 LSB planes in order to raise the capacity of the embedding procedure according to the cost of the minimized imperceptibility [53]. In a recent study, the authors proposed an LSB object-oriented image steganography [27]. In the mentioned research work, the secret data is embedded in the skin region of the cover image where the skin objects are selected using a skin detection algorithm. The neural network approach is applied to find the largest object among selected skin-tone objects. While the proposed work gives high embedding PSNR, it uses more than one cover image to embed the secret data.

The major benefit of the LSB steganography related to its ease of the embedding and extraction procedures. Nonetheless, LSB techniques are vulnerable to different statistical attacks, with some manipulations within the stego-image. As the LSB steganography represents the way of modifying the cover's pixel values, its performance of extracting of the embedded data relies on some factors such as the compression quantization, noise effect, and intruder attacks.

3.1.2 Pixel Value Differencing (PVD) Steganography

Wu et al. presented a novel embedding aspect that relies on the occurring difference among pixel values [54]. The cover image consists of non-overlapping blocks of two joined pixels where the difference found within every block is changed. A greater difference between the two pixels allows a greater change and thus higher payload can be embedded. The number of secret bits, which are allowed to be embedded, relies on whether the pixel exists into a smooth or an edge location. In the edge location, the differences among neighboring pixels are found to be more, while in the smooth location it is found to be less. Therefore, more data can be embedded into the edge-area pixels in comparison with the smooth area. Since this technique aims to embed the data by changing the difference value within the two neighboring pixels instead of directly changing pixel values, it offers more effective results based on its stego-image quality and imperceptibility in comparison with the LSB replacement technique. Many techniques that relate to the PVD technique have been produced in order to offer several secure communications and to defeat any statistical attack. For instance, Hussain et al. [55] introduced an embedding technique for enhancing security based on the use of two modes that depend on the embedding procedure. In fact, this procedure is enhanced and based on two techniques, namely, the improved Rightmost Digit Replacement (iRMDR) and the Parity-Bit Pixel Value Difference (PBPVD). A further example of the enhanced security is the histogram analysis based vulnerability (PVD) technique [56]. To link the benefits of different embedding techniques together, hybrid embedding techniques are produced (i.e., Steganographic techniques that apply the LSB and PVD [57,58]).

Many enhanced PVD based image steganography versions were researched in order to improve the efficiency of PVD. The most significant versions apply the Adaptive PVD block technique by using different pseudo-random number techniques for determining the blocks [90] and tackling the fall-off boundary problem in the PVD technique [59]. In addition, Swain [32] proposed an adaptive PVD-based hiding scheme. In the mentioned work, the cover image is divided up into 1 × 2 overlapped blocks of adjacent pixels. After that, the method uses modular arithmetic and adaptive quantization range table to embed the secret data. The findings reveal that the mentioned scheme has higher PSNR value and embedding capacity in comparison with existing PVD schemes. However, the proposed scheme increases the algorithms' complexity of embedding and extracting the secret data [60].

3.1.3 Exploiting Modification Direction (EMD) Steganography

The Exploiting modification direction (EMD) method is a common method that keeps the increased fidelity pertaining to the stego-images protected [61]. In general, the secret digit is converted based on the (2n + 1)-ary system when the embedding procedure is taking place through this method, such that n denotes the number of the cover pixels. The range of the distortion's highest pixel value is just (±1). In particular, the EMD method applies a particular base for selecting the local variation corresponding to the pixel intensity in the cover image. Thus, more message size can be hidden in the pixels that exist in high texture areas. In fact, the EMD method delivers an effective visual quality in comparison with PVD and LSB methods. The highest capacity of the EMD method reaches 1.16 bpp for n = 2. At the same time, the embedding payload is radically reduced when the selected pixels are incremented. Consequently, various EMD methods are produced in order to enhance the embedding payload [33,62–64].

Kuo et al. [33] proposed the Generalized Exploiting Modification Direction (GEMD) technique where the major aim is that the (n + 1)-ary binary bits are embedded through n adjacent pixels. The findings demonstrate that the technique can keep the embedding payload (1 + 1/n) along with a modified set of pixels. However, the technique does not have the ability of hiding secret bits that are exceeding two per every pixel [5]. At the same time, it adjusts the entire pixels of the set when the embedding procedure of the secret is taking place. In order to tackle the issue of pixel modification, Kuo et al. [34] produced a new technique that is called the Modified Signed-Digit (MSD) technique. This technique can only adjust n/2 pixels but has only 1 bpp embedding payload. The MSD technique can proceed towards the RS steganalysis [65] with an efficient imperceptibility. Kuo et al. [35] introduced an embedding technique that is based on a multi-bit encoding function, which is applied in order to enhance the embedding payload. This technique embeds up to (k + 1/n) pixels on average for every available pixel, where k is selected based on how much embedded bits are existing per each pixel. Furthermore, the technique can minimize the conversion of the secret data's overhead and gives a simple relation among the adjacent pixels. In the meantime, the technique keeps its security in order to resist the RS and bit plain detection analysis. However, it suffers from low visual quality in comparison with many different available EMD based techniques.

