Review Article

Aditya Kumar Sahu* and Monalisa Sahu

Digital image steganography and steganalysis: A journey of the past three decades

https://doi.org/10.1515/comp-2020-0136
Received Apr 09, 2020; accepted May 28, 2020

Abstract: Steganography is the science and art of covert communication. Conversely, steganalysis is the study of uncovering the steganographic process. The evolution of steganography has been paralleled by the development of steganalysis. In this game of hide and seek, the two player's steganography and steganalysis always want to break the other down. Over the past three decades, research has produced a plethora of remarkable image steganography techniques (ISTs). The major challenge for most of these ISTs is to achieve a fair balance between the metrics such as high hiding capacity (HC), better imperceptibility, and improved security. This study aims to present an exhaustive scrutiny of various ISTs from the classical to recent developments in the spatial domain, with respect to various image steganographic metrics. Further, the current status, recent developments, open challenges, and promising directions in this field are also highlighted.

Keywords: Image steganography, steganalysis, hiding capacity, imperceptibility, security

1 Introduction

Recent innovation in digitization led to the production of an enormous amount of information every day. Storing, transmitting and sharing this confidential information over an open and insecure communication channel is still an unsolved challenge [1]. In this aspect, data security techniques such as cryptography, watermarking and steganography have received immense interest from researchers. Figure 1 shows the classification of various data security techniques. In fact, these three security techniques so closely equate to each other that their fundamental objective is to achieve confidentiality of data during transmission. However, the working principles and guiding paradigms are different from each other. Therefore, to have a clear understanding of their functionalities and to eradicate the fuzziness, Table 1 compares these three security techniques.

The literature has produced various state-of-the-art reviews on steganography and steganalysis. Table 4 summarizes their contributions in brief. In this paper, the authors have highlighted the major issues, current status, and critical challenges for various state-of-the-art spatial domain ISTs. The significant contributions of the proposed study are highlighted below.

1. Various cutting edge research articles ranging from infant to matured ISTs have been reviewed. Figure 2 shows a pictorial representation of the statistics for year-wise publications that are inspected in this work. Moreover, around 65% of the refereed papers are recent and published after 2015.
2. Further, the complete list of available IS parameters are discussed at length. Next, utilizing these parameters, a comparative analysis of the referred techniques is presented.
3. Also, the major issues and underlying benefits that exist with various spatial domain ISTs are presented with an accomplished illustration of each.
4. Additionally, the recent developments in this field, particularly with the advent of machine learning (ML) based ISTs are also discussed.
5. Finally, some promising future directions to look forward in this domain have been suggested.

The rest of the paper is organized as follows: A brief history of ancient steganography is presented in Section 1.1. Section 2 discusses various data security techniques. In Section 3, the performance appraisal metrics of ISTs are outlined. Then, Section 4 meticulously presents the review of various spatial domain ISTs with their merits and issues. Next, Section 5 overviews the recent development in steganography and steganalysis concerning ML algorithms. Further, Section 6 presents the open challenges

***Corresponding Author: Aditya Kumar Sahu:** Department of Computer Science and Engineering, GMRIT, Rajam, Andhra Pradesh 532127, India; Email: adityakumar.s@gmrit.edu.in, adityasahu.cse@gmail.com
Monalisa Sahu: School of Engineering and Technology (CSE), GIET University, Gunupur, Odisha, 765022, India

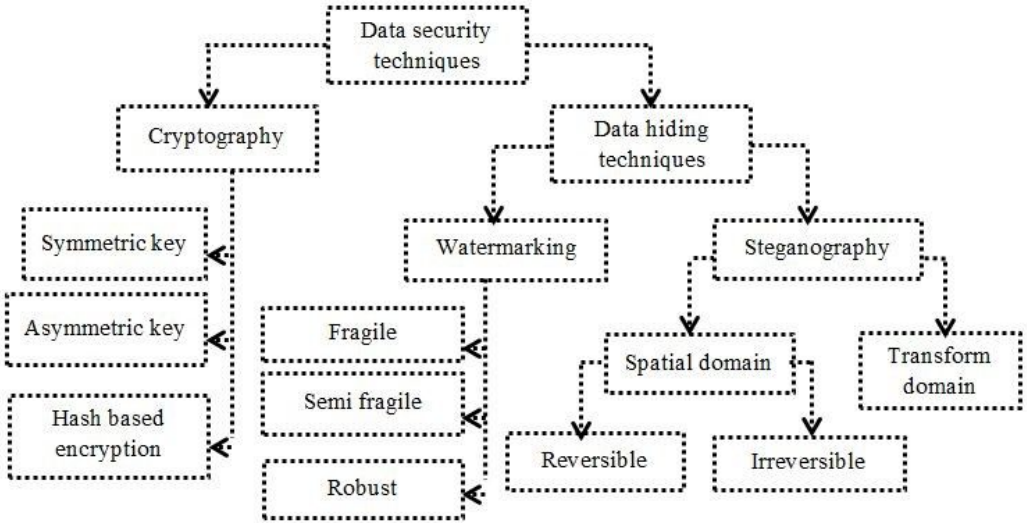

Figure 1: Classification of data security techniques

Table 1: Comparision of the working principles for cryptography, watermarking, and Steganography

Criterion	Cryptography	Watermarking	Steganography
Objective	Encrypted communication	Content authentication and copyright preservation	Covert communication
Authentication	Yes	Yes	No
Cover selection	Not required	Usually image, audio, or video	Any digital object
Key	Mandatory	Optional	Optional
Attacks	Cryptanalysis attacks: ciphertext only attack, known-plaintext attack, chosen-plaintext attack, brute-force attack, man in the middle attack, birthday attack, timing attack, dictionary attack	Image processing attacks: salt and pepper noise, cropping attack, rotation attack, sharpening attack, JPEG attack, median filtering attack, quantization, temporal modification	Steganalysis attacks: regular and singular (RS) analysis, pixel difference histogram (PDH) attack, chi-square attack, and sample pair analysis (SPA)
Robustness	Not required	Should be high	Should be high
HC	Not required	Should be high	Should be high
Imperceptibility	Not required	Should be high	Should be high
Visibility	Always visible	Depending upon the type of watermarking, it can be visible or invisible	Always invisible
Output	Encrypted text	Watermarked object	Camouflage object
Merits	It offers both authentication and integrity, along with confidentiality.	It offers both authentication and integrity, along with confidentiality.	None apart from the sender and receiver can suspect the existence of the communication.
Demerits	The communication is visible to the outsider	HC is usually low	Steganography itself alone can not provide authentication and integrity
Purpose is lost	If the communicating message is decrypted	If the watermark is abolished or heavily tampered	If the attacker knows communication
Origin	Very ancient	Modern era	Very ancient

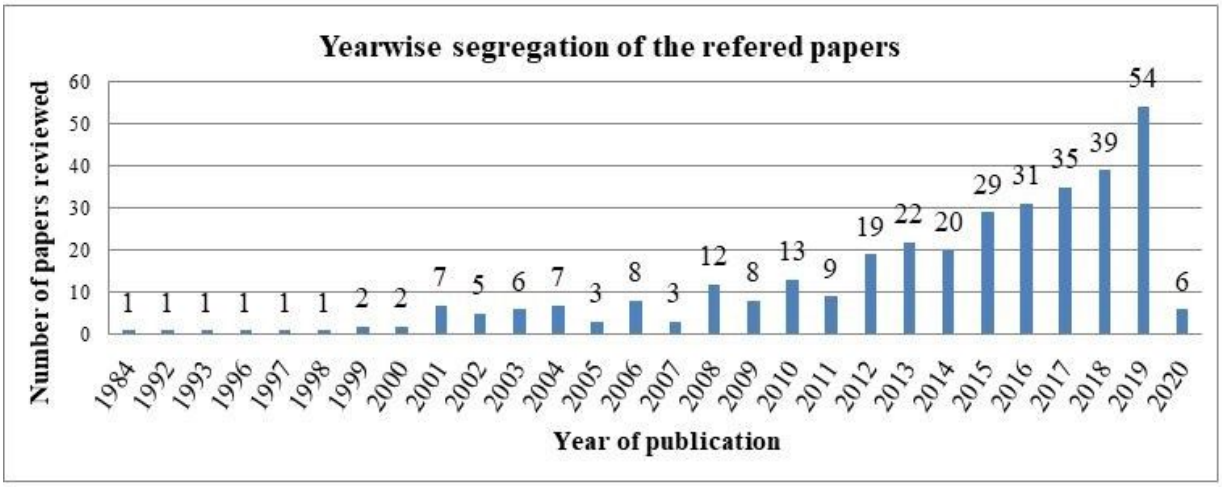

Figure 2: Displaying year-wise publications considered in this review.

and future scopes of IS. Finally, the concluding remarks are drawn in Section 7.

1.1 Ancient steganography

The etymology of steganography is Greek in origin, and is a combination of two different words 'steganos' which means covered and 'graphia' which means writing. This section briefly discusses the rich history of steganography. The literature suggests the term 'steganography' was first coined in c. 1499 by Johannes Trithemius in his work 'Steganographia'. However, the steganographic practices were in use during the centuries before Trithemius publication. In his book 'The Histories', Herodotus mentioned, during the middle of 400 BC, how Demaratus (king of Sparta) and Histiaeus (ruler of Miletus) skilfully communicate using hidden messages. Demeratus wrote the warning message to Greece about the forthcoming attack inside the piece of wood, which was placed beneath a wax tablet. Likewise, Histiaeus tattooed a message on his messenger's shaved scalp and then waited for the hair to regrow. The message was sent to Aristagoras (leader of Miletus), who once again shaved the scalp of the messenger to recover the hidden message. During World War I the German secret service agencies were using invisible ink for spy communication. Here, the confidential messages are hidden on paper using secret inks and once the ink becomes dry, the paper looks as though nothing has been written on it. However, using some skilful techniques, the hidden messages can be visible either by sloping the paper at a fixed angle, or by applying heat. This depends upon the ink being used. Another interesting and popular steganography technique is the microdot that was extensively practiced during World War II. The invention of the microdot is credited to the Germans, and it was they who were using it with balloons and pigeons. In the microdot technique, the secret messages can be reduced to a very small dot (close to 1 mm) and embedded in another message. Later the dot can be enlarged to retrieve the original message. One such fascinating idea was to send the messages using ideograms or ideographs. An ideogram is just a symbol to represent a given message. In the ancient days, it was a popular embedding technique in China. History also tells, steganography was used in many forms, such as inserting a message in a postage stamp, null cipher, and morse code, etc. These are a few notable steganography techniques that people were using mostly before digitization.

2 Data security techniques

This section discusses three data security techniques, namely, cryptography, watermarking and steganography. In short, the rich history of these techniques, working principles, and the potential application areas are discussed.

2.1 Cryptography

Around 4000 ages ago, ancient Egyptian's were using logographic scripts or characters called 'hieroglyphs' for secret communication. Later, these pictographic forms were the basis of cryptography and thereby gave the birth for various digital cipher techniques such as mono-alphabetic substitution and Caesar shift. Cryptography is the art of secret writing by converting secret information into a mean-

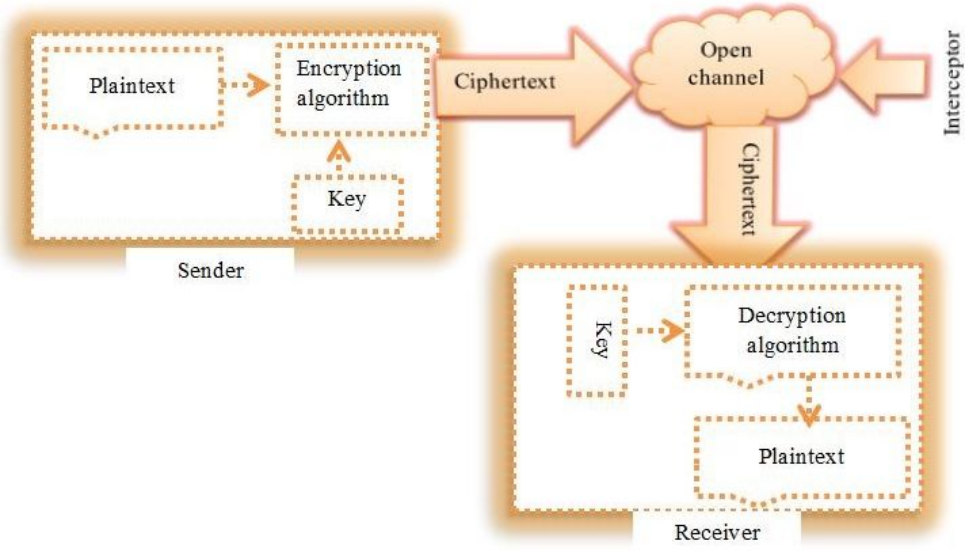

Figure 3: General structure of the cryptographic communication process.

ingless or unintelligible form. This can be accomplished by using mathematical theories and computational intelligence.

Figure 3 displays the general working principle of cryptographic communication between the sender and receiver. The basic components of cryptographic systems are (1) the information which has to be securely transmitted (plaintext) (2) the encryption algorithm, which uses secret information to transform the plaintext into an absurd form (ciphertext) (3) the decryption algorithm for retrieving the secret information, and (4) the key. Generally, the encryption and decryption algorithms require the use of keys for encryption and decryption. Therefore, the keys need to be strong and have to be stored in a safe place, in order to make the encryption computationally unbreakable. So, the keys are the key to achieving a high degree of confidentiality. The cryptographic keys are grouped into either secret or public keys. Secret keys are those that are known only to the originator and the intended receiver. Conversely, public keys are known to all. Cryptanalysis is the process of breaking the encrypted information to retrieve confidential information. From hieroglyphs to World War II, cryptography has been extensively used primarily for secure communications between the sender and receiver. Recently, cryptography had become the cornerstone of various modern-day applications. Figure 4 shows some of the applications of cryptography.

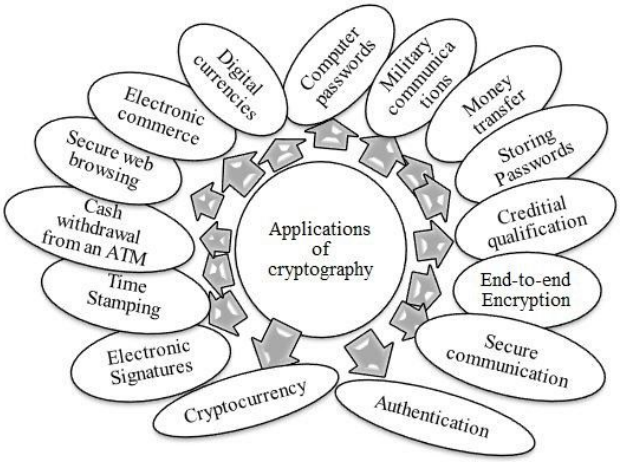

Figure 4: Applications of cryptography.

2.2 Digital Watermarking

Watermarking is a kind of digital marking technique predominantly utilized for ownership identification. Digitally, it was initially coined by Andrew Tirkel *et al.* [38] in 1992. Generally, the watermark is inserted in a signal known as the host signal. The receiver retrieves the watermark from the watermarked signal. Imperceptibility and robustness are the two fundamental requirements for watermarking techniques. Figures 5 and 6 show the procedure of watermark insertion and extraction pictorially. Watermarking can be fragile, robust, or semi-fragile. The fragile watermark can not extract the watermark after the slightest modification to the watermark. Consequently, they are commonly applicable for authentication purposes only. On the

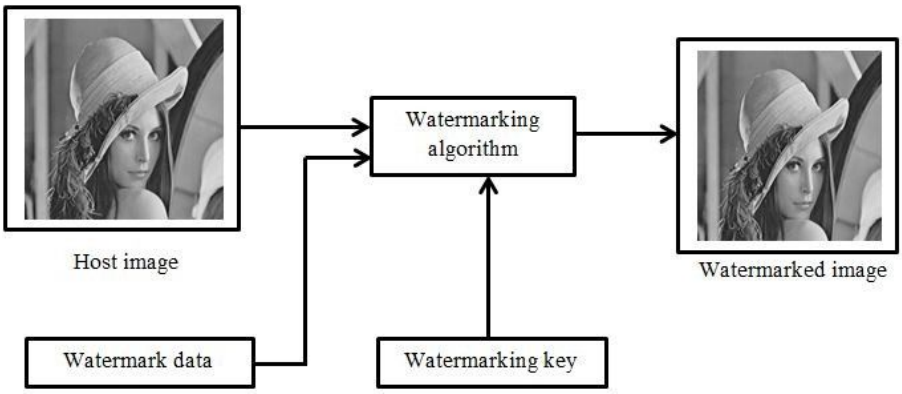

Figure 5: Watermarking embedding process.

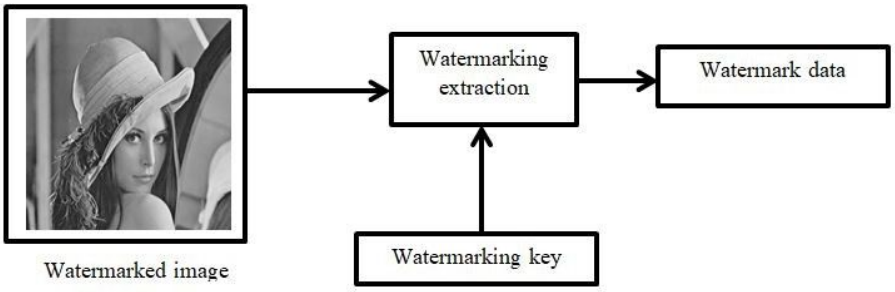

Figure 6: Watermarking extraction process.

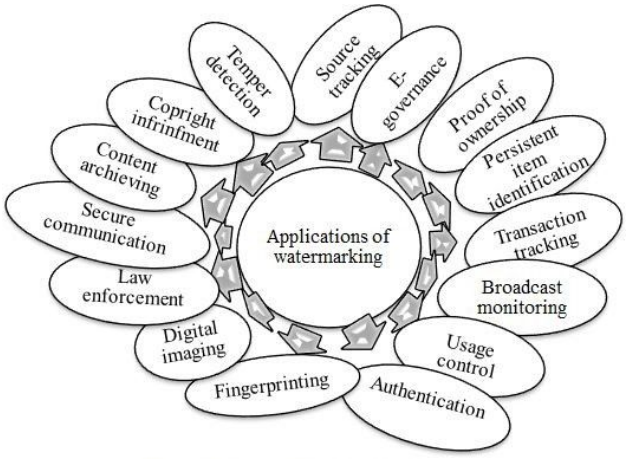

Figure 7: Applications of digital watermarking.

other hand, the robust watermarking technique is able to extract the watermark accurately even after there has been some alteration to the watermark. Therefore, these techniques are commonly applied for copyright protection. Finally, the semi-fragile watermark technique takes benefits from both robust and fragile watermarks. These techniques are primarily used for both integrity and authentication. Further, the semi-fragile watermark techniques are able to detect the tempered area localization and recovery.

Figure 7 shows the various applications of watermarking in real life.

2.3 Digital steganography

The basic idea of steganography is to hide the very existence of the secret communication from the unintended receiver. With advances in digitization, steganography has seen enormous possibilities. Since the core concept of steganographic communication lies in the secrecy of the transmission, therefore, it is more suitable in applications where encryption-based communication is restricted. Today, steganography has been part and parcel for various IoT enabled industry applications, smart cities, medical imaging, and military applications, etc. Figure 8 displays the general structure of the steganographic embedding and extraction process.

Instinctively, steganography is a kind of double-edged sword. Due to the property of invisibility, steganography is also famous among antisocial elements for covert communication. It is believed that steganographic communication was one of the weapons behind the 9/11 World Trade Center attack. Figure 9 shows various real-life applications of steganography.

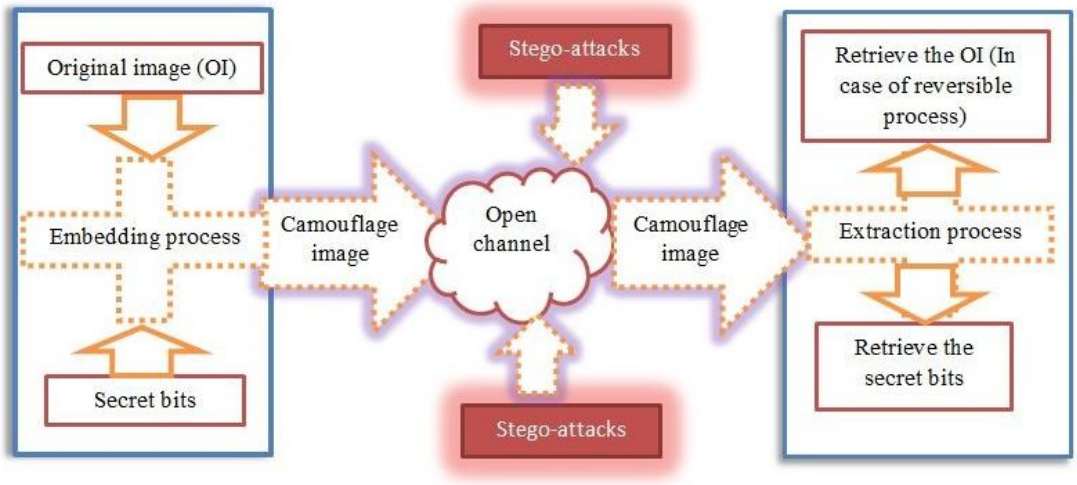

Figure 8: General structure of the steganographic communication process.