3.1.4 Multiple Base Notational System (MBNS) Steganography

A further spatial-domain embedding technique that relies on the Multiple Base Notational Systems (MBNSs) is proposed in order to transform the secret information through to the notational scheme prior to the embedding procedure [5]. In 2006, this technique was initially proposed to enhance the original LSB substitution technique such that bit planes are applied in order to hide the secret bits [66,67].

In several techniques related to the MBNSs, secret information is changed into symbols and re-expressed according to the used MBNS (e.g., octal, decimal and binary systems) [5]. Additionally, an embedding process is applied for such symbols to be embedded into the pixels' intensities. In general, when the notational base symbol is large, the embedding rate gets also large. Several studies aim at enhancing the capacity of the embedding process through different MBNS based techniques. Zhang et al. [68] produced such steganography. Particular bases are selected based on the local variation's degree pertaining to the pixel magnitudes within the cover image such that busy area' pixels can carry more secret bits. High embedding payload is obtained by this method. Comparisons of the obtained findings by the MBNSs are conducted with the PVD technique where it can be inferred that it achieves a superior and an effective quality factor and PSNR.

In [36], an adaptive embedding technique is produced according to the Varying-Radix Numeral System (VRNS). This technique divides any secret data into different numerals, which contain a capacity of different amounts of variable information. This division relates to the tolerance of cover pixels when managing the highest adulteration of the greater secret data. It is found to be proven from the findings that the payload is large enough while keeping an acceptable imperceptibility. Additionally, it controls the way it maintains security towards the RS steganalysis [65]. However, embedding the payload is still limited to many different radix-based methods. Consequently, an enhancement of the method in [36] has been conducted in [69]. The enhanced method is called the VRNS method, which is based on a hidden information when applying the Adaptation and Radix (AIHR) algorithm. Nonetheless, such a method obtains a greater payload compared to other available VRNS systems. On the other hand, this method contains few ambiguities in proposed flow. For example, there might be a way a receiver and sender are synchronized based on determining their bases. Additionally, in the AIHR extraction procedure, the ambiguity of selecting the multiple M might lead to not recovering the full secret data. Chen et al. [37] produce a General Multiple-Base (GMB) embedding technique in order to convert the secret bits into a number of M-ary secret digits that belong to a pixel-cluster (i.e., n pixels). The multiple M is selected in an automatic manner based on the end user's input function. It offers various styles of the multi-purpose embedding procedure leading to high embedding payload or high quality of the stego-image. At less than or equal to 1.0 bpp, the GMB method resists the non-structural SPAM features and the RS steganalysis [65].

3.1.5 Gray Level Modification (GLM) Steganography

Potdar et al. [70] proposed the GLM technique in order to map the data based on changing the pixels' gray levels (i.e., not embedding it). According to a few mathematical functions, a group of pixels is determined where the values of their gray levels are organized in the bit stream that relates to the secret message, which could have been mapped within the cover image [71]. This technique applies the even and odd numbers aspect in order to provide an effective way of mapping the data through to the cover image. For instance, number '1' is mapped as an odd data value, while number '0' is mapped as an even data value. The benefits of such a technique comprise the reduced computational complexity and increased embedding payload. The hybrid embedding technique relies on the GLM technique, which is produced by Safarpour et al. [72] for embedding more secret data, and consequently, increasing the embedding payload.

3.1.6 Quantization Index Modulation (QIM) Steganography

The Quantization Index Modulation (QIM) technique [73] is considered an effective data embedding technique in the field of digital watermarking where it is applied in different steganography domains. This technique is based on embedding the information into the cover medium by first performing a modulation of an index or a set of indices with the embedded data. After that, the host is quantized according to the involved quantizer(s). The technique has high embedding payload, and it aims at allowing the embedder to manage the robustness and distortion levels obtained during the embedding process. Chung et al. introduced an enhanced data embedding technique that relies on a Singular Value Decomposition (SVD) and a vector quantization. The findings showed a better compression ratio and a more effective image quality [74]. A lossless data-hiding algorithm that applies the Side Match Vector Quantization (SMVQ) and the Search Order Coding (SOC) is proposed in [75]. This algorithm performs a compression rate of 0.325 bpp including a 256 of codebook size. A reversible data-hiding technique that is applied for several VQ indices is discussed in detail in [76]. This technique enhances several techniques such as enhancing the proposed techniques by Tsai and Yang and Lin and Chang, which provides 0.49 bpp of a compression rate.

For enhancements based on the embedding payload and the reduction of distortion, several enhanced quantization-based steganography versions are researched. One of these versions utilizes the elastic indicators and adjacent correlation. Through this approach, the indexes are encoded based on the difference values that are derived from the neighbouring indexes and the elastic sub codebooks are applied to enhance the compression rate [77].

3.1.7 Palette Based Steganography

The Palette based steganography is proposed in [78] to utilize the palette-based images as cover images. Image formats such as TIFF, PNG and GIF are appropriate for such a technique. In palette-based steganography, the colour that has a similar parity of a secret bit within a palette is used for the embedding procedure. The major advantage of the palette-based steganography is that the entire distortion within the stego-image is seen to be smaller in comparison with other related spatial techniques. On the other hand, the major drawback of this technique refers to the demand of particular images, which have lossless compression formats.

Imaizumi et al. [40] introduced a dense embedding technique based on the use of the palette based steganography that maintains the visual quality within an adequate level for an untraceable communication. Multiple secret bits are embedded in one pixel once the difference is assessed according to the Euclidian distance measures, knowing that the majority of the palette-based methods follow a strategy of single bit per pixel. As a comparison with further palette-based methods, the embedding payload is marginally increased, and the visual quality is seen to be further increased through the PSNR value of ~40 dB.

3.1.8 Prediction Based Steganography

The prediction based embedding technique has currently attracted many researchers [5]. In the prediction-based steganography, the embedding procedure is based on directly changing the pixel values, which causes a substantial distortion in the stego-image [1]. This leads to poor visual quality and a low embedding payload. In order to tackle such a problem, a predictive coding technique is provided such that existing pixel values are effectively predicted based on the use of a predictor rather than changing the pixel values. The Error Values (EVs) of prediction are modified for the purpose of embedding the secret bits. Referring to the international standards for lossless and near lossless image compression, the process of compression comprises two different steps, which include the prediction and entropy coding of predicting EVs. The predictive rule is expressed as follows [1]:

$$X' = \begin{cases} \min(\mathrm{a}, \mathrm{b}), & \mathit{if}\ c \geq \max(\mathrm{a}, \mathrm{b}) \\ \max(\mathrm{a}, \mathrm{b}), & \mathit{if}\ c \leq \min(\mathrm{a}, \mathrm{b}) \\ a + b - c, & \mathit{otherwise} \end{cases} \tag{3}$$

During the prediction step, a predictor is employed to estimate the pixel values of the host image. After that, the entropy coder is used to compress the prediction EV. The Median Edge Detector (MED) technique and the Gradient Adjusted Prediction (GAP) techniques represent new predictors that are applied in several prediction-based image coding techniques. Many different reversible prediction-based embedding techniques are enhanced and highlighted in the literature. Every technique attempts at enhancing many available proposed existing techniques.

Hong et al. [79] proposed an embedding technique that relies on the modification of prediction error (MPE), which adjusts the prediction errors' histogram in order to select the unoccupied area for embedding the secret data. The visual quality pertaining to the MPE method ensures more than 48 dB. To acquire an increased embedding payload, the authors in [41] proposed a multiple predictor base steganographic technique, which is considered as an enhancement to the MPE technique without the need for adding any predictor overhead. Determining the accurate predictor in the embedding process is based on the predictor's history. The produced technique demonstrates that the enhancement occurs for the visual quality and embedding payload where its security is not evaluated by any steganalysis technique.

Recently, Benhfid et al. [42] adopted the interpolation through multiple linear box-splines (MLBS) on three directional mesh in order to develop a reversible embedding technique. The secret data is embedded within the error between the interpolated and cover pixels. The secret data is initially put into the interpolated pixels as a particular error. The error is adopted to acquire several stego-pixels that are extremely close to the cover pixels. Furthermore, the LSBs pertaining to the secret data's interpolated pixels are replaced into the cover pixels. After that, the Optimal Pixel Adjustment Procedure (OPAP) is used for the purpose of minimizing the difference between the original cover pixel and the stego-pixel. To compare with other studies in the literature, the findings reveal that the produced technique contains a great embedding payload when the PSNR values are retained at a good level. Additionally, the findings show that this technique achieves a low detectability rate when examined through different steganalysis attacks.

3.1.9 Deep Learning Steganography

In recent years, the introducing of deep learning in steganography has shown a great improvement in the effectiveness of steganography methods. Deep learning steganography is learned from machine learning. Several deep learning steganography methods [43–45] have been developed to improve the imperceptibility and security of steganography. Baluja [43] designed a convolutional neural network (CNN) model based on an encoder-decoder structure. The encoder successfully conceals the secret image into a cover image of the same size of the secret image, while the decoder reveals the complete secret image. The proposed method has a large payload with a minimum degree of distortion to the cover image. It distributes the bits of secret image across all the available bits of the cover image. However, in terms of security, the generated stego-images are distorted in color. In addition, this model takes more time to embed the secret image and requires much more memory since it uses three networks in the embedding and extracting processes [80].

Zhu et al. [44] proposed a deep learning data hiding method, called HiDDeN, based on using Generative adversarial networks (GANs). This method consists of a stego-image generator, an attack simulator, and an extractor. Different noises, such as JPEG compression and Gaussian filter, were modeled in the simulator to train the network. The proposed HiDDeN method can extract the hidden bits with high accuracy even under different attacks, such as JPEG compression and Gaussian blur. However, while this method is resistance to a set of various noises, it requires excessive memory, and therefore cannot effectively embed large payloads [81].