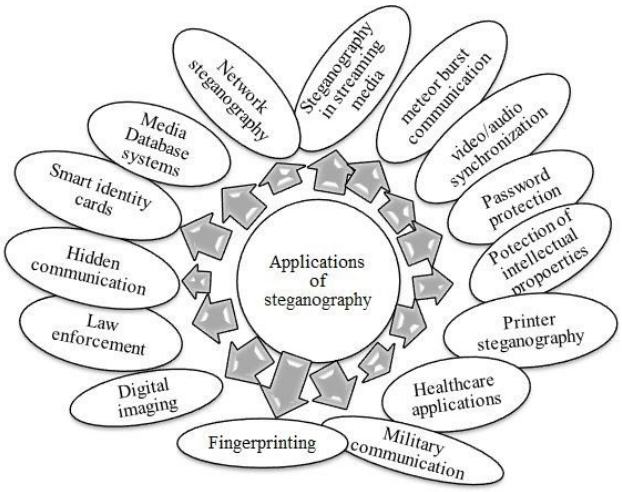

Figure 9: Applications of steganography.

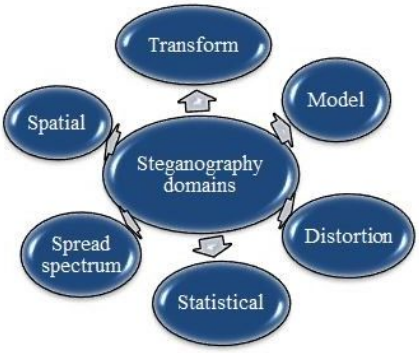

Figure 10: Various steganography domains.

The steganographic process uses various digital objects as the carrier signals such as image, text, DNA, video, audio, and text, etc. Due to the property of innocence of digital images, researchers have preferred images as the carrier signal for hiding secret information. Also, the presence of redundant pixels in an image makes it even more suitable for embedding secret information. Hiding confidential information inside the image is known as image steganography (IS). Figure 10 shows various domains in which steganography can be operated. However, most of the techniques presented in the literature were highly focused on either the spatial or transform domain.

Spatial domain techniques depend solely on the pixels of the image for data embedding. Mostly, direct manipulation of the OI pixels is performed to achieve the objective. Therefore, spatial domain techniques are simple and less time-consuming. On the other hand, transform domain techniques utilize the frequency content, and they are based on orthogonal transformation (frequency and phase) to the image. In the transform domain, applying various transformations and inverse transformations, such as Fourier, Laplace, and Z the embedding process is carried out. Some common transform domain techniques are (1) discrete Fourier transformation (DFT) (2) discrete wavelet transformation (DWT) (3) discrete cosine transformation (DCT), and (4) singular value decomposition. Figure 11 displays the classification of spatial domain ISTs.

In the context of IS, the original image (OI) is the one input image that is used for sending the secret data. Similarly, the camouflage image (CI) is the output image which carries the secret information. The secret information is the confidential message that the sender wants to transmit to the receiver. Finally, the embedding and extraction algorithms are the data hiding algorithms that are used to embed and extract the secret bits, respectively.

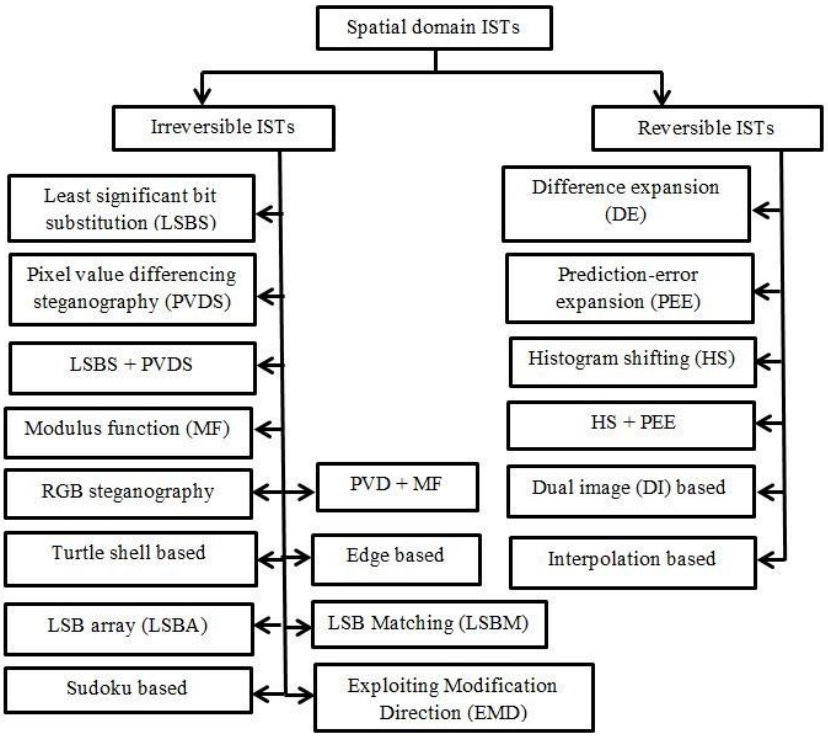

Figure 11: Classification of spatial domain ISTs.

3 Performance appraisal metrics for the ISTs

The primary objectives for any ISTs are to simultaneously achieve (1) high HC, (2) better imperceptibility, and (3) greater robustness or security. The HC refers to the ability to hide the maximum number of secret data. It is usually computed in bits. Imperceptibility suggests CI quality. The CI and OI should be visually indistinguishable. In other words, the CI should be imperceptible from the OI. The quality of subtlety in the CI can be computed using various image quality assessment metrics such as (1) mean square error (MSE), (2) peak signal-to-noise ratio (PSNR), (3) weighted PSNR (WPSNR) (4) root mean square error (RMSE), (5) universal image quality index (Q), (6) structural similarity index (SSIM), (7) normalized cross-correlation (NCC), (8) Kullback-Leibler (KL) divergence (D_{KL}), (9) Manhattan distance (MD) and (10) Euclidean distance (ED).

Similarly, security refers to the attack resistance ability (ARA). However, these metrics has an adverse impact on the performance of each other. Figure 12 shows the conflicting relation among these three metrics. So, an ideal IST should always look to achieve a fair balance among these three conflicting measures. Further, the requirements for an efficient and competent IST are mentioned in Table 2. Following this, the performance appraisal metrics for the ISTs are presented below in Table 3.

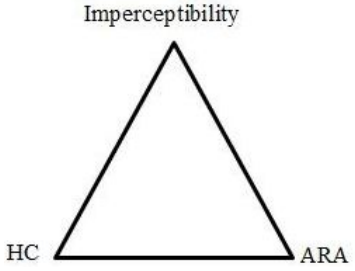

Figure 12: Adverse relation among the HC, imperceptibility, and security.

Table 2: Requirements for an efficient IST.

Metric	Condition
HC	Should be High
Imperceptibility	Should be High
Security or ARA	Should be High
Tamper resistance	Should be High
Computation complexity	Should be Low

Table 3: IS performance appraisal metrics.

The **hiding capacity (HC)** is the total number of bits an image can conceal. It is also known as embedding capacity, or capacity. The HC should be high for delivering a considerable amount of secret bits. Further, the bits per pixel (*BPP*) gives the average embedding rate for each pixel. *BPP* is found using Equation (1).

$$BPP = \frac{Size\ of\ concealed\ bits}{Size\ of\ OI} \tag{1}$$

PSNR computes the distortion in the CI in Decibel (dB). Better quality of CI can be obtained when the *PSNR* is high. It can be measured using Equation (2).

$$PSNR = 10 \times \log_{10} \frac{255 \times 255}{\text{MSE}} \tag{2}$$

Where *MSE* can be calculated using Equation (3).

$$MSE = \frac{1}{x \times y} \Sigma_{p=1}^{x} \Sigma_{q=1}^{y} \left(O_{pq} - C_{pq}\right)^2 \tag{3}$$

Where O_{pq} and C_{pq} are the corresponding OI and CI pixels at p^{th} and q^{th} coordinates.

RMSE measures the distortion in the CI. It can be obtained using Equation (4).

$$RMSE = \sqrt{\frac{1}{x \times y} \Sigma_{p=1}^{x} \Sigma_{q=1}^{y} \left(O_{pq} - C_{pq}\right)^2} \tag{4}$$

The **WPSNR** quality metric is an advancement of *PSNR*. *WPSNR* considers the properties of the human visual system. *WPSNR* can be obtained using Equation (5).

$$WPSNR = 10 \times log_{10} \frac{255 \times 255}{MSE \times NVF} \tag{5}$$

Where *NVF* represents the noise visibility function. *NVF* ranges from 0 (complete complex area) to 1 (complete smooth area). Equation (6) is used to obtain *NVF*.

$$NVF = NORM\left(\frac{1}{1 + \sigma_{BLOCK}^2}\right) \tag{6}$$

Where σ is the standard deviation and NORM function used to normalize the obtained value to either 0 or 1.

Normalized absolute error (NAE) is used to measure image quality. *NAE* can be computed using Equation (7).

$$NAE = \frac{\Sigma_{p=1}^{x} \Sigma_{q=1}^{y} (|O_{pq} - C_{pq}|)}{\Sigma_{p=1}^{x} \Sigma_{q=1}^{y} O_{pq}} \tag{7}$$

A larger value for the *NAE* is the indication of a distorted image.

Normalized Cross Correlation (NCC) is used to compute the degree of proximity or similarity between the OI and CI. NCC can be calculated using Equation (8).

$$NCC = \sum_{p=1}^{x} \sum_{q=1}^{y} \frac{(O_{pq} \times C_{pq})}{(O_{Pq})^2} \tag{8}$$

NCC ranges from −1 to 1. The value of NCC close to 1 denotes the high proximity between the OI and CI.

The **MD** is used to find the sum of the fluctuation between the corresponding pixels. Assume the OI pixels are O(o_0, o_1, o_2, o_3……, o_{255}) and the CI pixels are C(c_0, c_1, c_2, c_3……, c_{255}). In other words, the MD finds the fluctuation between the histograms of the OI and CI. It can be obtained using Equation (9).

$$MD(O, C) = \Sigma_{p=0}^{255} |o_p - c_p| \tag{9}$$

The **ED** is used to find the root of the total square differences. The $ED(OI, CI)$ can be obtained using Equation (10).

$$ED(OI, CI) = \sqrt{\Sigma_{p=0}^{255} |(o_P - c_P)^2|} \tag{10}$$

KL divergence (D_{KL}) is utilized to compute the difference between the histograms of the OI and CI. Assume h_1 and h_2 are the respective histograms for the OI and CI. Let D_{KL1} represent the D_{KL} from h_1 to h_2. Similarly, assume D_{KL2} represents the D_{KL} from h_2 to h_1. $D_{KL1}$and D_{KL2} can be obtained using Equations (11) and (12).

$$D_{KL1} = \Sigma_{p=0}^{255} h_1(p) \times log \frac{h_1(p)}{h_2(p)} \tag{11}$$

$$D_{KL2} = \Sigma_{p=0}^{255} h_2(p) \times log \frac{h_2(p)}{h_1(p)} \tag{12}$$

Finally, the mean D_{KL} (D_{KLmean}) is obtained using Equation (13).

$$D_{KLmean} = \frac{D_{KL1} + D_{KL1}}{2} \tag{13}$$

Q and **SSIM** both measure the similarity between OI and CI. The optimum value for both Q and SSIM is 1. Q can be found using Equation (14).

$$Q = \frac{4\sigma_{oc}\overline{o}\overline{c}}{\left(\sigma_o{}^2 + \sigma_c{}^2\right)\ \left[\left(\overline{o}\right)^2 + \left(\overline{c}\right)^2\right]} \tag{14}$$

Where σ_{oc} is the co-variance, $\overline{o}$ and $\overline{c}$ are the mean, σ_o^2 and σ_c^2 are the standard deviation for the corresponding OI and CI. $\overline{o}$, $\overline{c}$, σ_o^2, σ_c^2, and σ_{oc} are calculated using Equations (15), (16), (17), (18) and (19).

$$\overline{o} = \frac{1}{x \times y} \Sigma_{p=1}^{x} \Sigma_{q=1}^{y} (o_{pq}) \tag{15}$$

$$\sigma_o^2 = \frac{1}{x \times y - 1} \Sigma_{p=1}^{x} \Sigma_{q=1}^{y} (o_{pq} - \overline{o})^2 \tag{16}$$

$$\overline{c} = \frac{1}{x \times y} \Sigma_{p=1}^{x} \Sigma_{q=1}^{y} (c_{pq}) \tag{17}$$

$$\sigma_c^2 = \frac{1}{x \times y - 1} \Sigma_{p=1}^{x} \Sigma_{q=1}^{x} (c_{pq} - \overline{c})^2 \tag{18}$$

$$\sigma_{oc} = \frac{1}{x \times y - 1} \Sigma_{p=1}^{x} \Sigma_{q=1}^{x} (o_{pq} - \overline{o})(c_{pq} - \overline{c}) \tag{19}$$

SSIM can be computed by using Equation (20).

$$SSIM = \frac{(2\mu_o\mu_c + k_1)(2\sigma_{oc} + k_2)}{(\mu_o^2 + \mu_c^2 + k_1)(\sigma_o^2 + \sigma_c^2 + k_2)} \tag{20}$$

Where, k_1 are k_2 are the constants. σ_{oc} is the covariance. μ_o and μ_c are the mean, μ_o^2 and μ_c^2 are variance and σ_o^2 and σ_c^2 are the standard deviations for the corresponding OI and CI.

An overflow and underflow problem (OUP) occurs when the pixels after embedding exceeds 255 or goes below 0. Since the value beyond 255 or below 0 is not considered, therefore, the OUP pixel loses its original value. With this, the secret bits that are embedded in those pixels will also be lost. So, at the receiving end, the secret bits cannot be extracted accurately. This results in an incorrect output image. Also, the hidden data inside the pixels will be lost. To avoid this, the OUP pixels should not be chosen for embedding. Therefore, the occurrence of OUP results in an inaccurate CI or reduces the HC significantly. So, OUP should be avoided.

Steganalysis: Security to the embedded data is of paramount importance during data transmission. Therefore, for any steganography technique, the success primarily lies in its ARA. In this aspect, the process of finding the presence of secret information from the SI is called steganalysis. There are many such steganalysis techniques available, and they can be classified into either structural or non-structural steganalysis. Some of the structural steganalysis techniques are RS analysis, bit plane analysis, pixel difference histogram (PDH) analysis, chi-square statistical attack, sample pair analysis (SPA) and weighted stego (WS) analysis. On the other hand, non-structural steganalysis utilizes the concept of feature extraction to model the OI. Further, the trained classifier identifies the difference in features for the Ol as well as the CI. Some commonly used non-structural steganalysis techniques are subtractive pixel adjacency matrix (SPAM) and spatial-rich model (SRM).

RS analysis is statistical analysis. To implement this, initially, partition the image into various disjoint pixel groups. Suppose one such group is $O = (o_i, o_{i+1} \ldots o_n)$, where o_i, $o_{i+1} \ldots o_n$ are the pixels belonging to this group. To measure the smoothness of each pixel group, the discrimination function defined as $f(o_i, o_{i+1} \ldots o_n) = \sum_{i=1}^{n-1} |o_{i+1} - o_i|$. A greater value for f() signifies the greater scale of noise and vice versa. Further, the two opposite flipping functions F_1 and F_{-1} are used for the transformation from an even to odd and odd to even pixel respectively. Then, the pixels are grouped into regular (R_m and R_{-m}), and singular (S_m and S_{-m}) groups. Equations (21), (22), (23) and (24) are used to compute the regular and singular pixel groups.

$$R_m = \frac{Total\ number\ of\ blocks\ satisfying\ f\ (F_1(O)) > f(O)}{Total\ number\ of\ blocks} \tag{21}$$

$$S_m = \frac{Total\ number\ of\ blocks\ satisfying\ f\ (F_1(O)) < f(O)}{Total\ number\ of\ blocks} \tag{22}$$

$$R_{-m} = \frac{Total\ number\ of\ blocks\ satisfying\ f\ (F_{-1}(O)) > f(O)}{Total\ number\ of\ blocks} \tag{23}$$

$$S_{-m} = \frac{Total\ number\ of\ blocks\ satisfying\ f\ (F_{-1}(O)) < f(O)}{Total\ number\ of\ blocks} \tag{24}$$

Now, using these groups, the RS-plot is observed where the HC is represented in the x-axis, and the regular and singular groups are represented in the y-axis. At first, ten CIs are obtained from the OI. Here, the first SI contains 10% of the secret data. Similarly, for the successive images, the embedding rate is promoted at the rate of 10% each. Finally, the tenth CI contains 100% of the secret data. Then, drawing the curves for the regular and singular groups, the RS plot can be obtained. Further, from the observed plot, if the case $R_m \approx R_{-m} > S_m \approx S_{-m}$ is satisfied, then the technique effectively withstands against RS analysis. But, the case $R_{-m} - S_{-m} > R_m - S_m$ exposes the technique.

PDH analysis analyzes the difference between the OI and CI using a histogram. This is implemented as follows. At first, create blocks of two successive pixels each. Let v_i be the fluctuation between two successive pixels in each block. The minimum and maximum intensity values for a pixel are 0 and 255. Therefore, $v_i$values will be in the range from −255 to 255. Now, calculate the frequency of each v_i. Plot a graph with the frequency of v_i in the y-axis and the distinct v_i values on the x-axis. Observe the above steps for both OI and CI. Then the PDH plot will be obtained. Now, from the PDH plot, if we observe the curves for both the OI and CI are smooth lines which overlap each other, then there is no evidence of hidden data. However, a zig-zag curve with clear separation from the OI curve for the CI exposes the technique.

Bit plane analysis: The bit plane analysis can capture the presence of embedded information from the LSBs of the pixels. Each plane for a pixel has some correlation with their neighbor planes. The structural feature for the pixels can be altered when there is a change to any of the bit planes. Therefore, analyzing the individual bit planes of the CI can lead to exposing the presence of secret information for the LSBS based techniques.

Chi-square analysis (x_c^2): A Chi-square test is a statistical test initially developed by Westfield and Pfitzmann [34]. The basic idea of this analysis is to measure whether the observed and expected sets of data are similar or not. This degree of similarity finds the probability of whether embedding has happened or not. A Chi-square test provides this degree of probability. This test states that, for a typical image, it is unusual for the frequency of DCT coefficient 2k to be nearly equal to the frequency of DCT coefficient 2k+1. However, after embedding the secret bits using an embedding algorithm that produces a pair of values, then the frequencies of 2k and 2k+1 become equal or nearly so. Therefore, this attack is primarily designed to identify the near equal pair of values. Equation (25) is used to perform this test,

$$x_c^2 = \sum \frac{(O_i - E_i)^2}{E_i} \tag{25}$$

where c, O and E denote the degrees of freedom, observed, and expected values, respectively.

SPAM steganalysis is the universal steganalysis that uses different feature extraction strategies to train the classifiers. One of the earliest developments on universal steganalysis was proposed in that take out the SPAM features with 686 dimensions. SPAM features are extracted using the difference between the adjacent pixels and utilize the first and second order of Markov chains. SPAM features with the 686 dimensions are extracted as features to compute the higher-order dependence among the pixels. In the Markov chain SPAM feature extraction process, the signal-to-noise ratio (SNR) is raised by finding the residuals of adjacent pixels.

Table 4: Silent features of various state-of-art review papers that are reported till date.