Recently, Shang et al. [45] proposed a deep learning steganography method based on GANs and adversarial example techniques to enhances the security of deep learning steganography. This method consists of two phases, namely, model training and security improving. By the security improving phase (i.e., using adversarial example techniques), the generated stego-images can fool the deep learning steganalysis techniques and the extracted secret images are less distorted. The experiments reveal that the MSE values of stego-images are less than one percent. However, the proposed method has lower embedding payload (~0.4 bpp).

Many spatial-domain steganography techniques can achieve high payload, but they are susceptible to extremely few updates, which are likely to be encountered based on different image processing tasks (e.g., scaling, rotation, cropping, and so on). Moreover, these techniques recompense the image's statistical features indicating a weak robustness towards image filters and lossy compression. As a summary, Tab. 4 provides number of significant comparisons for the merits and demerits pertaining to the well-known spatial-domain steganography techniques.

Table 4: The merits and demerits of well-known spatial-domain image steganography

Technique	Merits	Demerits
LSB	Acceptable payload & simple implementation	Not robust against statistical attacks and noise
PVD	High payload with acceptable imperceptibility	Not robust against statistical attacks
EMD	Better imperceptibility compared with LSB & PVD	Low payload
MBNS	High payload & more robust against steganalysis process	Not robust against geometrical attacks
GLM	High payload & low computational complexity	Not robust against attacks
QIM	High payload	Prone to steganalysis & geometrical attacks
Palette based	High payload & less distortion compared to other spatial-domain techniques	Not secure & it needs covers of specific lossless compression format
Prediction based	Not prone to steganalysis attacks	Limited payload
Deep learning based	Better imperceptibility and security	Limited payload

4 Future Research

4.1 Steganographic Aspects for Improving the Embedding Efficiency

The major challenges incurred in the spatial-domain image steganography comprise having high embedding payload and security, and having a lowest detectability [20]. Although many researchers provide an extensive research in this domain in the past, the aforementioned demands are yet not entirely achieved. Knowing that the steganographic features are highly based on each other, developing a few features can reduce some different aspects' efficiency. The challenge relates to finding a solution has not yet been completed for the entire demands at the same time. A few steganographic aspects are provided below in order to develop the efficiency pertaining to the current spatial-domain steganography.

a) The emphasis over the adaptive steganography: An adaptive approach represents the basic notion for obtaining an optimized method. Adaptiveness does not only develop the embedding efficiency but can as well protect the attempts of steganalysis with appropriate and efficient counter measures. The majority of the prediction and deep learning techniques are considered to represent the most effective selection for obtaining an adaptive nature to the system. This allows providing further improvements for all image steganography concepts starting from the imperceptibility along towards the embedding payload in comparison with different traditional embedding techniques.
b) Statistics aware modelling: Due to the further improvements in steganalysis techniques, forming the most secure steganography method is getting more crucial. In order to form this method, the embedding secret data is added to particular regions instead of the whole image. These regions are called the Region of Interest (ROI). These regions must be determined based on applying the embedding procedure within the image's portions that yield to obtain the lowest distortion. Consequently, it can be inferred that embedding the secret data through the ROI by considering the image's statistical features will assist in obtaining the required results.
c) Soft computing tools: Determining suitable locations for the embedding process has an essential role in embedding the secret data. The determination of such embedding locations is performed based on applying soft computing tools. Applying different optimization algorithms, such as neural networks, can assist in embedding the secret data into the host image in a way that increases the embedded payload, innocuousness, and stego-image quality.
d) Enhancing the secret data's security: Using the encrypted form of the secret data assists in improving the security. Such techniques as the DES and RSA are applied to acquire an encrypted version of the secret data to be hidden in the cover image.
e) Selecting the most effective cover for hiding the data: researchers have previously concentrated on just applying the optimum selection pertaining to the locations of the data embedding in order to acquire an effective image quality. Nonetheless, the findings show that selecting an appropriate cover image maintains the rigidness of a system against any stego attacks while preserving high embedding payload.

4.2 Recommendations

In this subsection, a set of recommendations are provided in order to forward the researchers to develop efficient spatial-domain steganography techniques.

a) The compound of steganography with cryptography: the encryption of the secret data prior to embedding it adds as an extra security layer. If the steganographic algorithm could be exposed by a steganalysis attack, then the encryption has to be broken by the attacker so that the secret data could be possibly recovered.
b) The integration of irreversible and reversible techniques: The integration of reversible and irreversible embedding can raise the security and the embedding payload. The same set of pixels are recursively employed by number of different reversible and irreversible techniques where it is hard for an attacker to have the secret data recovered.
c) Hybrid embedding techniques: Multiple embedding techniques can raise the security of the data and can cause confusion with some steganalysis techniques. Additionally, the weaknesses and strengths

of the available techniques are exploited for designing a more effective embedding technique. Hybrid embedding techniques might likely represent effective techniques in terms of security and protection.

d) Universal steganography: The study demonstrates that the majority of the available steganographic techniques represent domain and format/type dependents. It is significant that the universal image steganographic techniques are revealed and formed in a way not to rely on the domain or type. Moreover, these techniques offer effective resistances for different attacks.

e) Minimizing the additive noise distortion: Minimizing the distortion resulting from the additive noise can resist modern steganalysis. In general, modern steganalysis attacks compute various distinctive features pertaining to the cover image and stego-image in order to differentiate the images types. At most, such features can be created based on an additive noise exists in the stego-image. Accordingly, challenges for reducing the additive noise in developing new embedding techniques are still in demand.

f) Blind (cover-less and key-less) extraction approaches: Both approaches refer to the capability of recovering the embedded secret data from the stego-image without the need for the cover image or the stego-key. When the original cover image is needed for the extraction procedure, the cover image gets suspicious. In the same context, sending a stego-key might likely be alarming. Consequently, the blind (cover-less and key-less) extraction procedure improves the security of the embedding techniques.

g) Multi-purpose embedding techniques: Many of these techniques are formed in order to achieve a single goal by either acquiring high embedding payload or high imperceptibility. A multi-purpose embedding technique can minimize the method's complexity and streamline the implementation. In fact, real-time applications acquire these benefits when designing multi-purpose steganography methods.

h) Ideal image steganography techniques must provide high imperceptibility, high embedding payload, and resistance towards statistical steganalysis attacks. However, no any ideal steganography technique in reality. All indicated techniques have merits and demerits, which rely on the adopted algorithm and their applications' types. Subsequently, the significance of a steganography method is based on the provided application.

5 Conclusion

In this review paper, a comprehensive survey related to recent spatial-domain embedding techniques are introduced. The difference between information hiding and cryptography is provided. Comparisons among available proposed embedding techniques in the spatial domain are explained based on their merits and demerits according to a graphical and tabular design. Additionally, many different recommendations, which might assist future researchers to proceed further in the spatial-image steganography, are elaborated in this paper. The major challenges pertaining to spatial-domain image steganography are comprised of the followings: (i) Maintaining imperceptibility within an increased level, (ii) Giving an increased security for the hidden secret data, (iii) Providing robust procedures towards many different intruder attacks and (iv) Providing an increased embedding payload. Generally, the majority of spatial-domain steganography techniques are considered more appropriate if high embedding payload is persistently required. However, the most commonly found flaw of spatial-domain steganography is the weak defense against geometric attacks, such as scaling, rotation, and cropping. As per the literature, it is inferred that adaptive embedding techniques are effective, and thus, the research may be directed towards applying adaptive approaches for high quality steganography techniques.

Funding Statement: The APC was funded by the Deanship of Scientific Research, Saudi Electronic University.

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

References

[1] M. S. Subhedar and V. H. Mankar, "Current status and key issues in image steganography: A survey," *Computer Science Review*, vol. 13, pp. 95–113, 2014.

[2] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," *Computer*, vol. 31, no. 2, pp. 26–34, 1998.

[3] A. Cheddad, J. Condell, K. Curran and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Processing*, vol. 90, no. 3, pp. 727–752, 2010.

[4] F. A. Petitcolas, R. J. Anderson and M. G. Kuhn, "Information hiding-a survey," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1062–1078, 1999.

[5] 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.

[6] S. Barve, U. Nagaraj and R. Gulabani, "Efficient and secure biometric image stegnography using discrete wavelet transform," *International Journal of Computer Science & Communication Networks*, vol. 1, no. 1, pp. 96–99, 2011.

[7] A. Cheddad, J. Condell, K. Curran and P. Mc Kevitt, "Biometric inspired digital image steganography," in *15th Annual IEEE Int. Conf. and Workshop on the Engineering of Computer Based Systems*, IEEE, Belfast, Northern Ireland, pp. 159–168, 2008.

[8] J. Cummins, P. Diskin, S. Lau and R. Parlett, "Steganography and digital watermarking," School of Computer Science, The University of Birmingham, 2004, [Online]. Available: https://www.cs.bham.ac.uk/~mdr/teaching/modules03/security/students/SS5/Steganography.pdf.

[9] T. Morkel, J. H. Eloff and M. S. Olivier, "An overview of image steganography," *ISSA*, vol. 1, no. 2, pp. 1–12, 2005.

[10] M. Douglas, K. Bailey, M. Leeney and K. Curran, "An overview of steganography techniques applied to the protection of biometric data," *Multimedia Tools and Applications*, vol. 77, no. 13, pp. 17333–17373, 2018.

[11] G. Smitha and E. Baburaj, "A survey on image steganography based on least significant bit matched revisited (LSBMR) algorithm," in *2016 Int. Conf. on Emerging Technological Trends (ICETT)*, IEEE, Kollam, India, pp. 1–6, 2016.

[12] S. Atawneh, A. Almomani and P. Sumari, "Steganography in digital images: Common approaches and tools," *IETE Technical Review*, vol. 30, no. 4, pp. 344–358, 2013.

[13] E. Zielińska, W. Mazurczyk and K. Szczypiorski, "Trends in steganography," *Communications of the ACM*, vol. 57, no. 3, pp. 86–95, 2014.