Referred paper	Year of publication	Key features	Number of papers reviewed
Kadhim *et al.* [2]	2019	Provided a complete overview of ISTs including the background of steganography, properties, applications, performance evaluation parameters, general operation, and classification of ISTs. Also presents an overview of signature and statistical steganalysis.	277
Cheddad *et al.* [3]	2010	Presented a state-of-the-art review of existing ISTs along with the possible applications of steganography. Advocates for the object-oriented data hiding. Finally, discusses steganalysis using visual inspection and histogram analysis.	127
Johnson and Jajodia [4]	1998	Facilitated the information about the evolution of steganography and available steganographic software. Also, presents an overview of various image files and formats.	10
Hussain *et al.* [5]	2018	Gave the general structure of the IS system and its classifications. Discussed various performance parameters and steganalysis attacks. Further, highlighted the pros and cons of existing up-to-date techniques.	145
Atawneh *et al.* [6]	2014	Discusses the LSBS technique and other frequency-domain techniques such as DCT, DFT, and DWT. Provides the details about many steganography software like F5, outGuess, JPEG-JSteg, model-based steganography, Perturbed quantization, S-Tools and compares them.	74
Nisha and Monoth [7]	2019	Furnished the general concepts of PVDS techniques and latest developments in PVDS techniques.	27
Karampidis *et al.* [8]	2018	Presented various steganalysis techniques such as visual, signature, statistical, spread spectrum, transform domain, universal or blind for detection of hidden data.	119
Nissar and Mir [9]	2010	Presented various steganalysis techniques such as signature and statistical. Further, some promising statistical steganalysis techniques have been advocated.	115
Singh *et al.* [10]	2018	Briefly overviewed digital image watermarking techniques, its applications, the concept of watermark embedding and extraction processes, common types of watermarking techniques, major classification of watermarking attacks.	80
Subhedar and Mankar [11]	2014	Reviewed the fundamental IS concepts, performance analysis measures, security aspects, compared various reversible and irreversible spatial as well as transform ISTs in terms of HC and image quality. Also, provides current status and future directions of IS.	105
Hussain *et al.* [12]	2015	Presented the critical analysis of existing literature of PVDS based techniques with respect to HC, ARA, and imperceptibility. Also, highlights the potential future applications of PVDS technique.	20
Sahu and Swain [13]	2016	Reviewed various literature on LSBS and PVDS ISTs. Further, presents the comparative evaluation of these ISTs with respect to HC, imperceptibility, security, and computational complexity.	41
Kharrazi and Sencar [14]	2006	Discussed the impact of factors such as length of the embedding payload, texture area, compression, recompression, computational resources on the performance of the ISTs and steganalysis.	21
Li *et al.* [15]	2011	Reviewed the fundamental concepts of IS. Also, it presented the current status and progress of spatial domain ISTs, JPEG steganography. Further illustrates various steganalysis techniques such as RS analysis, histogram analysis, universal steganalysis, histogram characteristic function of the center of mass (HCF-COM).	89

Table 4: ... continued

Referred paper	Year of publication	Key features	Number of papers reviewed
Judge [16]	2001	Explored steganography from inception and outlined some promising directions.	52
Amirtharajan *et al.* [17]	2012	Highlighted the possible ways of random IS with theoretical illustrations.	49
Kahn [18]	1996	Presented the rich history of steganography with various illustrative incidences.	––
Mishra *et al.* [19]	2012	Provided a brief report on various spatial and transform domain techniques.	16
Provos and Honeyman [20]	2003	Explored the practical applications of statistical steganalizer tools such as histogram, receiver operating characteristic (ROC) for outGuess and F5 detection.	29
Petitcolas *et al.* [21]	1997	Presented the overview and general working principle of steganography. Further discussed attacks such as basic, robustness, mosaic attack, and interpretation attacks.	149
Vinodhini *et al.* [22]	2017	Presented various ISTs, especially focused on DNA, DI based steganography with their merits and issues.	15
Wang and Wang [23]	2004	Outlined the background of steganography. Also discussed existing steganography and steganalysis tools and techniques.	12
Altaay [24]	2012	Briefly presented various types of steganography with their requirements.	33
Abraham and Paprzycki [25]	2004	Presented various LSBS techniques and provided a direction to achieve robustness for LSBS techniques.	16
Amirtharajan and Rayappan [26]	2013	Presented the principles and attributes for steganography techniques. Further, an insight into the future directions of steganography is discussed.	78
Pradhan [27]	2016	Provided the complete IS parameters. Also illustrated the effectiveness of RS and PDH analysis.	42
Meng *et al.* [28]	2018	Provided a detailed insight on various ISTs based on deep learning.	147
Girdhar and Kumar [29]	2018	Presented a comprehensive review of recent advances and practices of 3D IS. Furthermore, the current status and limitations of 3D IS has also been reported.	67
Artz [30]	2001	Provided the use and limitations of steganography.	5
Trivedi *et al.* [31]	2016	Various spatial domain ISTs are compared with their merits and issues.	36
Jung [32]	2016	Performance of several DI based RDH techniques are compared in terms of the HC and the CI visual quality.	16
Shi *et al.* [33]	2016	Provided an exhaustive discussion on the various categories of RDH techniques along with its merits and demerits.	199

4 Review of various spatial domain ISTs with their merits and issues

This section reviews various spatial domain ISTs with respect to the IS parameters like BPP, PSNR, OUP pixels, and ARA to various stego-attacks. Predominantly, techniques like LSBS, LSBA, LSBM, PVDS, LSB+PVD, LSB+PVD+MF, edge-based, reversible, convolution neural network (CNN) based, and some other related ISTs are discussed. To measure the imperceptibility, usually, PSNR is the ideal parameter that has been considered by many researchers. Next, the HC of the respective techniques can be gauged by knowing the BPP. Therefore, these two parameters are consistently utilized for measuring the performance of all the reviewed techniques. Next, the ARA for these techniques against various steganalysis attacks is also presented. Again, the PVDS based techniques suffer from OUP; therefore, the ability of these techniques against OUP is also shown. In Tables 5, 7, 10, 11, 12, 13 and 14, the symbols $\surd$, × and – represents 'yes', no' and 'unknown' for the various parameters. Below, the discussion on various ISTs is presented with their merits and issues.

4.1 LSBS technique

The LSBS technique is by far the oldest and simplest IS technique that replaces the LSBs of the OI pixels with secret bits [39]. Also, the HC can be further improved by substituting secret bits with the LSBs of the OI pixels. An illustration of the 1LSBS technique is displayed in Figure 13. The literature has produced various LSBS based techniques where some improved the HC and others the CI quality. However, the classical LSBS techniques are exposed to statistical analysis such as RS analysis, bit plane analysis and chi-square analysis.

Figure 14a shows the RS plot of the Lena image when there is no data embedded inside the image. This can be clearly observed in the case $R_m \approx R_{-m} > S_m \approx S_{-m}$. On the contrary, the presence of the secret information is quite clearly noticeable for the simple 1LSBS technique. This is shown in Figure 14b. Here, the condition $R_{-m} - S_{-m} > R_m - S_m$ holds well. Similarly, when we plot the histogram for the CI of the three LSBS techniques with the original one, it is found that the histogram of OI and CI for the 1LSBS technique is identical. However, the zig-zag nature of the CI can be easily spotted for both 2LSBS and 3LSBS techniques. Figure 15a,b,c shows the respective PDH-plots for the 1LSBS, 2LSBS and 3LSBS techniques.

At the same time, if we perform bit plane analysis on the LSB plane for the simple LSBS technique, one can easily identify the visual artifacts on the planes of the CI, and that differs from the OI planes. Figure 16 shows the corresponding plane images for the respective bit planes of the original Lena image. Similarly, Figure 17 shows the corresponding plane images of the 1st bit plane for (a) original Lena image (b) 1LSBS (c) LSBM [77] and (d) Wu and Tsai [94]. It is desirable to mention here that the 1LSBS technique performs sequential embedding, whereas the other two that are considered here follow the randomized embedding procedure. From the obtained images, it is evident that the 1LSBS technique is smooth and different from the first bit plane of the OI. Therefore, anyone can easily guess the presence of information. On the other hand, bit plane images in Figures 17c and 17d are quite random and similar to the bit plane of the OI. Therefore, they show resistance to the bit plane analysis. Finally, it is reasonable to conclude that bit plane analysis can highlight the manipulated regions for the sequential LSBS embedding technique. However, to escape from this analysis, one can perform randomized embedding instead of sequential embedding.

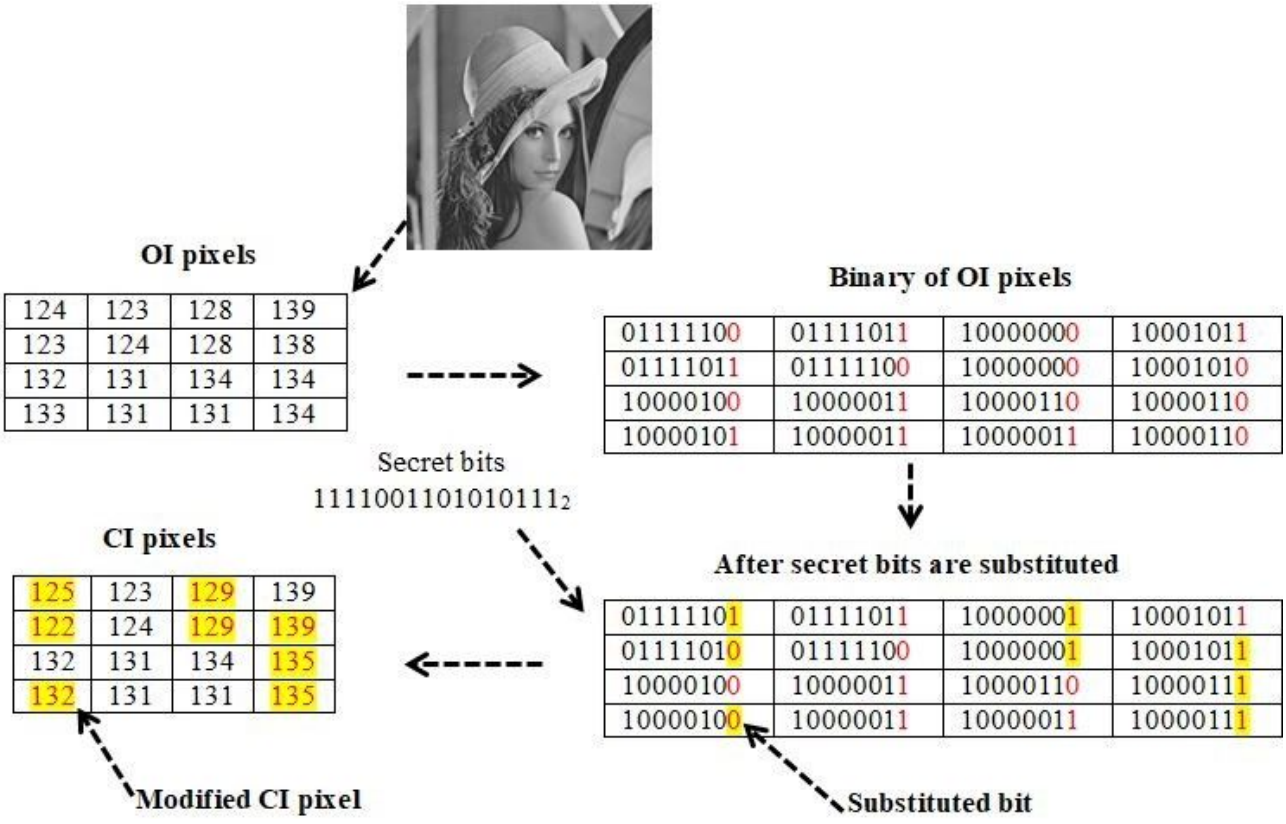

Figure 13: An illustration of 1LSBS technique.

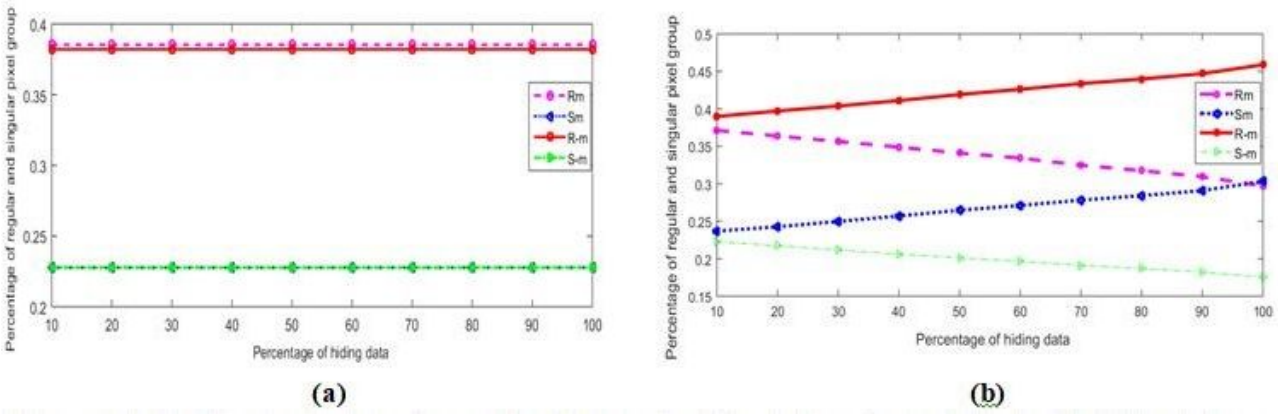

Figure 14: RS plots for the Lena image (a) with no embedding information and (b) for 1LSBS technique.

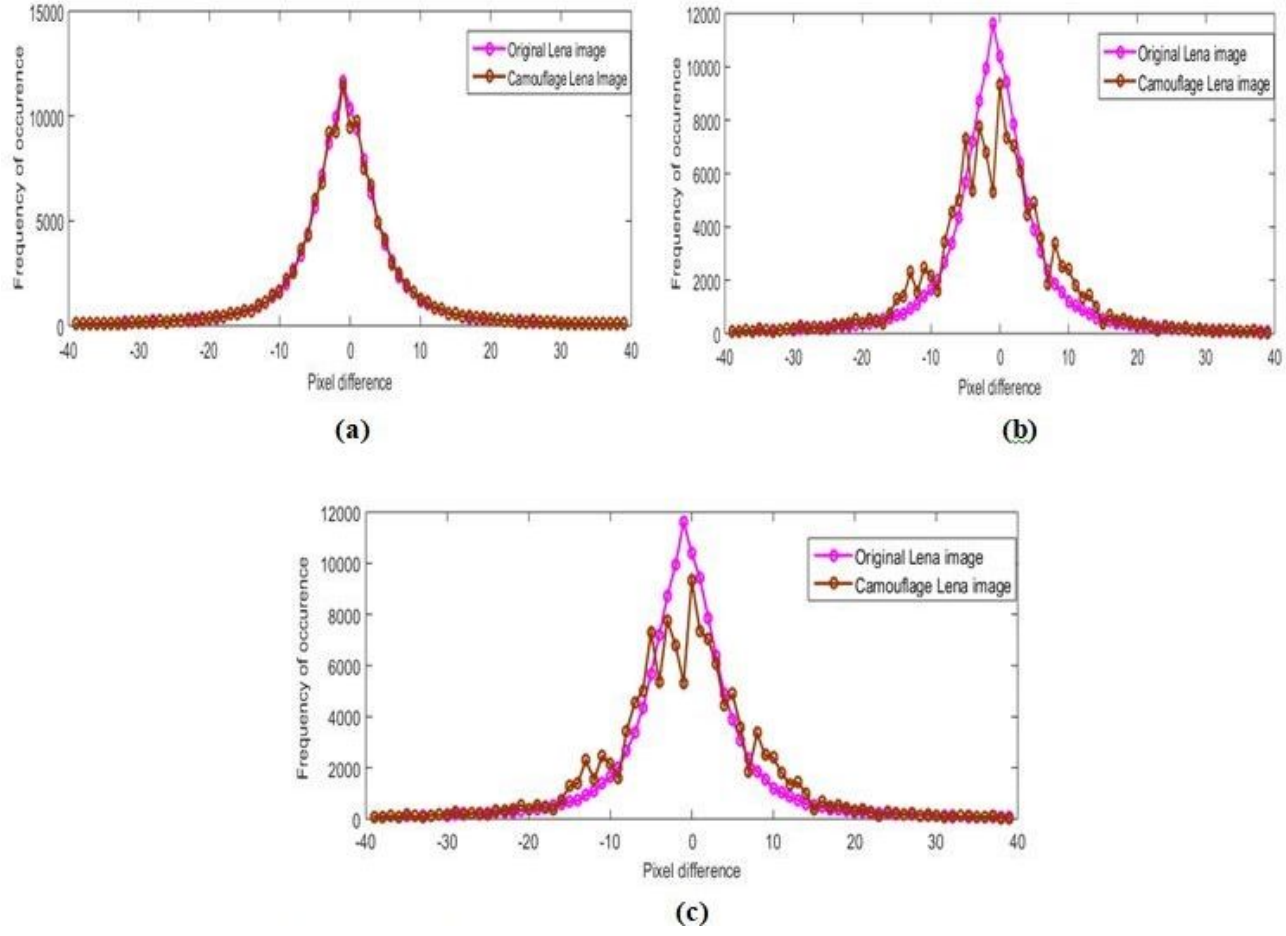

Figure 15: PDH-plots for Lena OI and CI for (a) 1LSBS, (b) 2LSBS and (c) 3LSBS.

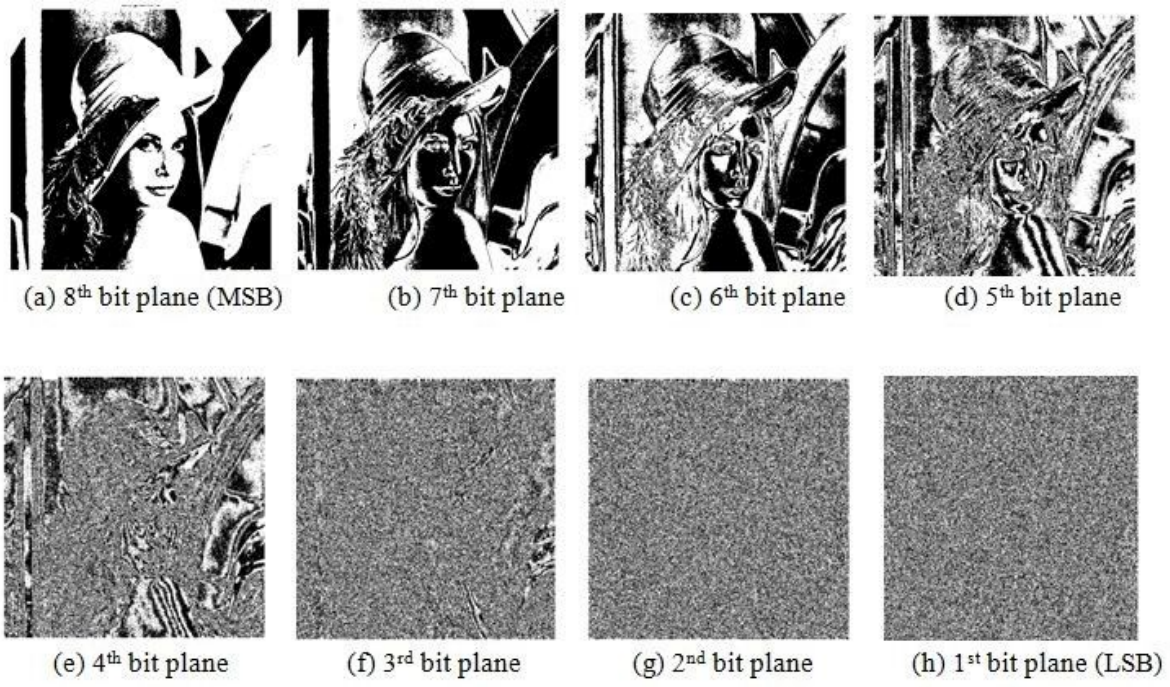

Figure 16: Respective bit planes (starting from LSB) for the Lena OI (with no embedding information).

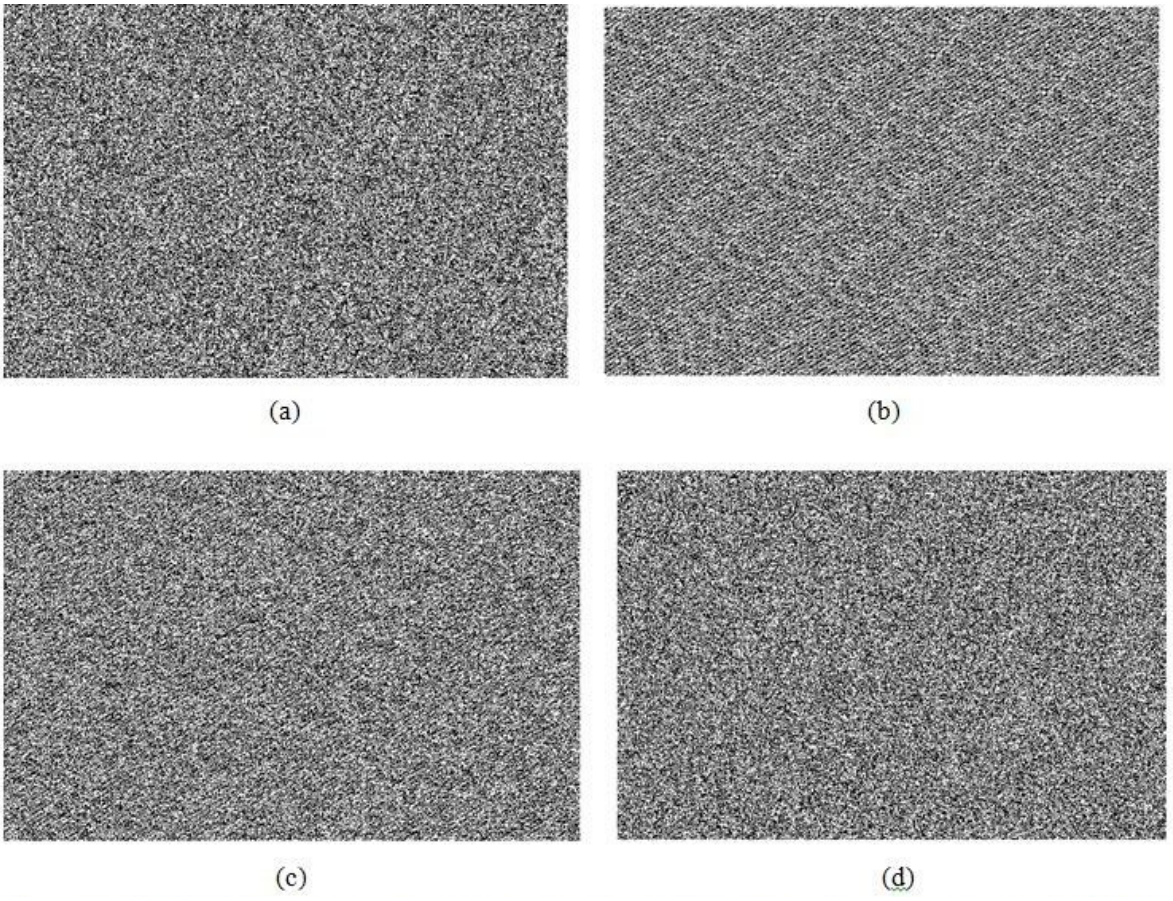

Figure 17: Displaying the produced images from the 1^{st} bit planes of (a) original Lena image (b) 1LSBS (c) LSBM [77], and (d) Wu and Tsai [94].