[14] 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," *Multimedia Tools and Applications*, vol. 76, no. 18, pp. 18451–18472, 2017.

[15] W. Bender, W. Butera, D. Gruhl, R. Hwang, F. J. Paiz *et al.,* "Applications for data hiding," *IBM Systems Journal*, vol. 39, no. 3.4, pp. 547–568, 2000.

[16] S. Katzenbeisser and F. A. Petitcolas, "Introduction to information hiding, " in K. Stefan and P. Fabien (eds.), *Information Hiding: Techniques for Steganography and Digital Watermarking*, Artech House, Boston, London: Artech House, pp. 1–14, 2000.

[17] S. G. Miaou, C. M. Hsu, Y. S. Tsai and H. M. Chao, "A secure data hiding technique with heterogeneous data-combining capability for electronic patient records," in *Proc. of the 22nd Annual Int. Conf. of the IEEE Engineering in Medicine and Biology Society (Cat. No. 00CH37143),* vol. 1, IEEE, pp. 280–283, 2000.

[18] D. Anand and U. Niranjan, "Watermarking medical images with patient information," in *Proc. of the 20th Annual Int. Conf. of the IEEE Engineering in Medicine and Biology Society*, Hong Kong, China: IEEE, vol. 2, pp. 703–706, 1998.

[19] Y. Li, C. T. Li and C. H. Wei, "Protection of mammograms using blind steganography and watermarking," in *Third Int. Sym. on Information Assurance and Security*, Manchester, UK: IEEE, pp. 496–500, 2007.

[20] 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.

[21] M. Kharrazi, H. T. Sencar and N. D. Memon, “Performance study of common image steganography and steganalysis techniques,” *Journal of Electronic Imaging*, vol. 15, no. 4, pp. 041104, 2006.

[22] S. Sarreshtedari and M. A. Akhaee, “One-third probability embedding: A new ± 1 histogram compensating image least significant bit steganography scheme,” *IET Image Processing*, vol. 8, no. 2, pp. 78, 2014.

[23] K. Qazanfari and R. Safabakhsh, “A new steganography method which preserves histogram: Generalization of LSB++,” *Information Sciences*, vol. 277, pp. 90–101, 2014.

[24] T. D. Nguyen, S. Arch-Int and N. Arch-Int, “An adaptive multi bit-plane image steganography using block data-hiding,” *Multimedia Tools and Applications*, vol. 75, no. 14, pp. 8319–8345, 2016.

[25] K. Muhammad, J. Ahmad, N. U. Rehman, Z. Jan and M. Sajjad, “CISSKA-LSB: Color image steganography using stego key-directed adaptive LSB substitution method,” *Multimedia Tools and Applications*, vol. 76, no. 6, pp. 8597–8626, 2017.

[26] S. Rajendran and M. Doraipandian, “Chaotic map based random image steganography using LSB technique,” *International Journal of Network Security*, vol. 19, no. 4, pp. 593–598, 2017.

[27] A. O. Vyas and S. V. Dudul, “A novel approach of object oriented image steganography using LSB,” in *ICDSMLA 2019*. Singapore: Springer, pp. 144–151, 2020.

[28] C. Balasubramanian, S. Selvakumar and S. Geetha, “High payload image steganography with reduced distortion using octonary pixel pairing scheme,” *Multimedia Tools and Applications*, vol. 73, no. 3, pp. 2223–2245, 2014.

[29] S. Shen, L. Huang and Q. Tian, “A novel data hiding for color images based on pixel value difference and modulus function,” *Multimedia Tools and Applications*, vol. 74, no. 3, pp. 707–728, 2015.

[30] G. Swain, “Adaptive pixel value differencing steganography using both vertical and horizontal edges,” *Multimedia Tools and Applications*, vol. 75, no. 21, pp. 13541–13556, 2016.

[31] I. R. Grajeda-Marín, H. A. Montes-Venegas, J. R. Marcial-Romero, J. Hernández-Servín and G. De Ita, “An optimization approach to the TWPVD method for digital image steganography,” in *Mexican Conf. on Pattern Recognition*, Springer, Guanajuato, Mexico, pp. 125–134, 2016.

[32] G. Swain, “Adaptive and non-adaptive PVD steganography using overlapped pixel blocks,” *Arabian Journal for Science and Engineering*, vol. 43, no. 12, pp. 7549–7562, 2018.

[33] W. C. Kuo, S. H. Kuo and Y. C. Huang, “Data hiding schemes based on the formal improved exploiting modification direction method,” *Applied Mathematics & Information Sciences Letters*, vol. 1, no. 3, pp. 1–8, 2013.

[34] W. C. Kuo, C. C. Wang and H. C. Hou, “Signed digit data hiding scheme,” *Information Processing Letters*, vol. 116, no. 2, pp. 183–191, 2016.

[35] W. C. Kuo, S. H. Kuo, C. C. Wang and L. C. Wuu, “High capacity data hiding scheme based on multi-bit encoding function,” *Optik*, vol. 127, no. 4, pp. 1762–1769, 2016.

[36] S. Geetha, V. Kabilan, S. Chockalingam and N. Kamaraj, “Varying radix numeral system based adaptive image steganography,” *Information Processing Letters*, vol. 111, no. 16, pp. 792–797, 2011.

[37] W. S. Chen, Y. K. Liao, Y. T. Lin and C. M. Wang, “A novel general multiple-base data embedding algorithm,” *Information Sciences*, vol. 358–359, pp. 164–190, 2016.

[38] H. Nyeem, “Reversible data hiding with image bit-plane slicing,” in *2017 20th Int. Conf. of Computer and Information Technology (ICCIT)*, Dhaka, Bangladesh, pp. 1–6, 2017.

[39] K. Muhammad, J. Ahmad, H. Farman, Z. Jan, M. Sajjad *et al.,* “A secure method for color image steganography using gray-level modification and multi-level encryption,” *TIIS*, vol. 9, no. 5, pp. 1938–1962, 2015.

[40] S. Imaizumi and K. Ozawa, “Multibit embedding algorithm for steganography of palette-based images,” in *Pacific-Rim Symposium on Image and Video Technology*, Springer, Guanajuato, Mexico, pp. 99–110, 2013.

[41] I. F. Jafar, K. A. Darabkh, R. T. Al-Zubi and R. A. Al Na’mneh, “Efficient reversible data hiding using multiple predictors,” *Computer Journal*, vol. 59, no. 3, pp. 423–438, 2016.

[42] A. Benhfid and Y. Taouil, “Reversible steganographic method based on interpolation by bivariate linear box-spline on the three directional mesh,” *Journal of King Saud University-Computer and Information Sciences*, vol. 32, no. 7, pp. 850–859, 2018.

[43] S. Baluja, “Hiding images in plain sight: Deep steganography,” in *Advances in Neural Information Processing Systems*, CA, USA, pp. 2069–2079, 2017.

[44] J. Zhu, R. Kaplan, J. Johnson and L. Fei-Fei, “Hidden: Hiding data with deep networks,” in *Proc. of the European Conf. on Computer Vision (ECCV)*, Munich, Germany, pp. 657–672, 2018.

[45] Y. Shang, S. Jiang, D. Ye and J. Huang, “Enhancing the security of deep learning steganography via adversarial examples,” *Mathematics*, vol. 8, no. 9, pp. 1–10, 2020.

[46] M. Sutaone and M. Khandare, “Image based steganography using LSB insertion,” IET Int. Conf. on Wireless. 2008.

[47] R. Chandramouli and N. Memon, “Analysis of LSB based image steganography techniques,” in *Proc. 2001 Int. Conf. on Image Processing (Cat. No. 01CH37205)*, IEEE, Thessaloniki, Greece, vol. 3, pp. 1019–1022, 2001.

[48] V. Ajith, S. Kanagaraj and P. Malathi, “Image steganography based on LSB matching revisited using secret sharing application,” *International Journal of Applied Engineering Research*, vol. 10, pp. 2931–2938, 2015.

[49] W. Luo, F. Huang and J. Huang, “Edge adaptive image steganography based on LSB matching revisited,” *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 201–214, 2010.

[50] S. Chakraborty, A. S. Jalal and C. Bhatnagar, “LSB based non blind predictive edge adaptive image steganography,” *Multimedia Tools and Applications*, vol. 76, no. 6, pp. 7973–7987, 2017.

[51] H. Dadgostar and F. Afsari, “Image steganography based on interval-valued intuitionistic fuzzy edge detection and modified LSB,” *Journal of Information Security and Applications*, vol. 30, pp. 94–104, 2016.

[52] S. Bhatt, A. Ray, A. Ghosh and A. Ray, “Image steganography and visible watermarking using LSB extraction technique,” in *2015 IEEE 9th Int. Conf. on Intelligent Systems and Control (ISCO)*, IEEE, Coimbatore, India, pp. 1–6, 2015.

[53] T. C. Lu, C. Y. Tseng and J. H. Wu, “Dual imaging-based reversible hiding technique using LSB matching,” *Signal Processing*, vol. 108, pp. 77–89, 2015.

[54] D. C. Wu and W. H. Tsai, “A steganographic method for images by pixel-value differencing,” *Pattern Recognition Letters*, vol. 24, no. 9–10, pp. 1613–1626, 2003.

[55] 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 Processing: Image Communication*, vol. 50, pp. 44–57, 2017.

[56] X. Zhang and S. Wang, “Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security,” *Pattern Recognition Letters*, vol. 25, no. 3, pp. 331–339, 2004.

[57] G. Swain, “A steganographic method combining LSB substitution and PVD in a block,” *Procedia Computer Science*, vol. 85, pp. 39–44, 2016.

[58] M. Kalita and T. Tuithung, “A novel steganographic method using 8-neighboring PVD (8nPVD) and LSB substitution,” in *2016 Int. Conf. on Systems, Signals and Image Processing (IWSSIP)*, IEEE, Bratislava, Slovakia, pp. 1–5, 2016.