→ **Merits of LSBS based technique**

- One of the most significant advantages of the LSBS technique is its simplicity.
- Further, the HC can be raised by a greater number of LSBs for embedding the secret bits.

→ **Issues of LSBS based technique**

- The CI quality degrades when the MSBs are utilized for embedding the secret bits.
- Another major drawback is its weak ARA to various statistical analyses like RS analysis, bit plane analysis, and chi-square analysis.

In the past, authors have reported improved LSBS techniques. Wang *et al.* [52] suggested a local pixel adjustment process using the moderately-significant-bit strategy to improve the HC without reducing the CI quality. To further improve the CI quality, authors in [53] devised an optimal MSB replacement technique. Wang *et al.* [54] obtained an imperceptible CI compared to the classical LSBS technique using a perceptual modeling strategy at the cost of computational complexity. Next, to reduce the computational complexity and to improve the CI quality, Chan and Cheng [55] suggested an optimal pixel adjustment process (OPAP). Chang *et al.* [56] reduced the complexity of Wang *et al.*'s [52] technique by proposing an LSBS based technique in combination with encryption. Zakaria *et al.* [57] came up with a data mapping strategy using the MSB and LSB bits to produce better CI quality with higher HC. Furthermore, this technique can survive against RS and histogram attacks. Experimentally, it has been shown that this technique outperforms [58] and [122]. Yang *et al.* [58] found the noise non-sensitive areas of the image can tolerate substantial modifications compared to noise-sensitive areas. With this, the abrupt modification to the texture area of the image is avoided. Further, this technique outperforms Yang *et al.*'s [59] and Wu *et al.*'s [134] techniques in terms of HC and PSNR. Gupta *et al.* [60] ensured dual-layered security can be achieved by using cryptography with one, and steganography with the other. Here the Rivest, Shamir, Adleman algorithm and Diffie Hellman algorithm are used during encryption, and the LSBS technique is utilized for embedding. A varying index-based LSBS technique using secret stego-keys has been suggested by Khan *et al.* [61]. This technique reduces the MSE at the cost of increased computational complexity. Authors in [63] suggested a novel n-bit embedding strategy where the value of n can range from 1 to 4. In this technique, n secret bits are embedded in the n-rightmost bits to achieve imperceptible SI as well as larger HC. Many improved LSBS techniques have been proposed by the authors in [64–93]. Following this, Wu and Hwang's [62] and LSBM [77] techniques are discussed below.

4.1.1 Wu and Hwang's improved LSBS technique [62]

Wu and Hwang [62] suggested an improved LSBS technique that produces high-quality CI. During data embedding, three consecutive pixels are considered from the OI and three secret bits are embedded in these three pixels. Consider o_1, $o_2$and o_3 to be the three consecutive pixels and b_1, b_2 and b_3 to be the three secret bits. Now, represent o_1, o_2 and o_3 in binary, as follows:

$$o_{bin1} = o_1^{LSB8} o_1^{LSB7} o_1^{LSB6} o_1^{LSB5} o_1^{LSB4} o_1^{LSB3} o_1^{LSB2} o_1^{LSB1}$$
$$o_{bin2} = o_2^{LSB8} o_2^{LSB7} o_2^{LSB6} o_2^{LSB5} o_2^{LSB4} o_2^{LSB3} o_2^{LSB2} o_2^{LSB1}$$
$$o_{bin3} = o_3^{LSB8} o_3^{LSB7} o_3^{LSB6} o_3^{LSB5} o_3^{LSB4} o_3^{LSB3} o_3^{LSB2} o_3^{LSB1}$$

Then, utilizing the notion of XOR operation using Equations (26), (27) and (28) the values of A, B and C are computed.

$$A = o_1^{LSB1} \oplus o_1^{LSB2} \oplus o_2^{LSB1} \tag{26}$$

$$B = o_2^{LSB1} \oplus o_2^{LSB2} \oplus o_3^{LSB1} \tag{27}$$

$$C = o_3^{LSB1} \oplus o_3^{LSB2} \oplus o_1^{LSB1} \tag{28}$$

Then, pixels are adjusted after comparing the values of A, B and C with b_1, b_2 and b_3. At the receiving end, the CI pixels are c_1', c_2' and c_3'. Next obtain the secret bits b_1, b_2 and b_3 from the CI pixels using Equations (26), (27) and (28). An illustration of Wu and Hwang's [62] technique is displayed in Figure 18. From the observed results, this technique offers high-quality CI as compared to the conventional LSBS and LSBM [77] techniques. Further, this technique successfully survives the statistical RS attack. However, low HC remains the major issue for this technique as this technique hides only 1 bit in each pixel.

4.1.2 LSBM steganography [77]

The LSBS technique directly replaces the LSBs with secret bits. Therefore, these techniques are exposed to RS analysis. A novel embedding strategy where the OI pixels are randomly modified with ±1 has been suggested by Sharp [76]. This technique is called the LSBM technique. However, the actual implementation of LSBM was first performed by Mielikainen [77]. The embedding and extraction steps of Mielikainen's [77] LSBM technique are discussed

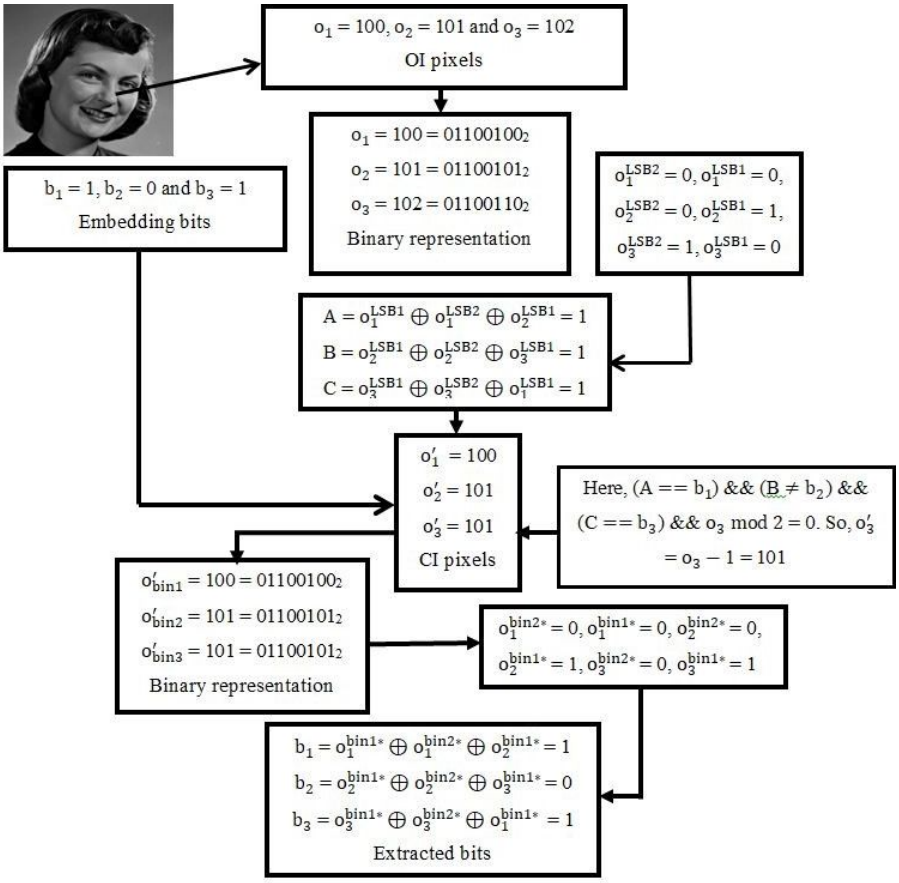

Figure 18: An illustration of Wu and Hwang's [62] technique.

below. Also, an illustration of the technique has been displayed in Figure 19.

Step 1: At the embedding end, assume $(o_1, o_2, o_3, \ldots o_n)$ are the OI pixels. Considering (o_1, o_2) as the pair of two successive pixels, and b_1 and b_2 as the embedding bits, the embedding procedure is discussed below.

Step 2: Using the function $f(.)$ and Equation (29) the stego-pixels are obtained.

$$(o_1^\star, o_2^\star) = \begin{cases} (o_1,\ o_2), if\ (LSB(o_1) = b_1) \\ and\ (f(o_1, o_2) = b_2) \\ (o_1,\ o_2 + 1), if\ (LSB(o_1) = b_1) \\ and\ (f(o_1, o_2)\ \neq b_2) \\ (o_1 - 1,\ o_2), if\ (LSB(o_1) \neq b_1) \\ and\ (f(o_1 - 1, o_2) = b_2) \\ (o_1 + 1,\ o_2), if\ (LSB(o_1) \neq b_1) \\ and\ (f(o_1 - 1, o_2)\ \neq b_2) \end{cases} \quad (29)$$

where $f(o_1,o_2) = \text{LSB}(\lfloor o_1/2 \rfloor + o_2)$.

Step 3: During extraction, obtain the secret bit b_1 from the LSB of $o_1^\star$ and b_2 from Equation (30).

$$b_2 = LSB\left(\lfloor o_1^\star/2 \rfloor + o_2\right) \quad (30)$$

The *LSBM* technique offers imperceptible CI. Further, RS and PDH analysis is not able to identify the presence of secret information in the CI. However, the LSBM technique offers very low HC.

In 2009, Juneja and Sandhu [80] initiated the idea of matching the secret bits with the OI bits. Later, using this concept, Swain and Lenka [81] proposed the LSBA based technique. In this technique, the LSB bits are collected and kept in an array. This array is named LSBA and then the secret bits are mapped with the LSBA. The index of the positions where the maximum bits are matching has been recorded for the retrieval. This technique observes excellent imperceptibility since very few bits of the OI are modified. Authors in [82, 83] have also utilized the concept of LSBA to improve the CI quality as well as the HC. Table 5 presents the results of the average PSNR, BPP, ARA to RS analysis and any other steganalysis attacks for various LSBS, LSBM and LSBA based techniques.

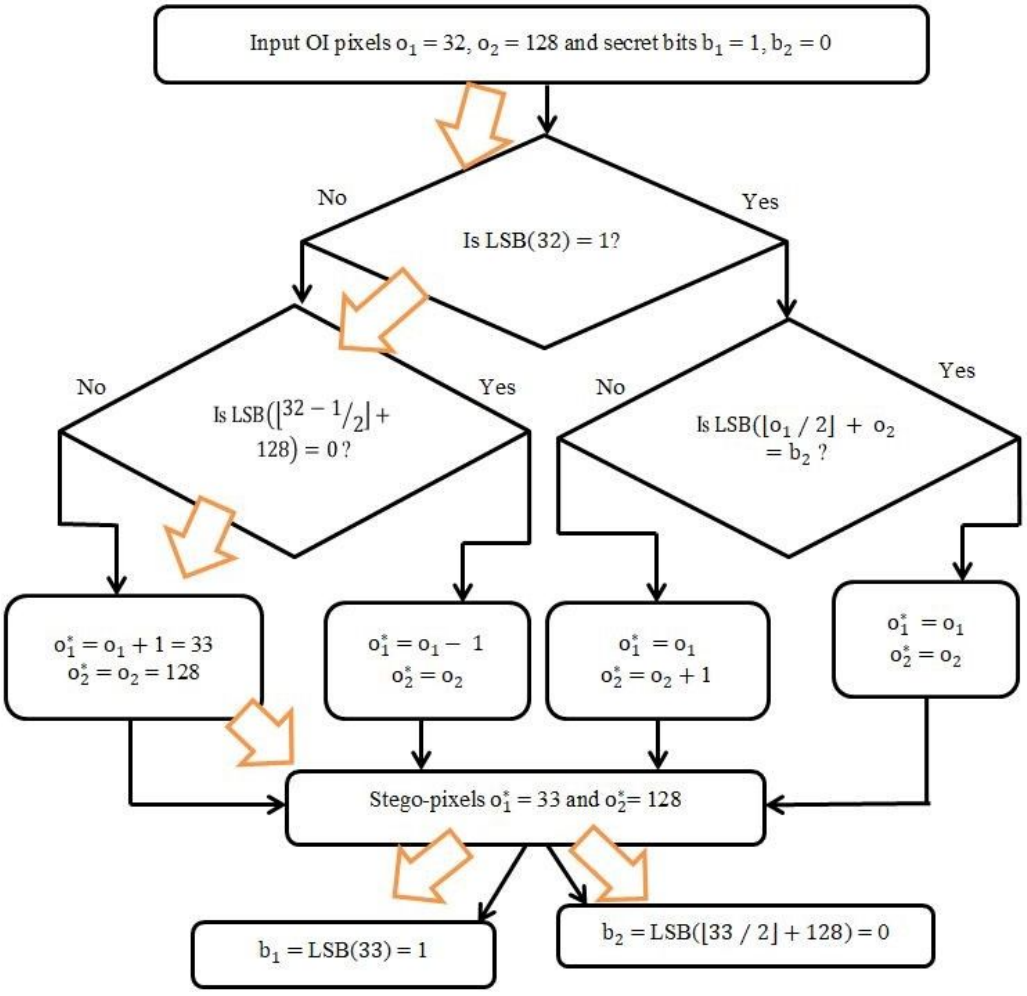

Figure 19: An illustration for Mielikainen's [77] technique.

Table 5: Analysis of LSBS, LSBM, and LSBA based techniques.

Ref.	Techniques adopted		Average PSNR (in dB)	BPP	ARA to RS analysis	ARA to any other steganalysis
Kurak and McHugh [51]	Classical LSBS technique	1LSBS	51.14	1.00	×	×
		2LSBS	44.02	2.00		
		3LSBS	37.86	3.00		
		4LSBS	31.33	4.00		
Chan and Cheng [55]	OPAP		51.14	1.00	–	–
			46.32	2.00		
			40.60	3.00		
			34.48	4.00		
Chang *et al.* [56]	Data encryption standard+LSBS +OPAP		44.17	2.00	–	–
Zakaria *et al.* [57]	LSB based data mapping strategy		42.15	3.24	√	Histogram analysis
Wu and Hwang [62]	Three pixel-based ±1 modification		52.92	1.00	√	–
Sahu and Swain [63]	n-rightmost bit replacement		51.21	1.00	√	S&P noise
			44.08	2.00		
			40.72	3.00		
			34.83	4.00		

Table 5: ... continued

Ref.	Techniques adopted	Average PSNR (in dB)	BPP	ARA to RS analysis	ARA to any other steganalysis
Hussain *et al.* [64]	Right-Most Digit Replacement +Adaptive LSBS	39.00	3.05	√	PDH analysis
Sahu and Swain [65]	Multi Stego-image based LSBM	36.06 37.88 39.60 41.00	4.00	√	–
Sahu and Swain [66]	Bit flipping (variant 1)	47.40	1.50	√	–
	Bit flipping (variant 2)	47.34	2.00	√	–
Shreelekshmi *et al.* [67]	Inverse Transitions+LSBS	50.04	1.50	–	–
Kim *et al.* [68]	Hamming code+LSBS+OPAP	51.49	1.99	√	Histogram analysis
Zhou *et al.* [69]	Quantum IS+LSBS	50.22	0.50	–	–
Sahu and Swain [70]	Three group of bits substitution	44.32	3.00	–	–
Swain [71]	1 group of bits substitution	51.64	1.00	√	PDH analysis
	2 group of bits substitution	49.76	2.00		
Jung [72]	2×2 block+Parity based	19.80	0.02	–	–
	3×3 block+Parity based	20.31	0.02		
	4×4 block+Parity based	21.72	0.01		
	5×5 block+Parity based	22.67	0.01		
	6×6 block+Parity based	23.78	0.01		
	7×7 block+Parity based	24.75	0.01		
Laskar and Hemachandran [73]	Encrypted using transposition cipher+LSBS	51.63	0.04	–	–
Elmasry [74]	Cyclic redundancy check 32+Advanced encryption standard+LSBS	40.08	2.21	√	Histogram analysis, chi-square analysis
Chakraborty *et al.* [75]	Modified median edge detector predictor+LSBS	51.87	0.15	√	Blind steganalysis
Mielikainen [77]	LSBM	52.46	1.00	√	Histogram analysis
Sahu and Swain [78]	LSBS+LSBM Variant 1	44.07	2.00	–	–
	LSBS+LSBM Variant 2	47.45	1.50		
	LSBS+LSBM Variant 3	54.38	1.00		
Sabeti *et al.* [79]	Complexity based LSBM	52.11	0.80	–	Wavelet Absolute Moment
Swain and Lenka [81]	Mapping words with LSBA	60.57	0.08	√	–
Swain and Lenka [82]	4LSBA	52.93	0.15	–	Histogram analysis
Jung and Yoo [84]	Semi-reversible+Interpolation +LSBS	43.93 37.60	1.50 2.25	–	–
Lee and Chen [85]	Variable size LSBS+Minimuin -error replacement method	32.57	4.03	–	Bit plane analysis
Sarreshtedari and Akhaee [89]	One third LSBS embedding	52.90	1.00	–	HCF COM, histogram analysis

4.2 Pixel Value Differencing Steganography (PVDS) [94]

An image consists of texture and smooth regions. The texture regions of the image can conceal potentially a greater number of secret bits than that of the smooth regions. However, LSBS based techniques do not distinguish the texture and smooth regions of an image. Wu and Tsai [94] introduced the concept of PVDS. The PVDS technique is based on the notion of pixel difference or fluctuation value (FV). Initially, the image is divided into various blocks with two consecutive pixels (CPs). Then, FVs between the CPs of the respective blocks are obtained. Later, using these FVs, the embedding process is performed in each block. The embedding and extraction algorithm for Wu and Tsai's [94] PVDS technique is discussed below, followed by an illustration in Figure 20. Next, Table 7 presents the results of the average PSNR, BPP, ARA to RS or PDH analysis or any other steganalysis attacks, and the OUP status for various PVDS based techniques.

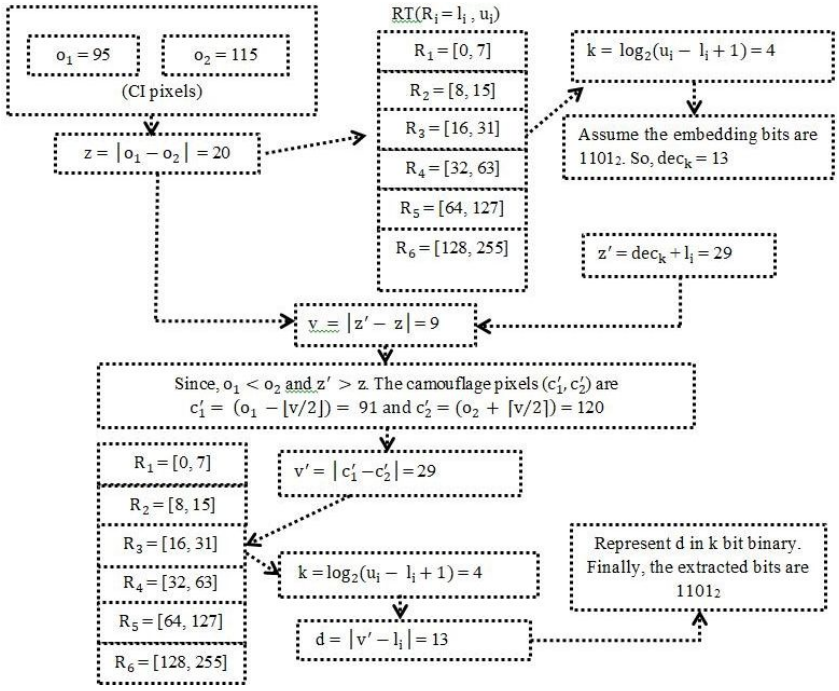

Figure 20: An illustration of Wu and Tsai's [94] PVDS technique

PVDS Embedding Algorithm

Step 1: Let (o_1, o_2) be the two CPs of a block. The FVs for each block is computed using $z = |o_1 - o_2|$. Then, using the FVs, the embedding bits (k) are obtained using Equation (31).

$$k = \log_2(u_i - l_i + 1) \tag{31}$$

where l_i is the lower bound and u_i is upper bound of the range R_i in the range table (RT).

Step 2: Now, obtain the decimal for the k bits, which will be denoted by dec_k. Then, obtain z' using Equation (32).

$$z' = \text{dec}_k + L_n \tag{32}$$

Step 3: Find v as the difference between z and z' as $v = |z' - z|$.

Step 4: Apply Equation (33) to find the camouflage pixels (c'_1, c'_2).

$$(c'_1, c'_2) = \begin{cases} (o_1 + \frac{\lceil v}{2\rceil}, \ o_2 - \frac{\lfloor v}{2\rfloor}), \\ \text{if } o_1 \geq o_2 \text{ and } z' > z \\ \left(o_1 - \frac{\lfloor v}{2\rfloor}, \ o_2 + \frac{\lceil v}{2\rceil}\right), \\ \text{if } o_1 < o_2 \text{ and } z' > z \\ \left(o_1 - \frac{\lceil v}{2\rceil}, \ o_2 + \frac{\lfloor v}{2\rfloor}\right), \\ \text{if } o_1 \geq o_2 \text{ and } z' \leq z \\ \left(o_1 + \frac{\lceil v}{2\rceil}, \ o_2 - \frac{\lfloor v}{2\rfloor}\right), \\ \text{if } o_1 < o_2 \text{ and } z' \leq z \end{cases} \tag{33}$$

PVDS Extraction Algorithm

Step 1: At the receiving end, first obtain the camouflage pixels (c'_1, c'_2) from the block.

Step 2: Then, find the FV using $v' = |c'_1 - c'_2|$. Using this v', from the RT obtain its l_i and u_i. Again, obtain k using the Equation (31).

Step 3: Next, obtain the value d using Equation (34).

$$d = |v' - l_i| \tag{34}$$

Step 4: Finally, represent d in k binary bits. These are the extracted secret bits.

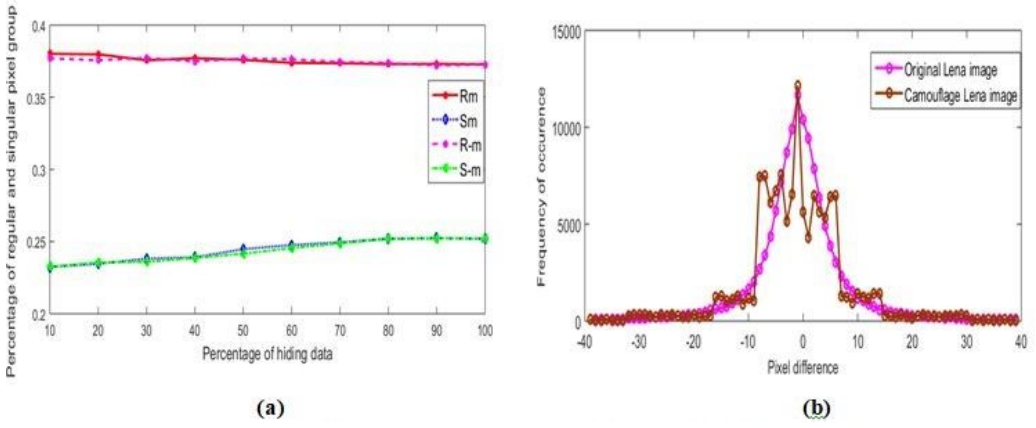

Figure 21: (a) RS-plot and (b) PDH-plot of Lena image for Wu and Tsai's PVDS [94] technique.

→ **Merits of Wu and Tsai's [94] PVDS technique**

- The PVDS technique successfully utilizes the smooth and texture regions of the image adequately for embedding secret bits. Therefore, it resists the RS analysis. Figure 21a shows the RS-plot of the Lena image for the PVDS technique. It can be observed that the condition $R_{-m} - S_{-m} > R_m - S_m$ is satisfied.
- Besides this, Wu and Tsai's PVDS [94] technique has been the stepping stone for almost all of the PVD based steganography techniques that were proposed recently by many researchers.

→ **Issues with Wu and Tsai's [94] PVDS technique**

- One of the biggest issues of Wu and Tsai's [94] PVDS technique is the resistance to PDH analysis. Figure 21b shows the PDH-plot of the Lena image after embedding the secret bits. It can be observed that the histogram for the CI is of a zig-zag nature, *i.e.* it is not smooth, which suggests the CI carries some information.
- Next, most of the PVDS techniques suffer from OUP. To prove this, embedding some random data in the collected images (Figure 23) from [339, 340], Table 6 provides the number of pixels that suffer from OUP in case of the Wu and Tsai's [94] technique, Wu *et al.*'s [117] technique, Khodaei and Faez's [122] technique, and Jung's [125] technique. Since these techniques implement the concept of PVDS, therefore, these techniques are also considered for the evaluation. Further, an illustration of OUP pixel in Wu and Tsai's [94] PVDS technique is shown in Figure 22.

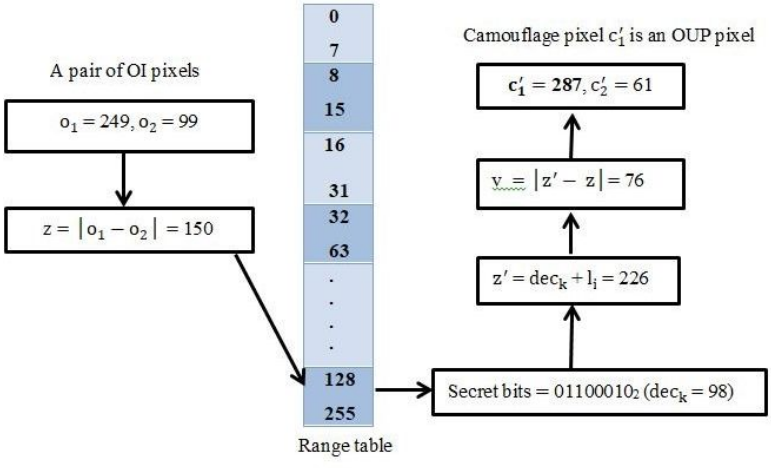

Figure 22: An example of OUP in PVDS [94] embedding process.

Figure 23: 512×512 grayscale images.

Table 6: No. of pixels that suffer from OUP for various PVDS based techniques.

Gray image (512×512)	Wu and Tsai [94]	Wu *et al.* [117]	Khodaei and Faez [122]	Jung [125]
Lena	0	0	0	2
Aerial	259	46	194	329
Barbara	673	746	1	492
Baboon	22	3	11	4566
Baby	472	30	207	1576
Zelda	5	0	5	631
Boat	99	81	4	256
House	0	1	0	0
Houses	3165	1545	2267	3707
Couple	173	74	64	631
Clown	146	140	2	15909
Girlface	4283	172	2065	11383
Peppers	391	228	58	4138
Crowd	980	64	967	1458
Airfield	4001	734	3813	4566
Average	**978**	**258**	**644**	**3310**

Table 7: Analysis of PVDS based techniques.

Ref.	Techniques adopted	Average PSNR (in dB)	BPP	ARA to RS analysis	ARA to PDH analysis	ARA to any other steganalysis	OUP avoided
Wu and Tsai [94]	PVDS technique using the fluctuation between two CPs	40.60	1.60	√	×	–	×
Yang *et al.* [95]	Processes four-pixel blocks at a time for data embedding	38.91	1.62	√	–	–	√
Chang *et al.* [96]	Tri-way PVDS in a block of four pixels using the reference point	40.40	1.02	√	–	–	–
Hussain *et al.* [97]	Parity-bit PVDS (PBPVD) (with RT 1)	40.45	2.07	√	√	–	√
	Parity-bit PVDS (with RT 2)	39.09	2.17	√	√	–	√
	Improved rightmost digit replacement (iRMDR)+PVDS	38.47	3.00	√	√	–	√
Tseng and Leng [98]	PVD+Perfect Square Number	48.25	0.78	–	–	–	–
Swain [99]	Adaptive range selection. Processes+(2*2) pixel blocks by exploring vertical and horizontal edges for embedding	46.65	1.74	√	√	–	√
	Adaptive range selection+(3*3) pixel blocks by exploring vertical and horizontal edges at a time for embedding	50.17	0.29				
Hong *et al.* [100]	PVDS with diamond encoding	44.72	2.34	√	√	–	–
Lee *et al.* [101]	JPEG2000 compression+Tri-way PVDS (TWPVDS)	41.66	1.25	√	–	–	–
Chang *et al.* [102]	Overlapping PVDS using RT 1 of Wu and Tsai	35.87	3.78	–	–	–	–
	Overlapping PVDS using RT 2 of Wu and Tsai	41.06	2.06	–	–	–	–
Luo *et al.* [103]	Adaptive PVDS range selection	49.65	0.40	–	√	LSB matching steganalysis	–
Balasubramanian *et al.* [104]	Octonary PVDS	38.98	3.72	√	√	LSB matching steganalysis	–
Swain [105]	Adaptive RT PVDS	42.97	2.96	√	√	–	√
	Non-adaptive RT PVDS	36.88	3.16				
Hameed *et al.* [106]	Color image and adaptive PVDS by inspecting diagonal, vertical, and horizontal directions in a block	45.49	1.65	–	√	–	–
Marin *et al.* [107]	Optimal-TWPVDS	38.33	2.41	–	–	–	√
	Extra bit optimal-TWPVDS	38.22	2.66	–	–	–	√
Hosam and Halima [108]	Adaptive PVDS with the median as the reference point	32.47	2.93	√	√	–	–
Prasad and Pal [109]	Overlapping PVDS using color images	32.79	2.53	–	√	–	×
Jung and Yoo [110]	Index based PVDS	28.43	2.45	–	√	–	–
Lu *et al.* [111]	3*3 block PVDS	35.45	2.08	–	–	–	√
Liu *et al.* [112]	PVDS+Side match technique	35.17	2.79	×	–	–	–
Marin *et al.* [113]	Optimization strategy+PVDS	38.33	2.41	–	–	–	–
Mandal *et al.* [114]	Adaptive steganography+Modified PVDS	40.67	1.58	–	–	–	√
Kim *et al.* [115]	Multidirection PVDS+Two directions	PSNR 1 = 31.41 PSNR 2 = 33.26	4.64	–	√	–	√
	Multidirection PVDS+Three directions	PSNR 1 = 29.26 PSNR 2 = 31.68	7.03				
Zhang and Wang [116]	Modified PVDS	43.35 47.23	1.55 0.11	√	√	–	√

4.3 LSBS + PVDS [117] technique

Wu *et al.* [117] were the first to combine the LSBS and PVDS together to achieve a larger HC. This technique, at first, partitions the CPs into various blocks. Then the FVs for each block are obtained. The FVs are the absolute difference between the two CPs of the respective blocks. Now using the FVs, each block is identified either as smooth (lower level) or as edge blocks (upper level). LSBS is performed on the block if the FV belongs to the smooth area. On the other hand, Wu and Tsai's [94] embedding strategy is observed for the pixels of edge blocks. An illustration of the embedding and extraction procedure has been displayed in Figure 24. Table 10 presents the results of the average PSNR, BPP, ARA to RS and PDH analysis and any other steganalysis attacks, and the OUP status for various LSBS+PVDS based techniques. Following this, the embedding, as well as the extraction algorithm of Wu *et al.*'s [117] technique, is discussed below. Then, Jung's [125] LSBS+PVDS technique is discussed.

During embedding, execute the following steps to embed the secret bits in a block.

Step 1: Assume the two CPs of a block are o_1 and o_2, and the secret bits are $b_1b_2b_3b_4b_5b_6$.

Step 2: Let z be the FV between o_1 and o_2.

Step 3: Using this z value, identify the smooth or edge area for the SP.

Step 4: If z < 16, then the block is smooth or else in the edge area. Perform Steps 5 and 6, if the block is smooth else perform Wu and Tsai's [94] embedding steps for concealing the secret bits in the edge areas.

Step 5: Let o_1^{bin} and o_2^{bin} be the eight-bit binary representations of o_1 and o_2. Observe 3LSBS in the pixels o_1 and o_2 to obtain o_1' and o_2'.

Step 6: Now obtain z' as the difference between o_1' and o_2'. If $z' > 15$, then, obtain the camouflage pixels using Equation (35).

$$(c_1^*, c_2^*) = \begin{cases} (o_1' - 8,\ o_2' + 8), & \text{if } o_1' \geq o_2' \\ (o_1' + 8,\ o_2' - 8), & \text{if } o_1' < o_2'. \end{cases} \tag{35}$$

Now execute the following steps to extract the secret bits from the c_1^* and c_2^*.

Step 7: At first, find $z^* = |c_1^* - c_2^*|$. If $z^* < 15$, perform 3LSBS extraction from c_1^* and c_2^*. Otherwise, perform Step 8 for extraction of the bits.

Step 8: If $z^* > 15$, observe the extraction steps of Wu and Tsai's [94] PVDS to retrieve the secret bits.

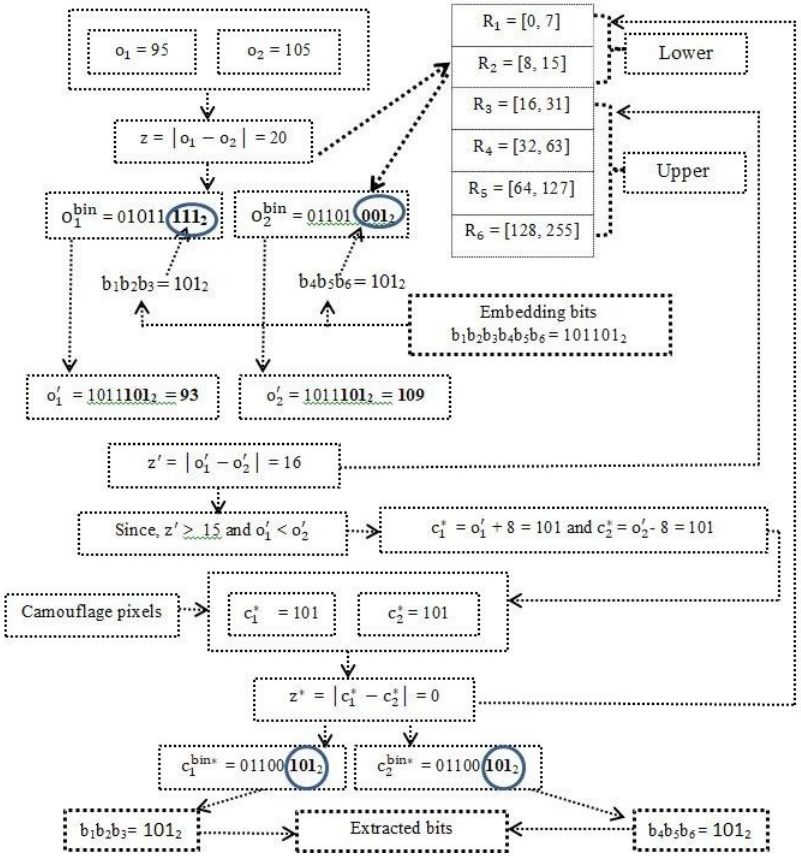

Figure 24: A pictorial illustration of embedding and extraction for Wu *et al.*'s [117] technique.

→ **Issues with Wu *et al.*'s [117] LSBS + PVDS technique**

- Wu *et al.*'s [117] technique performs the embedding using both LSBS and PVDS. However, this technique is more leaning towards the LSBS technique. This is because if we find the FVs for the images, 84.28% (average of 15 images) of the blocks falls under lower level or smooth areas. Therefore, LSBS is applied in those regions. At the same time, PVDS is applied to only 15.72% of the blocks. Table 8 presents the number of blocks that belong to the smooth and edge areas for 15 gray images.
- LSBS is exposed to both RS and PDH analysis; therefore, Wu *et al.*'s [117] technique is also exposed to RS analysis. Figure 25a,b validates the same.

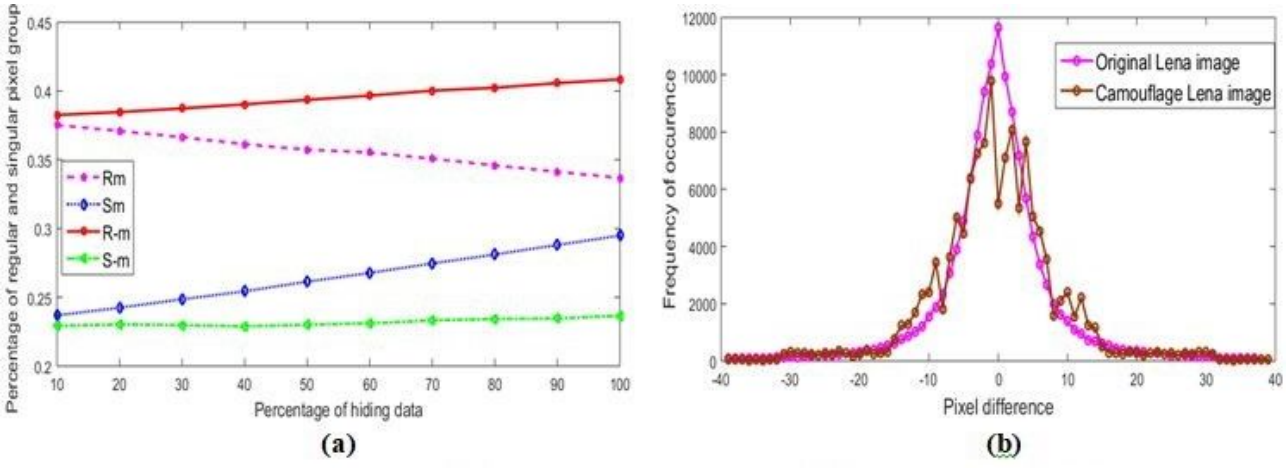

Figure 25: (a) RS-plot and (b) PDH-plot for Wu *et al.*'s [117] technique for the Lena image

Table 8: The number of lower and higher level FVs for 15 images for Wu *et al.*'s [117] technique.

512×512 grayscale image	Lower level {0 to 15}	Upper level {16 to 255}
Lena	118698	12374
Aerial	104438	26634
Barbara	91195	39877
Baboon	86947	44125
Baby	127697	3375
Zelda	125416	5656
Boat	111894	19178
House	116578	14494
Houses	96673	34399
Couple	111201	19871
Clown	111790	19282
Girlface	122537	8535
Peppers	120870	10202
Crowd	121790	9282
Airfield	99266	31806
Average	**111133**	**19939**
Average (%)	**84.28**	**15.72**

Table 9: Range table of Jung's [125] technique.

Range (R_i), (l_i, u_i)	$R_1 = [0, 7]$	$R_2 = [8, 15]$	$R_3 = [16, 31]$	$R_4 = [32, 63]$
Capacity, b	3	3	4	5

4.3.1 Jung's LSBS+PVDS technique [125]

In 2018, Jung [125] proposed a capacity promotive technique by taking advantage of both LSBS and PVDS strategies. The steps of both the embedding and the extraction processes are discussed below.

Step 1: At the embedding end, the image is partitioned into blocks of two OI pixels (o_1, o_2) each. Next, two separate bitplanes are obtained from each block. Let (o_{11}, o_{12}) and (o_{21}, o_{22}) be the two planes that can be found using Equations (36) and (37).

$$(o_{11},\ o_{12}) = o_1\ div\ 2^k, o_2\ div\ 2^k \tag{36}$$

$$(o_{21},\ o_{22}) = o_1\ mod\ 2^k, o_2 mod\ 2^k \tag{37}$$

where the value of k can be 2 or 3. Here the operations div and mod stand for the quotient division and the remainder division, respectively.

Step 2: Find the FV as $v = |o_{11} - o_{12}|$.

Step 3: Now, this v value is mapped to Table 9 to find the lower (l_i) and upper (u_i) bounds for the ith range. Let the corresponding capacity be b. It can be found using, $b = \log_2(u_i - l_i + 1)$.

Step 4: Take b bits of secret data and find the decimal value dec_b. Calculate a new FV as $v' = l_i + dec_b$.

Step 5: Now find $d = |v' - v|$ and calculate (o'_{11}, o'_{12}) for (o_{11}, o_{12}) using Equation (38).

$$(o'_{11}, o'_{12}) = \begin{cases} \left(o_{11} - \frac{d}{2},\ o_{12} + \frac{d}{2}\right), \\ if\ d\ is\ even \\ \left(o_{11} - \frac{d}{2},\ o_{12} + \frac{d}{2}\right), \\ if\ d\ is\ odd \end{cases} \tag{38}$$

Step 6: Take $e_1 = e_2 = e$ bits of secret data and convert to their respective decimal values as dec_{e1} and dec_{e2}.