[59] H. Sajedi and M. Jamzad, “Using contourlet transform and cover selection for secure steganography,” *International Journal of Information Security*, vol. 9, no. 5, pp. 337–352, 2010.

[60] C. Nisha and T. Monoth, “Analysis of spatial domain image steganography based on pixel-value differencing method,” in *Soft Computing for Problem Solving*, Singapore: Springer, pp. 385–397, 2020.

[61] X. Zhang and S. Wang, “Efficient steganographic embedding by exploiting modification direction,” *IEEE Communications Letters*, vol. 10, no. 11, pp. 781–783, 2006.

[62] T. D. Kieu and C. C. Chang, “A steganographic scheme by fully exploiting modification directions,” *Expert Systems with Applications*, vol. 38, no. 8, pp. 10648–10657, 2011.

[63] W. C. Kuo and M. C. Kao, “A steganographic scheme based on formula fully exploiting modification directions,” *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 96, no. 11, pp. 2235–2243, 2013.

[64] X. Liao, Q. Wen and J. Zhang, "A novel steganographic method with four-pixel differencing and exploiting modification direction," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 95, no. 7, pp. 1189–1192, 2012.

[65] J. Fridrich, M. Goljan and R. Du, "Reliable detection of LSB steganography in color and grayscale images," in *Proc. of the 2001 Workshop on Multimedia and Security: New Challenges*, Ottawa, Canada, pp. 27–30, 2001.

[66] B. C. Nguyen, S. M. Yoon and H. K. Lee, "Multi bit plane image steganography," in *Int. Workshop on Digital Watermarking*, Springer, Jeju Island, Korea, pp. 61–70, 2006.

[67] U. Ghosh, D. Burman, S. Maity and I. Mukherjee, "Adaptive multi-bit image steganography using pixel-pair differential approach," in *Progress in Advanced Computing and Intelligent Engineering*, Singapore: Springer, pp. 47–56, 2018.

[68] X. Zhang and S. Wang, "Steganography using multiple-base notational system and human vision sensitivity," *IEEE Signal Processing Letters*, vol. 12, no. 1, pp. 67–70, 2004.

[69] M. Tang, W. Song, X. Chen and J. Hu, "An image information hiding using adaptation and radix," *Optik*, vol. 126, no. 23, pp. 4136–4141, 2015.

[70] V. M. Potdar and E. Chang, "Grey level modification steganography for secret communication," in *2nd IEEE Int. Conf. on Industrial Informatics, 2004*, IEEE, Berlin, Germany, pp. 223–228, 2004.

[71] S. Mukherjee and G. Sanyal, "Edge based image steganography with variable threshold," *Multimedia Tools and Applications*, vol. 78, no. 12, pp. 16363–16388, 2019.

[72] M. Safarpour and M. Charmi, "Capacity enlargement of the PVD steganography method using the GLM technique," ArXiv Preprint ArXiv:1601.00299, pp. 1–6, 2016.

[73] B. Chen and G. W. Wornell, "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding," *IEEE Transactions on Information Theory*, vol. 47, no. 4, pp. 1423–1443, 2001.

[74] K. L. Chung, C. H. Shen and L. C. Chang, "A novel SVD-and VQ-based image hiding scheme," *Pattern Recognition Letters*, vol. 22, no. 9, pp. 1051–1058, 2001.

[75] C. C. Chang, T. S. Nguyen and C. C. Lin, "A novel VQ-based reversible data hiding scheme by using hybrid encoding strategies," *Journal of Systems and Software*, vol. 86, no. 2, pp. 389–402, 2013.

[76] C. C. Chang, T. S. Nguyen and C. C. Lin, "A reversible data hiding scheme for VQ indices using locally adaptive coding," *Journal of Visual Communication and Image Representation*, vol. 22, no. 7, pp. 664–672, 2011.

[77] C. T. Huang, L. C. Lin, D. E. Sun and S. J. Wang, "A security-based steganographic scheme in vector quantization coding between correlated neighboring blocks," *Multimedia Tools and Applications*, vol. 78, no. 3, pp. 3131–3151, 2019.

[78] M. Niimi, H. Noda, E. Kawaguchi and R. O. Eason, "High capacity and secure digital steganography to palette-based images," in *Proc. Int. Conf. on Image Processing*, IEEE, NY, USA, vol. 2, pp. II-II, 2002.

[79] W. Hong, T. S. Chen and C. W. Shiu, "Reversible data hiding for high quality images using modification of prediction errors," *Journal of Systems and Software*, vol. 82, no. 11, pp. 1833–1842, 2009.

[80] P. Wu, Y. Yang and X. Li, "Stegnet: Mega image steganography capacity with deep convolutional network," *Future Internet*, vol. 10, no. 6, pp. 1–15, 2018.

[81] K. A. Zhang, A. Cuesta-Infante, L. Xu and K. Veeramachaneni, "SteganoGAN: High capacity image steganography with GANs," ArXiv Preprint arXiv:1901.03892, pp. 1–11, 2019.