Step 7: The camouflage-pixel block (c'_1, c'_2) for the original block (o_1, o_2) is computed using Equation (39).

$$(c'_1,\ c'_2) = (o'_{11} \times 2^e + dec_{e1},\ o'_{12} \times 2^e + dec_{e2}) \tag{39}$$

The extraction from the block $(c'_i,\ c'_2)$ is performed using the following steps.

Step 1: At first, obtain (c'_{11}, c'_{12}) from $(c'_1,\ c'_2)$ using Equation (40).

$$(c'_{11}, c'_{12}) = \left(c'_1 - \left(c'_1\ mod\ 2^e\right)\right)\ div 2^e,\quad \left(c'_2 - \left(c'_2\ mod\ 2^e\right)\right)\ div 2^e \tag{40}$$

Step 2: Calculate the value of $v^* = |c'_{11} - c'_{12}|$. Let l_i be the lower bound, and b the capacity of the range of v^*, in Table 9. Now obtain $dec_{dv} = v^* - l_i$ and convert dec_{dv} to b binary bits and append to extracted data. Here, $b = \log_2(u_i - l_i + 1)$.

Step 3: Find o'_{21} and o'_{22} using Equation (41).

$$(o'_{21}, o'_{22}) = (o'_1\ mod\ 2^e, o'_2\ mod\ 2^e) \tag{41}$$

Now, convert o'_{21} to e_1 and o'_{22} to e_2 binary bit and append to the extracted secret bits.

4.3.1.1 Illustration of OUP in Jung's [125] technique

Jung's [125] technique suffers from OUP. Figure 26 shows an illustration of an OUP block in this technique. It is self-explanatory.

→ **Issues of Jung's [125] technique**

- This technique offers excellent HC at a rate of 4.01 BPP. However, the technique is exposed to both RS and PDH analysis.
- Further, OUP is one of the major issues for this technique. Table 6 presents the number of OUP pixels that occur in this technique. From Table 6, it can be observed that an average of 3310 pixels for fifteen images suffers from OUP.

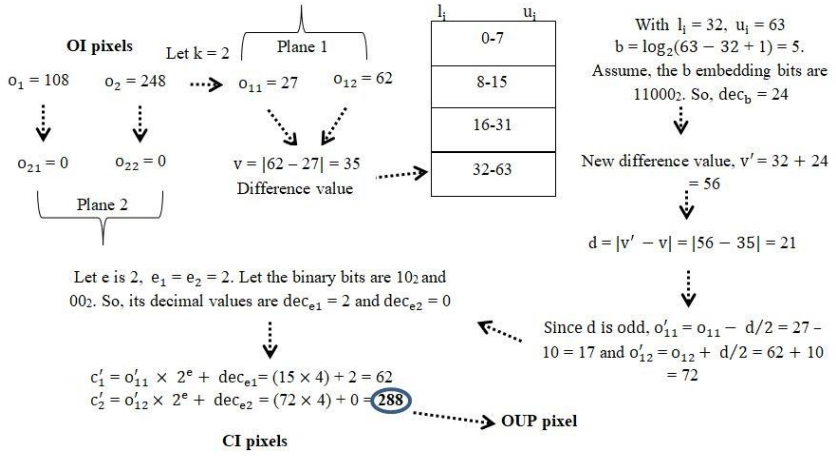

Figure 26: An illustration of OUP in Jung's [125] technique.

Table 10: Analysis of LSBS + PVDS based techniques.

Reference	Techniques adopted		Average PSNR (in dB)	BPP	ARA to RS analysis	ARA to PDH analysis	ARA to other steganalysis	OUP avoided
Wu *et al.* [117]	LSBS+PVDS	2LSBS+PVDS	39.01	2.02	×	×	–	×
		3LSBS+PVDS	35.75	2.91				
Yang *et al.* [118]	Varied LSBS+PVDS		38.96	2.91	√	–	–	√
Gulve and Joshi [119]	2×3 block-based LSBS+PVDS		41.34	2.98	√	–	Histogram analysis	–
Swain [120]	3×3 block based LSBS+PVDS		41.18	1.86	√	–	–	–
Darabkh [121]	Quinary-PVDS-MLSBS+(2×3) block based		40.17	2.73	–	–	–	√
	Octa-PVDS-MLSBS+(3×3)block based		40.07	2.83				
Khodaei and Faez [122]	A block consisting of 3 successive pixels+k-LSBS applied to the central pixel	k = 3 for RT 1	38.04	3.04	√	×	First-order SPAM features	×
		k = 4 for RT 1	36.05	3.37				
		k = 5 for RT 1	32.58	3.7				
		k = 6 for RT 1	31.06	4.08				
		k = 3 for RT 2	37.55	3.14				
		k = 4 for RT 2	35.36	3.47				
		k = 5 for RT 2	32.12	3.86				
		k = 6 for RT 2	30.95	4.42				
Hussain *et al.* [123]	LSBS+PVDS Shift +Modification of prediction Error		38.14	3.11	√	–	–	√
Shukla *et al.* [124]	Compression+encryptio+LSBS+PVDS		36.38	4.00	√	–	–	–
	Encryption + LSBS+PVDS		36.38	3.28				
Jung [125]	2 bit plane LSBS+PVDS		32.61	4.01	×	×	–	×
Khodaei *et al.* [126]	LSBS+PVDS		35.75	2.91	–	–	–	–
Liao *et al.* [127]	Four-pixel differencing and modified LSBS		39.11	3.15	–	–	–	–
Yang *et al.* [128]	Adaptive LSBS+PVDS		32.42	4.10	–	–	–	–
Kalita *et al.* [129]	3×3 block based LSBS+PVDS		38.23	3.49	√	√	–	–
Jung *et al.* [130]	LSB+Multi-pixel differencing		34.00	2.40	–	–	–	–
Gulve and Joshi [131]	2×2 block based LSBS+PVDS		41.58	2.49	√	√	–	√
Sahu and Swain [132]	Adaptive LSBS+PVDS		37.01	3.02	√	√	–	√
Halder *et al.* [133]	LSBS+PVDS+OPAP	3×3 block	33.02	3.26	–	–	–	√
		2×2 block	37.17	3.37				
		1×2 block	35.58	3.60				

Table 11: Analysis of LSBS+PVDS+MF based techniques.

Ref.	Techniques adopted	Average PSNR (in dB)	BPP	ARA to RS analysis	ARA to PDH analysis	OUP avoided
Wang *et al.* [134]	PVDS+MF	43.64	1.57	√	×	√
Joo *et al.* [135]	PVDS+MF+Turnover policy	41.93	1.60	√	×	√
Xu *et al.* [136]	Modulo-three strategy+LSBS	37.42	3.17	–	–	√
Li & He [137]	PVDS+MF+PSO	41.65	2.21	√	–	–
Swain [138]	2×3 block based MFPVD+LSBS	39.29	3.34	√	√	√
Swain [139]	Quotient value differencing (QVD)+(3×3) block	36.39	4.00	√	√	√
	MF+PVD+(2×3) block	43.15	2.64			
Swain [140]	QVD+LSBS	33.06	4.55	√	√	√
Liao *et al.* [141]	Improved PVDS+MF	39.97	2.98	–	–	–
Dhamari and Darabkh [142]	Block-based PVDS+MF	38.28	2.56	–	–	–
Sairam and Boopathybagan [143]	Pixel value adjustment+MF+n^2 ary notational system	32.62	4.00	–	–	–
Shen *et al.* [144]	PVDS+MF+Median concept	37.14	1.50	√	√	√
Lee and Chen [145]	Secret key+MF	51.16	1.00	–	–	√
		44.15	2.00			
		37.93	3.00			
		31.84	4.00			
Maleki *et al.* [146]	Secret key+Adaptive PVDS+MF	47.00	1.68	√	√	√
	Secret key+Non-adaptive PVDS+MF	51.15	1.00	√	√	√
		46.37	2.00			
		40.73	3.00			
		34.81	4.00			
Zhao *et al.* [147]	PVDMF+Intermediate equation	47.90 (WPSNR)	1.60	√	√	√
Nagaraj *et al.* [148]	Pixel value modification+MF	42.54	2.56	–	–	–
Sahu and Swain [149]	PVDS+MF 1	42.04	2.20	√	–	√
	PVDS+MF 2	38.36	3.10			
Sahu and Swain [150]	Overlapped PVDS+MF	36.03	3.15	√	–	√
	Overlapped PVDS	37.01	3.00	–		
Sahu and Swain [151]	PVDS+MF	36.16	3.15	√	–	–
Maniriho and Ahmad [152]	DE+MF	55.17	0.09	√	√	√
Kuo [153]	Modulus data hiding scheme	49.90	1.50	–	–	√
Pan *et al.* [154]	PVDS+MF+(3×3) block based	43.20	2.30	√	√	√
Liao *et al.* [155]	Four-pixel differencing+MF	40.11	2.24	–	–	√
Liao *et al.* [156]	MF+Readjustment algorithm	39.07	2.98	–	–	√

4.4 LSBS+PVDS+MF based steganography

Wang *et al.* [134] were the first who introduced the concept of embedding secret bits by utilizing both PVDS and MF strategy. Here, instead of directly modifying the difference between the two pixels, as was done in the conventional PVDS [94] technique, they modified the remainder of the two CPs. Further, Wang *et al.*'s [134] technique utilized an optimization strategy to avoid the OUP. The results of the investigation suggest that Wang *et al.*'s [134] technique offers imperceptible CI and acceptable BPP. Further, this technique showed good ARA to RS analysis. Joo *et al.* [135] pointed out the weakness of Wang *et al.*'s [134] technique to PDH analysis. They found abnormal fluctuation in the PVD histogram for the CI with the Wang *et al.*'s [134] technique. Further, they addressed this issue by proposing a novel PVD+MF based technique using turnover policy and pixel readjustment process. Xu *et al.* [136] suggested a novel LSB substitution and modulo three strategy technique using the concept of addition and subtraction to embed two ternary numbers in the respective pixels. This technique outperforms conventional LSB substitution techniques. Aimed at optimized CI, Li and He [137] devised a particle swarm optimization based PVDS+MF technique. This technique provides a balanced imperceptible

tibility and HC. Later Swain [138, 139] illustrated the range mismatch issue that occurs in Wang *et al.*'s [134] technique. Also, to address this issue, a novel PVDS+MF+LSBS [138] technique has been suggested. Further, experimentally it has been proved that the proposed technique is secure against both RS and PDH analysis. Further, the OUP has been successfully addressed. A new block-based technique combining MF+PVDS has been proposed by Dhamari and Darabkh [142] to improve the HC and imperceptibility. Sahu and Swain [149] proposed an optimal data hiding technique using PVDS and MF. There are two variants proposed. Both variants utilize the fluctuation between two CPs for embedding the secret bits. Later, using the MF the pixels are modified to improve the quality of the CI. Results show that variant 1 offers good imperceptibility, and variant 2 offers larger HC. Table 11 presents the results of the average PSNR, BPP, ARA to RS and PDH analysis, and OUP status for various LSBS+PVDS+MF based techniques.

4.5 Edge-based steganography

Edge-based steganography utilizes the concept of identifying the edge regions and performing the embedding in those regions. The human visual system can tolerate a significant change to the edge or texture regions. Therefore, embedding the secret bits in the edge regions is more productive. In the literature, authors have suggested various edge detection techniques such as Sobel, Fuzzy, Prewitt, Canny, Laplacian, and Hybrid [157, 178] to locate the edge regions effectively. However, an optimal selection of edge also depends on some other parameters such as Gaussian kernel, gradient descent, and the threshold selection. Sun [157] proposed an improved Canny edge detector (CED) based technique that can observe more edge pixels in an image. Further, using Huffman coding, the HC has been improved significantly. Also, a sorting table has been implemented to randomize the edge pixels to increase the ARA. Recently, an improved Fuzzy edge detection (FED) based technique using LSBM to improve the CI quality has been suggested by Dadgostar and Afsari [160]. To improve the HC, the LSBM based technique that can effectively dis-

Table 12: Analysis of edge based techniques.

Ref.	Techniques adopted	Average PSNR (in dB)	BPP	ARA to RS analysis	ARA to PDH analysis	ARA to any other steganalysis
Sun [156]	CED+Huffman encoding	61.97	0.20	–	–	Histogram analysis
Ioannidou *et al.* [157]	Laplacian or fuzzy edges+Random number generator (RNG)	46.88	1.26	–	–	–
	Laplacian or fuzzy edges+No RNG	45.12	1.89	–	–	–
	Sobel or fuzzy edges+RNG	46.88	1.25	–	–	–
	Sobel or fuzzy edges+No RNG	44.45	1.88	–	–	–
Karakis *et al.* [158]	Similarity-based LSB+No compression	Between 53.95 and 62.50 ± 2.34	1.97	–	–	Histogram analysis
	Fuzzy logic-based LSBS+No compression	Between 53.87 and 62.99 ± 2.43	1.97	–	–	Histogram analysis
Dadgostar and Afsari [159]	FED+Modified LSBS	46.18	2.19	–	–	–
Li *et al.* [160]	Sobel edge detection (SED)	43.97	6.3	–	–	–
Kumar *et al.* [161]	FED	48.59	0.70	–	–	Textural features based universal steganalysis
Lee *et al.* [162]	CED+Hybrid hamming codes	57.59	0.40	–	–	–
Bai *et al.* [163]	LSBS+CED	38.86	2.22	–	–	–
	LSBS+SED	41.90	2.10	–	–	–
	LSBS+FED	33.61	3.59	–	–	–
Tseng *et al.* [164]	HED	33.58	3.16	–	–	–
Hong [177]	Patched reference table+PVDS	52.39	1.00	√	√	Feature-based steganalysis
		46.74	2.00			
		40.92	3.00			
		34.96	4.00			

cover the edge areas has been suggested by Roy *et al.* [166]. Modi *et al.* [167] proposed a CED based technique that can embed 2 bits using LSBM in one of the color components (channel) for the RGB image. Also, the other two color components effectively embed the secret data bits. The major issue with this technique is the low HC. An LSBM based edge detection technique that finds the texture region to conceal more secret bits has been suggested by Luo *et al.* [168]. The horizontal and vertical edges are discovered using the fluctuation or difference between the successive pixels. Bassil *et al.* [169] devised a CED based 3LSBS technique using the color image where the embedding is performed in the RGB components of the image. The experimental result suggests this technique offers better HC compared to other state-of-art edge-based techniques. Islam *et al.* [170] suggested an edge-based technique that dynamically chooses the embedding bits. Since random selection is performed, therefore, this technique ideally avoids various stego-attacks. A combination of the Canny and Fuzzy edge detection techniques known as hybrid edge detection (HED) technique has been suggested by Chan and Chang [171]. Here, the embedding is performed using matrix coding and the Hamming code. Interval-valued intuitionistic fuzzy generators edge detection based techniques have been suggested in [172] to promote the HC without reducing the CI quality. Table 12 analyzes various edge-based techniques based on the average PSNR, BPP, ARA to RS, PDH, and other forms of steganalysis.

4.6 Reversible data hiding (RDH)

Recently, reversible or lossless ISTs have drawn sufficient interest among researchers due to their property of reproducing the original object. The concept of RDH was initiated by Barton [179] during the patent he filled out in 1997. Since then, there has been a rapid increase in the applications that utilize RDH. In many real-time operations, such as medical image processing, military communications, and IoT supported devices retrieving the carrier image along with the embedded information is highly essential. Several papers have been produced on RDH based techniques in recent times [180–228]. However, most of them are classified into either DE, HS or DI based RDH techniques. Tian [180] was the first to introduce the DE based RDH. Here, the FVs between the consecutive pixels are obtained. Then, the FV values are doubled to achieve reversibility. The expanded positions are located using the location map. DE is a basic and fundamental technique, and afterward, many techniques were reported using the DE and location map strategy. Alattar [181] extended the DE based technique to conceal n-1 bits in a vector of n pixels. Ni *et al.* [204] introduced the HS based technique that produces high-quality CI compared to DE based techniques. This technique identifies the zero and peak bins from the histogram for embedding the secret bits. Later, Tsai *et al.* [226] proposed a prediction strategy using the correlation between the neighbor pixels to improve the HC. Recently, authors in [227] devised a multilayer RDH technique to determine the optimal peak and zero bins. This technique reportedly claims to achieve larger HC as compared to its counterparts. Using sub-sampled images and thereby modifying the histogram in [182] the authors have achieved better CI quality with respect to [204] and [206]. Lu *et al.* [201] extended the LSB matching technique [77] to accomplish reversibility using two images to achieve two times more HC than that of [77]. Recently, authors in [192] suggested two improved RDH techniques. The first technique utilizes the modified LSB matching technique to improve the HC, as well as improved the imperceptibility compared to [77] and [201]. Further, the second technique is based on pixel differences. In this, at first four identical images originate from the OI. Then utilizing the n-LSBS technique, the secret bits are embedded. Results show that the second technique achieves better SI-quality for a lower value of n, *i.e.* for n = 1 and 2. At the same time, larger HC is attained for a higher value of n, *i.e.* for n = 3 and 4. Sahu and Swain [193] proposed an improved LSBM based RDH technique to maintain the right balance between the HC and imperceptibility. Once again, authors in [212] suggested a dual layer-based RDH technique using LSBM strategy. This technique offers higher HC as the data is stored in four different images. Table 13 shows the results of various RDH techniques with respect to the considered steganographic parameters.

Table 13: Analysis of RDH based techniques.

Ref.	Techniques adopted	Average PSNR	BPP	ARA to RS analysis	ARA to PDH analysis	ARA to any other steganalysis
Jana [183]	RDH+Weighted matrix	37.97	2.96	√	–	Histogram analysis
Qin *et al.* [184]	RDH+EMD+DI based	PSNR(1) = 52.11 PSNR(2) = 41.34	1.16	–	–	–
Nguyen and Chang [185]	RDH +Sudoku technique	48.00	0.46	–	–	–
Chang *et al.* [186]	RDH+Vector quantization	30.00	2.11	–	–	Histogram analysis
Liu *et al.* [187]	RDH+Logistic chaotic map+Additive homomor-phism+Encrypted image	8.45	1.11	–	–	Histogram analysis
Parah *et al.* [188]	RDH +Intermediate significant Bit substitution	46.51	0.75	–	–	JPEG attack, histogram equalization attack, sharpening attack, low Pass filtering, rotation attack, cropping attack, salt & pepper attack
Kumar *et al.* [189]	RDH+Encryptio+ Location map	49.5	2.68	–	–	–
Hu and Li [190]	RDH+Extended image interpolation	33.03	1.81	–	–	–
Tang *et al.* [191]	RDH+Interpolation	36.70	1.86	–	–	–
Sahu and Swain [192]	RDH+ DI based	PSNR(1) = 51.18 PSNR(2) = 51.17	2.00	√	√	Salt & pepper attack
	n-rightmost bit replacement+Pixel difference, n = 1	PSNR(1) = 54.16 PSNR(2) = 54.16 PSNR(3) = 38.32 PSNR(4) = 37.50	3.03			
	n-rightmost bit replacement+Pixel difference, n = 2	PSNR(1) = 49.28 PSNR(2) = 49.35 PSNR(3) = 38.31 PSNR(4) = 37.48	4.04			
	n-rightmost bit replacement+Pixel difference, n = 3	PSNR(1) = 43.65 PSNR(2) = 43.65 PSNR(3) = 38.29 PSNR(4) = 37.47	5.01			
	n-rightmost bit replacement+Pixel difference, n = 4	PSNR(1) = 37.84 PSNR(2) = 37.71 PSNR(3) = 38.24 PSNR(4) = 37.41	6.03			

Table 13: ... continued

Ref.	Techniques adopted	Average PSNR	BPP	ARA to RS analysis	ARA to PDH analysis	ARA to any other steganalysis
Sahu and Swain [193]	DI based pixel pair LSBM	PSNR(1) = 51.29 PSNR(2) = 51.30	2.00	√	√	–
	DI based modified LSBM	PSNR(1) = 51.19 PSNR(2) = 49.44	2.00	√	√	–
Chang and Lu [194]	RDH+DE	36.34	0.92	–	–	–
Chang *et al.* [195]	RDH+DI based	PSNR(1) = 45.12 PSNR(2) = 45.12	1.00	–	–	–
Wu and Chang [196]	RDH+Side-match prediction+Shortest spanning path	29.74	0.69	–	–	–
Li *et al.* [197]	Pixel value ordering +Quad-tree structure	59.50	0.08	–	√	–
Lin *et al.* [198]	DI based+Turtle shells	PSNR(1) = 49.38 PSNR(2) = 45.55	1.25	–	√	–
Lin *et al.* [199]	DI based+EMD	PSNR(1) = 52.40 PSNR(2) = 49.25	1.07	–	√	–
Xie *et al.* [200]	Turtle shell based+Two-dimensional HS	24.47	0.47	–	–	–
Lu *et al.* [201]	DI based+LSBM	PSNR(1) = 48.98 PSNR(2) = 49.10	2.00	–	–	–
Wang *et al.* [202]	HS+Right-left shift	31.92	1.30	–	–	–
Wang *et al.* [203]	DI based RDH+LSBM	PSNR(1) = 41.00 PSNR(2) = 41.26	2.34	–	–	–
Ni *et al.* [204]	RDH+Pixel value modification	48.20	0.02	–	–	Histogram analysis
Sahu and Swain [205]	RDH+Dual layer LSBM	47.86 48.05 46.51 48.14	6.00	√	√	–

4.7 Other ISTs

Recently, authors in [229–311] have devised various ISTs using strategies like EMD, side match, sudoku, turtle shell, genetic algorithms, interpolation, pixel pair matching, and 3D steganography, to achieve better HC as well as imperceptibility. Chang and Tseng [229] suggested a side match method that finds the correlation between the pixels to measures the smoothness or contrast of the region. Results show that the two-side match strategy offers good capacity, and four-side match method offers better SI quality. This technique is one of the cornerstones for many recent side match based techniques that exist in the literature. The idea of hiding the secret bits guided by a turtle shell was first coined in 2014 by Chang *et al.* [285]. The turtle shells usually have the shape of a hexagon with eight different digits (ranging from 0 to 7). These digits correspond to three bits of secret data each. Then a reference matrix is constructed using the turtle shell that covers every position of the matrix. Later the CI pixels are modified using the reference matrix. Experimental evaluation suggests this technique offers good PSNR compared to other techniques. Some authors have also utilized the logic number based puzzle called sudoku for embedding secret data [306]. Generally, sudoku contains 3×3 sub-blocks containing 1 to 9 digits. Recently, interpolation-based IS techniques were also reported by many authors [235]. Image interpolation techniques usually scale up the image from lower to higher resolution. It is seen that the interpolation-based techniques are more suited for achieving larger HC and reversibility. The EMD based technique represents the secret bits in a (2n+1)-ary notational system for n CI pixels. This technique is based on the idea that for each set of n OI pixels, there are 2n possible modifications. Usually, these techniques observe the maximum modification of ±1 to the OI pixels, and the EMD based techniques achieve imperceptible SI quality. Further, the directions of modifications are fully exploited; therefore, the chances of achieving larger HC is also high [298]. Like 2D images, 3D images can also embed secret data. A 3D image consists of three domains or coordinates, such as geometrical, topological, and representation domains [308]. Here the HC is measured with respect to the embedding bits per vertex of the OI. Since the 3D image constitutes of a number of points, therefore, the computational complexity is also high. Recently, many authors have proposed various ISTs using 3D images. Recently, authors in [343] proposed a counting based secret sharing schema using steganography to further increase the security. In this work, different secret sharing key sizes of 64-bit, 128-bit, and 256-bit are utilized to enhance security. An innovative technique for embedding the secret bits in Arabic text with Unicode Standard seamless is suggested in [344]. The proposed technique not only improves the HC but can also be widely adopted in related languages, such as Urdu and Farsi. Some other improved steganography techniques to promote the capacity and security are suggested in [345–348]. Next, Table 14 shows the results of some noteworthy techniques with respect to the considered measures.

Table 14: Analysis of other steganography techniques.

Ref.	Techniques adopted	Average PSNR (in dB)	BPP	ARA to RS analysis	ARA to PDH analysis	ARA to any other steganalysis
Chang and Tseng [229]	Side match+Pixel Correlation (Two-sided)	37.38	2.00	–	–	–
	Side match+Pixel Correlation (Three-sided)	39.98	1.43			
	Side match+Pixel Correlation (Four-sided)	43.37	0.88			
Chang and Wu [230]	DE based technique+Multiple-layer embedding.	46.36	1.00	–	–	–
		44.14	2.00			
		44.14	3.00			
		44.15	4.00			
Chang *et al.* [231]	Sudoku based	44.88	1.50	–	–	Histogram analysis
He *et al.* [232]	Mini-Sudoku matrix+MF	46.37	2.00	√	√	–
Liu *et al.* [233]	DI based+Secret image sharing+Turtle shell magic matrix	PSNR(1) = 41.94 PSNR(2) = 41.47	2.99	–	–	–
Lin [234]	Pixel difference+Sub image+Pixel vector	52.44	1.05	–	–	–

Table 14: ... continued

Ref.	Techniques adopted	Average PSNR (in dB)	BPP	ARA to RS analysis	ARA to PDH analysis	ARA to any other steganalysis
Jung and Yoo [235]	Neighbor mean interpolation	39.76	1.71	–	–	–
Xu *et al.* [236]	LSBM+Immune programming strategy	54.29 47.30 41.13 34.94	1.00 2.00 3.00 4.00	–	–	HCF COM
Xia *et al.* [237]	3D Sudoku	41.28	2.00	–	–	–
Kuo et al [238]	Multi-bit encoding function	51.01 43.73 37.25	1.25 2.25 3.25	√	–	Bit plane attack
Wazirali *et al.* [239]	GA+LSBS	45:22	2.00	–	–	Histograms analysis
Nguyen et al.[240]	Multi bit-planes block data-hiding	46.09	1.50	–	–	Bit plane analysis
Amirtharajan and Rayappan [241]	Adaptive Random k-bit embedding +Adaptive LSBS	17.57	4.00	–	–	Cryptographic attacks
Younus and Hussain [242]	RDH+Vigenere cipher+Huffman coding+EMD	55.75	1.60	–	–	Chi-square test
Kuo *et al.* [243]	PVDS+EMD	48.20	1.50	–	–	–
Kuo *et al.* [244]	Improved EMD	50.17	1.50	–	–	–
Kuo and Wang [245]	Generalised EMD	50.17	1.50	–	–	–
Kuo and Kao [246]	Fully EMD	52.38 34.82	1.00 4.50	–	–	–
Shen and Huang [247]	Hilbert filling curve+PVDS+any-ary notation	41.97	1.57	√	√	–
Liu *et al.* [248]	Enhanced generalized EMD	43.07	1.52	√	–	–
Kieu and Chang [249]	Exploiting eight modification directions	52.39 46.75 40.83 34.83 31.70	1.00 2.00 3.00 4.00 4.50	–	–	–
Biswas *et al.* [250]	Multi-bit LSBS	38.20	2.42	–	–	ROC, histograms analysis, chi-square analysis, quantative steganalysis, SPA, dual statistical method, stirmark analysis
Verma *et al.* [251]	RGB image based steganography	38.74	4.00	–	–	Modified weighted stego-image steganalysis
Vanmathi and Prabu [252]	FED6+Chaotic method	51.49	0.04	–	–	Histograms analysis
Wu *et al.* [253]	LSBS+EMD+MPE	45. 14	1.49	–	–	–
Yang and Wang [254]	Smart pixel-adjustment policy	43.80	1.98	–	–	Null attack, color quantization, edge sharpening, gaussian noise
Chen [255]	PVDS+Pixel pair matching	47.30	1.66	–	√	Chi-square analysis

Table 14: ... continued

Ref.	Techniques adopted	Average PSNR (in dB)	BPP	ARA to RS analysis	ARA to PDH analysis	ARA to any other steganalysis
Muhammad *et al.* [256]	Magic LSBS+Encryption	44.58	1.50	–	–	–

5 Steganography and steganalysis towards machine learning

With the rapid growth in the field of artificial intelligence, many steganographers move towards ML-based steganography and steganalysis [312]. It is too early to speak about whether a trained model can be really helpful in regards to hiding and recovering information from the digital object accurately. However, recently some researchers proved that it is possible for machines to hide the secret message in a digital image. Until now, the count of such techniques that use ML-based algorithms like CNN, artificial neural network, recurrent neural network, and deep learning are very few. But, these algorithms can be efficiently utilized as the steganalysis tools to analyze the hidden contents from the image [313]. They can capture the convoluted dependencies among the pixels to analyze and identify the presence of secret bits. Therefore, these ML-based steganalysis techniques pose a big challenge to the heuristic or conventional ISTs. The conventional ISTs are well handcrafted, but they are heuristic. It means a certain level of expertise is required to understand where and how exactly to embed the secret bits. Conversely, with minimum effort, deep learning based CNNs can accomplish this. The only thing here is to design the structure of the encoder and decoder. For example, the artificial neural network can effectively identify the optimal embedding location in an image. Therefore, in the near future, it is expected that the fight between steganography and steganalysis is going to be the fight between the neural networks. Further, it is also expected that the trained AI models can perform the embedding and extraction on their own when they are trained with supplying necessary features or inputs. Therefore, this can reduce human intervention for performing the embedding and extraction to a greater extent in the coming future. Therefore, ML-based techniques are promising to pay great attention to achieve a lot of wonders in the steganalysis domain.

Baluja [314] implemented LSBS and matrix coding-based data hiding technique using feed-forward neural networks to achieve enhanced capacity. Here the encoder network can hide an image inside the OI to produce the CI, and the decoder network can produce the complete hidden image from the CI. However, the robustness of the technique has not been verified. In [315], a two-stage authentication based deep steganography and matrix encoding technique has been proposed. Here, the secret message is not directly embedded in the pixels of the OI. Therefore, the distortion in the CI is significantly less than other existing techniques. Primarily, the objective of this schema is to improve identity authentication. An invisible steganography technique associating generative adversarial network and mixed loss function has been suggested in [316]. Here, a secret image is embedded in the original color image of equal size. However, to obtain imperceptible CI, the secret bits are embedded only in the Y channel, which do not carry any color-related features of the image. A U-Net CNN structure-based IST with two different networks such as hidden and extraction networks has been proposed in [317]. Using the hidden network, the sender embeds the secret image in an OI, and the receiver extracts the SI from the CI to obtain the SI. The resulting CI does not exhibit any visual cues to the outsider.

A coverless IST using the generative model has been proposed in [318]. The generative model takes the SI as the input and produces a new image that is independent of SI. Since the generated image has no relation with the SI, this technique does not give any indication of the SI to the intruder. In order to find the optimal embedding location and, therefore, to reduce the CI distortion, the authors in [319] devised a novel extreme learning machine technique. Also, the extreme learning technique has been trained by considering the smooth and texture features of the OI to produce larger HC. A trained neural network model using a generative adversarial network that can embed the secret bits without embedding has been suggested in [320]. Here, the secret bits are mapped to a noise vector and then based on the training data set. The receiver can then extract the secret bits from the CI. Various ML-based ISTs have been suggested by the authors in [321–325]. A CNN model based steganalysis that can learn the complex relationships and the dependency among the pixels has been proposed by Qian *et al.* [326]. The ML and deep learning-based steganal-

ysis techniques can effectively expose conventional ISTs. In this regard, the authors in [327–342] have suggested various steganalysis techniques in the recent literature.

6 Open challenges and future directions

The biggest challenge for a steganographer is to devise a steganography technique that can achieve a fair trade-off between the HC, imperceptibility, and security. Although some of the researchers devised excellent steganography techniques, these techniques are found to be exposed to one or more forms of steganalysis. Practically, there is no such steganography technique available that can achieve the aforementioned properties. Since these properties are mutually exclusive with each other, therefore, concentrating on one property can lead to expose the others. So, this is still an open challenge to researchers. It would be interesting to see how far the war between steganography and steganalysis can go on. After reviewing the literature in IS, the author has made the following recommendations that could be the promising directions in the coming days.

1. Today, the availability of high configuration computational setup is not an issue anymore. Therefore, using the powerful deep convolutional generative adversarial network models with proper training data sets, higher HC and robust ISTs can be produced.
2. Steganography alone cannot achieve authentication. So, the compound of encryption, watermarking, and steganography techniques can be an ideal option to fulfil this objective. Since encryption makes it harder for the opponent to guess, watermarking can even locate the tampered area, and steganography makes the object invisible. Therefore, the author strongly advocates combining them to achieve HC, better imperceptibility, and better security.
3. Another promising direction in this field is 3D IS. By far, most of the works that have been reported in this field use 2D images. Generally, 2D images are objects with two dimensions (breadth and height). By contrast, 3D images have three dimensions (breadth, height and depth). Therefore, the use of 3D images can significantly increase the hiding ratio over 2D images due to its additional dimension. Due to the nature of complexity in 3D images, very few attempts were made by the researchers to embed the secret bits in 3D images. However, these techniques are found to be superior to that of conventional ISTs that uses 2D images. Therefore, the author strongly advocates the use of 3D images for data embedding to improve HC in the future.
4. It is found that adaptive ISTs focus more on the texture regions of the image for embedding more secret bits and neglecting the smoother regions. In this process, the HC is sacrificed. It will be exciting to see how an improved technique can raise the HC without causing any distortion in the non-edge or smooth images.

7 Conclusions

This paper provides an extensive review of various image steganography and steganalysis techniques in the spatial domain. In addition, the taxonomy of image steganography techniques and the performance evaluation metrics are also discussed. Also, the results of various image steganography techniques with respect to the three diametrically opposed steganographic metrics are reported. Further, the existing issues and promising future scopes are also highlighted. Finally, in this era of digitization, steganography and steganalysis both are flourishing at a faster pace. Therefore, the author believes the proposed paper can support many researchers in not only understanding the background details of image steganography but also taking their ideas forward.

Conflict of Interests: The authors declare that there is no competing interest in publishing the articles.

Funding: The authors declare that this work is an independent work and no financial aid has been received for the work either directly or indirectly.

References

[1] Martin A., Sapiro G., Seroussi G., Is image steganography natural?, IEEE Transactions on Image processing, 2005, 14(12), 2040-2050

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

[3] Cheddad A., Condell J., Curran K., Mc-Kevitt P., Digital image steganography: Survey and analysis of current methods, Signal processing, 2010, 90(3), 727-752

[4] Johnson N. F., Jajodia S., Exploring steganography: Seeing the unseen, Computer, 1998, 31(2), 26-34

[5] Hussain M., Wahab A. W. A., Idris Y. I. B., Ho A. T., Jung K. H., Image steganography in spatial domain: A survey, Signal Processing: Image Communication, 2018, 65, 46-66
[6] Atawneh S., Almomani A., Sumari P., Steganography in digital images: Common approaches and tools, IETE Technical Review, 2013, 30(4), 344-358
[7] Nisha C. D., Monoth T., Analysis of Spatial Domain Image Steganography Based on Pixel-Value Differencing Method, In Soft Computing for Problem Solving, Springer, Singapore, 2020, 385-397. https://doi.org/10.1007/978-981-15-0184-5_34
[8] Karampidis K., Kavallieratou E., Papadourakis G., A review of image steganalysis techniques for digital forensics, Journal of information security and applications, 2018, 40, 217-235
[9] Nissar A. Mir A. H., Classification of steganalysis techniques: A study, Digital Signal Processing, 2010, 20(6), 1758-1770
[10] Singh L. Singh A. K. Singh P. K., Secure data hiding techniques: a survey, Multimedia Tools and Applications, 2018, 1-21. https://doi.org/10.1007/s11042-018-6407-5
[11] Subhedar M. S., Mankar V. H., Current status and key issues in image steganography: A survey, Computer science review, 2014, 13, 95-113
[12] Hussain M., Wahab A. W. A., Anuar N. B., Salleh R., Noor R. M., Pixel value differencing steganography techniques: Analysis and open challenge, In IEEE International Conference on Consumer Electronics-Taiwan, 2015, 21-22
[13] Sahu A. K., Swain G., A review on LSB substitution and PVD based image steganography techniques, Indonesian Journal of Electrical Engineering and Computer Science, 2016, 2(3), 712-719
[14] Kharrazi M., Sencar H. T., Memon N. D., Performance study of common image steganography and steganalysis techniques, Journal of Electronic Imaging, 2006, 15(4), 041104
[15] Li B., He, J., Huang J., Shi Y. Q., A survey on image steganography and steganalysis, Journal of Information Hiding and Multimedia Signal Processing, 2011, 2(2), 142-172
[16] Judge J. C., Steganography: past, present, future (No. UCRL-ID-151879), Lawrence Livermore National Lab., CA (US), 2001
[17] Amirtharajan R., Qin J., Rayappan J. B. B., Random image steganography and steganalysis: Present status and future directions, Information Technology Journal, 2012, 11, 566-576
[18] Kahn D., The history of steganography, In International Workshop on Information Hiding, Springer, Berlin, Heidelberg, 1996, 1-5
[19] Mishra M., Mishra P., Adhikary M. C., Digital image data hiding techniques: A comparative study, arXiv preprint arXiv:1408.3564, 2014
[20] Provos N., Honeyman P., Hide and seek: An introduction to steganography, IEEE security & privacy, 2003, 1(3), 32-44
[21] Petitcolas F. A., Anderson R. J., Kuhn M. G., Information hiding-a survey, Proceedings of the IEEE, 1999, 87(7), 1062-1078
[22] Vinodhini R. E., Malathi P., Kumar T. G., A survey on DNA and image steganography, In 4th International Conference on Advanced Computing and Communication Systems (ICACCS), 2017, 1-7
[23] Wang H., Wang S., Cyber warfare: steganography vs. steganalysis, Communications of the ACM, 2004, 47(10), 76-82
[24] Altaay A. A. J., Sahib S. B., Zamani M., An introduction to image steganography techniques, In International Conference on Advanced Computer Science Applications and Technologies (ACSAT), 2012, 122-126
[25] Abraham A., Paprzycki M., Significance of steganography on data security, In International Conference on Information Technology: Coding and Computing, 2004. Proceedings, ITCC 2004, 2004(2), 347-351
[26] Amirtharajan R., Rayappan J. B. B., Steganography-time to time: A review, Research Journal of Information Technology, 2013, 5(2), 53-66
[27] Pradhan A., Sahu A. K., Swain G., Sekhar K. R., Performance evaluation parameters of image steganography techniques, In International Conference on Research Advances in Integrated Navigation Systems (RAINS), 2016, 1-8
[28] Meng R., Cui Q., Yuan C., A survey of image information hiding algorithms based on deep learning, Computer Modeling in Engineering & Sciences, 2018, 117(3), 425-454
[29] Girdhar A., Kumar V., Comprehensive survey of 3D image steganography techniques, IET Image Processing, 2017, 12(1), 1-10
[30] Artz D., Digital steganography: hiding data within data, IEEE Internet computing, 2001, 5(3), 75-80
[31] Trivedi M. C., Sharma S., Yadav V. K., Analysis of several image steganography techniques in spatial domain: A survey, In Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies, 2016, 84
[32] Jung K. H., A survey of reversible data hiding methods in dual images, IETE Technical Review, 2016, 33(4), 441-452
[33] Shi Y. Q., Li X., Zhang X., Wu H. T., Ma, B., Reversible data hiding: advances in the past two decades, IEEE Access, 2016, 4, 3210-3237
[34] Westfeld A., Pfitzmann A., Attacks on steganographic systems, In International workshop on information hiding, Springer, Berlin, Heidelberg, 1999, 61-76
[35] Mousavi S.M., Naghsh A., Manaf A. A., Abu-Bakar S. A. R., A robust medical image watermarking against salt and pepper noise for brain MRI images, Multimedia Tools and Applications, 2017, 76(7), 10313–10342
[36] Wang Z., Bovik A. C., A universal image quality index, IEEE signal processing letters, 2002, 9(3), 81-84
[37] Bagnall R. J., Reversing the steganography myth in terrorist operations: The asymmetrical threat of simple intelligence dissemination techniques using common tools, SANS Information Security Reading Room, 2002, 19
[38] Tirkel A. Z., Rankin G. A., Van-Schyndel R. M., Ho W. J., Mee N. R. A., Osborne, C. F., Electronic watermark, Digital Image Computing, Technology and Applications (DICTA'93), 1993, 666-673
[39] Simmons G. J., The prisoners' problem and the subliminal channel, In Advances in Cryptology, Springer, Boston, MA, 1984, 51-67
[40] Fridrich J., Goljan M., Practical steganalysis of digital images: State of the art, Security and Watermarking of Multimedia Contents IV, International Society for Optics and Photonics, 2002, 4675, 1–14
[41] Zhang T., Ping X., A new approach to reliable detection of LSB steganography in natural images, Signal processing, 2003, 83(10), 2085-2093
[42] Xia Z., Wang X., Sun X., Liu Q., Xiong N., Steganalysis of LSB matching using differences between nonadjacent pixels, Multimedia Tools and Applications, 2016, 75(4), 1947-1962
[43] Zhang J., Xiong F., Zhang D., Steganalysis for LSB Matching Based on the Dependences Between Neighboring Pixels, Journal of multimedia, 2012, 7(5), https://doi.org/10.1002/sec.864
[44] Fridrich J., Goljan M., Du R., Reliable detection of LSB steganography in color and grayscale images, In Proceedings of the work-

shop on Multimedia and security: new challenges, 2001, 27-30
[45] Ker A. D., Steganalysis of LSB matching in grayscale images, IEEE signal processing letters, 2005, 12(6), 441-444
[46] Fridrich J., Goljan M., Du R., Detecting LSB steganography in color, and gray-scale images, IEEE multimedia, 2001, 8(4), 22-28
[47] Ker A. D., Improved detection of LSB steganography in grayscale images, In International workshop on information hiding, Springer, Berlin, Heidelberg, 2004, 97-115
[48] Pevný T., Filler T., Bas P., Using high-dimensional image models to perform highly undetectable steganography, In International Workshop on Information Hiding, Springer, Berlin, Heidelberg, 2010, 161-177
[49] Pevny T., Bas P., Fridrich J., Steganalysis by subtractive pixel adjacency matrix, IEEE Transactions on information Forensics and Security, 2010, 5(2), 215-224
[50] Zhang H., Ping X., Xu M., Wang R., Steganalysis by subtractive pixel adjacency matrix and dimensionality reduction, Science China Information Sciences, 2014, 57(4), 1-7
[51] Kurak C., Mc-Hugh J., A cautionary note on image downgrading, Proceedings Eighth Annual Computer Security Application Conference, 1992, 153-159
[52] Wang R. Z., Lin C. F., Lin J. C., Hiding data in images by optimal moderately-significant-bit replacement, Electronics Letters, 2000, 36(25), 2069-2070
[53] Chan C. K., Cheng L. M., Improved hiding data in images by optimal moderately-significant-bit replacement, Electronics Letters, 2001, 37(16), 1017-1018
[54] Wang R. Z., Lin C. F., Lin J. C., Image hiding by optimal LSB substitution and genetic algorithm, Pattern recognition, 2001, 34(3), 671-683
[55] Chan C. K., Cheng L. M., Hiding data in images by simple LSB substitution, Pattern recognition, 2004, 37(3), 469-474
[56] Chang C. C., Lin M. H., Hu Y. C., A fast and secure image hiding scheme based on LSB substitution, International journal of pattern recognition and artificial intelligence, 2002, 16(04), 399-416
[57] Zakaria A., Hussain M., Wahab A., Idris M., Abdullah N., Jung K. H., High-capacity image steganography with minimum modified bits based on data mapping and LSB substitution, Applied Sciences, 2018, 8(11), 2199
[58] Yang H., Sun X., Sun G., A high-capacity image data hiding scheme using adaptive LSB substitution, Radioengineering, 2009, 18(4), 509-516
[59] Cheng-Hsing Y., Chi-Yao W., Shiuh-Jeng W., Hung-Min S., Adaptive data hiding in edge areas of images with spatial LSB domain systems, IEEE Transactions on Information Forensics and Security, 2008, 3(3), 488-497
[60] Gupta S., Goyal A., Bhushan B., Information hiding using least significant bit steganography and cryptography, International Journal of Modern Education and Computer Science, 2012, 4(6), 27-34
[61] Khan S., Ahmad N., Wahid M., Varying index varying bits substitution algorithm for the implementation of VLSB steganography, Journal of the Chinese Institute of Engineers, 2016, 39(1), 101-109
[62] Wu N. I., Hwang M. S., A novel LSB data hiding scheme with the lowest distortion, The Imaging Science Journal, 2017, 65(6), 371-378
[63] Sahu A. K., Swain G., A novel n-rightmost bit replacement image steganography technique, 3D Research, 2019, 10(1), 2
[64] Hussain M., Abdul W. A., Javed N., Jung K. H., Hybrid data hiding scheme using right-most digit replacement and adaptive least significant bit for digital images, Symmetry, 2016, 8(6), 41
[65] Sahu A. K., Swain G., A novel multi stego-image based data hiding method for gray scale image, Pertanika Journal of Science and Technology, 2019, 29(2), 753-768.
[66] Sahu A. K., Swain G., Babu E. S., Digital image steganography using bit flipping, Cybernetics and Information Technologies, 2018, 18(1), 69-80
[67] Shreelekshmi R., Wilscy M., Madhavan C. V., Undetectable least significant bit replacement steganography, Multimedia Tools and Applications, 2019, 78(8), 10565-10582
[68] Kim C., Shin D., Kim B. G., Yang C. N., Secure medical images based on data hiding using a hybrid scheme with the Hamming code, LSB, and OPAP, Journal of Real-Time Image Processing, 2018, 14(1), 115-126
[69] Zhou R. G., Luo J., Liu X., Zhu C., Wei L., Zhang X., A novel quantum image steganography scheme based on LSB, International Journal of Theoretical Physics, 2018, 57(6), 1848-1863
[70] Sahu A. K., Swain G., Information hiding using group of bits substitution, International Journal on Communications Antenna and Propagation, 2017, 7(2), 162-167
[71] Swain G., Digital image steganography using variable length group of bits substitution, Procedia Computer Science, 2016, 85, 31-38
[72] Jung K. H., Data hiding of digital images based on bit position and parity bit, The Imaging Science Journal, 2012, 60(6), 329-337
[73] Laskar S. A., Hemachandran K., High Capacity data hiding using LSB Steganography and Encryption, International Journal of Database Management Systems, 2012, 4(6), 57
[74] Elmasry W., New LSB-based colour image steganography method to enhance the efficiency in payload capacity, security and integrity check, Sadhana, 2018, 43(5), 68
[75] Chakraborty S., Jalal A. S., Bhatnagar C., LSB based non blind predictive edge adaptive image steganography, Multimedia Tools and Applications, 2017, 76(6), 7973-7987
[76] Sharp T., An implementation of key-based digital signal steganography, In International Workshop on Information Hiding, Springer, Berlin, Heidelberg, 2001, 13-26
[77] Mielikainen J., LSB matching revisited, IEEE signal processing letters, 2006, 13(5), 285-287
[78] Sahu A. K., Swain G., An improved data hiding technique using bit differencing and LSB matching, Internetworking Indonesia Journal, 2018, 10(1), 17-21
[79] Sabeti V., Samavi S., Shirani S., An adaptive LSB matching steganography based on octonary complexity measure, Multimedia tools and applications, 2013, 64(3), 777-793
[80] Juneja M., Sandhu P. S., Designing of robust image steganography technique based on LSB insertion and encryption, In International Conference on Advances in Recent Technologies in Communication and Computing, 2009, 302-305
[81] Swain G., Lenka S. K., A novel steganography technique by mapping words with LSB array, International Journal of Signal and Imaging Systems Engineering, 2015, 8(1-2), 115-122
[82] Swain G., Lenka, S. K., LSB array based image steganography technique by exploring the four least significant bits, In International Conference on Computing and Communication Systems, Springer, Berlin, Heidelberg, 2011, 479-488
[83] Alshayeji M. H., Al-Roomi S. A., Abed S. E., A high-capacity and secure least significant bit embedding approach based on word and letter frequencies, Security and Communication Networks, 2016, 9(18), 5764-5788

[84] Jung K. H., Yoo K. Y., Steganographic method based on interpolation and LSB substitution of digital images, Multimedia Tools and Applications, 2015, 74(6), 2143-2155
[85] Lee Y. K., Chen L. H., High capacity image steganographic model, IEE Proceedings-Vision, Image and Signal Processing, 2000, 147(3), 288-294
[86] Rengarajan A., K., Infant A. K., Rayappan J. B. B., High performance pixel indicator for colour image steganography, Information Technology, 2013, 5(3), 277-290
[87] Laimeche L., Meraoumia A., Bendjenna H., Enhancing LSB embedding schemes using chaotic maps systems, Neural Computing and Applications, 2019, 1-19. https://doi.org/10.1007/s00521-019-04523-z (in press)
[88] Tavares J. R. C., Junior F. M. B., Word-Hunt: A LSB steganography method with low expected number of modifications per pixel, IEEE Latin America Transactions, 2016, 14(2), 1058-1064
[89] Sarreshtedari S., Akhaee M. A., One-third probability embedding: a new±1 histogram compensating image least significant bit steganography scheme, IET image processing, 2013, 8(2), 78-89
[90] Muhammad K., Ahmad J., Rehman N. U., Jan Z., Sajjad M., CISSKA-LSB: color image steganography using stego key-directed adaptive LSB substitution method, Multimedia Tools and Applications, 2017, 76(6), 8597-8626
[91] Wang Z. H., Chang C. C., Li M. C., Optimizing least-significant-bit substitution using cat swarm optimization strategy, Information Sciences, 2012, 192, 98-108.
[92] Qazanfari K., Safabakhsh R., A new steganography method which preserves histogram: Generalization of LSB++, Information Sciences, 2014, 277, 90-101
[93] Parvez M. T., Gutub A. A. A., RGB intensity based variable-bits image steganography, In IEEE Asia-Pacific Services Computing Conference, 2008, 1322-1327
[94] Wu D. C., Tsai W. H., A steganographic method for images by pixel-value differencing. Pattern Recognition Letters, 2003, 24(9-10), 1613-1626
[95] Yang C. H., Weng C. Y., Tso H. K., Wang S. J., A data hiding scheme using the varieties of pixel-value differencing in multimedia images, Journal of Systems and Software, 2011, 84(4), 669-678
[96] Chang K. C., Chang C. P., Huang P. S., Tu T. M., A Novel Image Steganographic Method Using Tri-way Pixel-Value Differencing, Journal of multimedia, 2008, 3(2), 37-44
[97] Hussain M., Wahab A. W. A., Ho A. T., Javed N., Jung K. H., A data hiding scheme using parity-bit pixel value differencing and improved rightmost digit replacement, Signal Processing: Image Communication, 2017, 50, 44-57
[98] Tseng H. W., Leng H. S., A steganographic method based on pixel-value differencing and the perfect square number, Journal of Applied Mathematics, 2013, Article ID 189706, 1-8, https://doi.org/10.1155/2013/189706
[99] Swain G., Adaptive pixel value differencing steganography using both vertical and horizontal edges, Multimedia Tools and Applications, 2016, 75(21), 13541-13556
[100] Hong W., Chen T. S., Luo C. W., Data embedding using pixel value differencing and diamond encoding with multiple-base notational system, Journal of Systems and Software, 2012, 85(5), 1166-1175
[101] Lee Y. P., Lee J. C., Chen W. K., Chang K. C., Su J., Chang C. P., High-payload image hiding with quality recovery using tri-way pixel-value differencing, Information Sciences, 2012, 191, 214-225
[102] Chang C. C., Chuang J. C., Hu, Y. C., Spatial domain image hiding scheme using pixel-values differencing, Fundamenta Informaticae, 2006, 70(3), 171-184
[103] Luo W., Huang F., Huang J., A more secure steganography based on adaptive pixel-value differencing scheme, Multimedia tools and applications, 2011, 52(2-3), 407-430
[104] Balasubramanian C., Selvakumar S., Geetha S., High payload image steganography with reduced distortion using octonary pixel pairing scheme, Multimedia tools and applications, 2014, 73(3), 2223-2245
[105] Swain G., Adaptive and non-adaptive PVD steganography using overlapped pixel blocks, Arabian Journal for Science and Engineering, 2018, 43(12), 7549-7562
[106] Hameed M. A., Aly S., Hassaballah M., An efficient data hiding method based on adaptive directional pixel value differencing (ADPVD), Multimedia Tools and Applications, 2018, 77(12), 14705-14723
[107] Grajeda-Marin I. R., Montes-Venegas H. A., Marcial-Romero J. R., Hernandez-Servin J. A., De-Ita G., An optimization approach to the TWPVD method for digital image steganography, In Mexican Conference on Pattern Recognition, Springer, Cham, 2016, 125-134
[108] Hosam O., Ben Halima N., Adaptive block-based pixel value differencing steganography, Security and Communication Networks, 2016, 9(18), 5036-5050
[109] Prasad S., Pal A. K., An RGB colour image steganography scheme using overlapping block-based pixel-value differencing, Royal Society Open Science, 2017, 4(4), 161066
[110] Jung K. H., Yoo K. Y., High-capacity index based data hiding method, Multimedia Tools and Applications, 2015, 74(6), 2179-2193.
[111] Lu H. C., Chu Y. P., Hwang M. S., New steganographic method of pixel value differencing. Journal of Imaging Science and Technology, 2006, 50(5), 424-426
[112] Liu H. H., Lin Y. C., Lee C. M., A digital data hiding scheme based on pixel-value differencing and side match method, Multimedia Tools and Applications, 2019, 78(9), 12157-12181
[113] Grajeda-Marín I. R., Montes-Venegas H. A., Marcial-Romero J. R., Hernández-Servín J. A., Muñoz-Jiménez V., Luna G. D. I., A New Optimization Strategy for Solving the Fall-Off Boundary Value Problem in Pixel-Value Differencing Steganography, International Journal of Pattern Recognition and Artificial Intelligence, 2018, 32(01), 1860010
[114] Mandal J., Das D., Steganography using adaptive pixel value differencing (APVD) of gray images through exclusion of overflow/underflow, In Second international conference on computer science, engineering and applications (CCSEA), 2012, 93–102
[115] Kim P. H., Yoon E. J., Ryu K. W., Jung K. H., Data-Hiding Scheme Using Multidirectional Pixel-Value Differencing on Colour Images, Security and Communication Networks, 2019, https://doi.org/10.1155/2019/9038650 (in press)
[116] Zhang X., Wang S., Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security, Pattern Recognition Letters, 2004, 25(3), 331-339
[117] Wu H. C., Wu N. I., Tsai C. S., Hwang M. S., Image steganographic scheme based on pixel-value differencing and LSB replacement methods, IEE Proceedings-Vision, Image and Signal Processing, 2005, 152(5), 611-615

[118] Yang C. H., Weng C. Y., Wang S. J., Sun H. M., Varied PVD+ LSB evading detection programs to spatial domain in data embedding systems, Journal of Systems and Software, 2010, 83(10), 1635-1643
[119] Gulve A. K., Joshi M. S., A high capacity secured image steganography method with five pixel pair differencing and LSB substitution, International Journal of Image, Graphics and Signal Processing, 2015, 7(5), 66-74
[120] Swain G., Digital image steganography using nine-pixel differencing and modified LSB substitution, Indian Journal of Science and Technology, 2014, 7(9), 1444-1450
[121] Darabkh K. A., Al-Dhamari A. K., Jafar I. F., A new steganographic algorithm based on multi directional PVD and modified LSB, Information Technology and Control, 2017, 46(1), 16-36
[122] Khodaei M., Faez K., New adaptive steganographic method using least-significant-bit substitution and pixel-value differencing., IET Image processing, 2012, 6(6), 677-686
[123] Hussain M., Wahab A. W. A., Javed N., Jung K. H., Recursive information hiding scheme through LSB, PVD shift, and MPE, IETE Technical Review, 2018, 35(1), 53-63
[124] Shukla A. K., Singh A., Singh B., Kumar A., A secure and high-capacity data-hiding method using compression, encryption and optimized pixel value differencing, IEEE Access, 2018, 6, 51130-51139
[125] Jung K. H., Data hiding scheme improving embedding capacity using mixed PVD and LSB on bit plane, Journal of Real-Time Image Processing, 2018, 14(1), 127-136
[126] Khodaei M., Sadeghi B. B., Faez K., Adaptive data hiding, using pixel-value-differencing and LSB substitution, Cybernetics and Systems, 2016, 47(8), 617-628
[127] Liao X., Wen Q. Y., Zhang J., A steganographic method for digital images with four-pixel differencing and modified LSB substitution, Journal of Visual Communication and Image Representation, 2011, 22(1), 1-8
[128] Yang C. H., Weng C. Y., Wang S. J., Sun H. M., Adaptive data hiding in edge areas of images with spatial LSB domain systems, IEEE Transactions on Information Forensics and Security, 2008, 3(3), 488-497
[129] Kalita M., Tuithung T., Majumder S., An adaptive color image steganography method using adjacent pixel value differencing and LSB substitution technique, Cryptologia, 2019, 1-24, https://doi.org/10.1080/01611194.2019.1579122 (in press)
[130] Jung K. H., Ha K. J., Yoo K. Y., Image data hiding method based on multi-pixel differencing and LSB substitution methods, In International Conference on Convergence and Hybrid Information Technology, 2008, 355-358
[131] Gulve A. K., Joshi M. S., An Image Steganography Method Resistive to fall off Boundary Value Problem with Five Pixel Pair Differencing, Journal of Mathematics and Computer Science, 2015, 5, 240-251
[132] Sahu A. K., Swain G., Data hiding using adaptive LSB and PVD technique resisting PDH and RS analysis, International Journal of Electronic Security and Digital Forensics, 2019, 11(4), 458-476
[133] Halder T., Karforma S., Mandal R., A Block-Based Adaptive Data Hiding Approach Using Pixel Value Difference and LSB Substitution to Secure E-Governance Documents, Journal of Information Processing Systems, 2019, 15(2), 1-8
[134] Wang C. M., Wu N. I., Tsai C. S., Hwang M. S., A high quality steganographic method with pixel-value differencing and modulus function, Journal of Systems and Software, 2008, 81(1), 150-158
[135] Joo J. C., Lee H. Y., Lee H. K., Improved steganographic method preserving pixel-value differencing histogram with modulus function, EURASIP Journal on Advances in Signal Processing, 2010, 2010(1), 249826
[136] Xu W. L., Chang C. C., Chen T. S., Wang L. M., An improved least-significant-bit substitution method using the modulo three strategy, Displays, 2016, 42, 36-42
[137] Li Z., He Y., Steganography with pixel-value differencing and modulus function based on PSO, Journal of information security and applications, 2018, 43, 47-52
[138] Swain G., A data hiding technique by mixing MFPVD and LSB substitution in a pixel, Information Technology and Control, 2018, 47(4), 714-727
[139] Swain G., Two new steganography techniques based on quotient value differencing with addition-subtraction logic and PVD with modulus function, Optik, 2019, 180, 807-823
[140] Swain G., Very high capacity image steganography technique using quotient value differencing and LSB substitution, Arabian Journal for Science and Engineering, 2019, 44(4), 2995-3004
[141] Liao X., Wen Q., Zhang J., Improving the adaptive steganographic methods based on modulus function, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2013, 96(12), 2731-2734
[142] Al-Dhamari A. K., Darabkh K. A., Block-based steganographic algorithm using modulus function and pixel-value differencing, Journal of Software Engineering and Applications, 2017, 10(1), 1-12.
[143] Sairam T. D., Boopathybagan K., An improved high capacity data hiding scheme using pixel value adjustment and modulus operation, Multimedia Tools and Applications, 2019, 1-11, https://doi.org/10.1007/s11042-019-7557-9 (in press)
[144] Shen S., Huang L., Tian Q., A novel data hiding for color images based on pixel value difference and modulus function, Multimedia Tools and Applications, 2015, 74(3), 707-728
[145] Lee C. F., Chen H. L., A novel data hiding scheme based on modulus function, Journal of Systems and Software, 2010, 83(5), 832-843
[146] Maleki N., Jalali M., Jahan M. V., Adaptive and non-adaptive data hiding methods for grayscale images based on modulus function, Egyptian Informatics Journal, 2014, 15(2), 115-127
[147] Zhao W., Jie Z., Xin L., Qiaoyan W., Data embedding based on pixel value differencing and modulus function using indeterminate equation, The Journal of China Universities of Posts and Telecommunications, 2015, 22(1), 95-100
[148] Nagaraj V., Vijayalakshmi V., Zayaraz G., Color image steganography based on pixel value modification method using modulus function, IERI Procedia, 2013, 4, 17-24
[149] Sahu A. K., Swain G., An Optimal Information Hiding Approach Based on Pixel Value Differencing and Modulus Function, Wireless Personal Communications, 2019, 108(1). 159-174
[150] Sahu A. K., Swain G., Pixel overlapping image steganography using PVD and modulus function, 3D Research, 2018, 9(3), 40
[151] Sahu A. K., Swain G., Digital Image Steganography using PVD and Modulo Operation, Internetworking Indonesian Journal, 2019, 10(2), 3-13
[152] Maniriho P., Ahmad T., Information hiding scheme for digital images using difference expansion and modulus function, Journal of King Saud University-Computer and Information Sciences, 2019, 31(3), 335-347

[153] Kuo W. C., Secure Modulus Data Hiding Scheme, KSII Transactions on Internet & Information Systems, 2013, 7(3), 600-612
[154] Pan F., Li J., Yang X., Image steganography method based on PVD and modulus function, In International Conference on Electronics, Communications and Control (ICECC), 2011, 282-284
[155] Liao X., Wen Q. Y., Zhao Z. L., Zhang J., A novel steganographic method with four-pixel differencing and modulus function, Fundamenta Informaticae, 2012, 118(3), 281-289
[156] Liao X., Wen Q., Zhang J., Improving the adaptive steganographic methods based on modulus function, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2013, 96(12), 2731-2734
[157] Sun S., A novel edge based image steganography with 2k correction and Huffman encoding, Information Processing Letters, 2016, 116(2), 93-99
[158] Ioannidou A., Halkidis S. T., Stephanides G., A novel technique for image steganography based on a high payload method and edge detection, Expert systems with applications, 2012, 39(14), 11517-11524
[159] Karakis R., Guler İ., Capraz I., Bilir E., A novel fuzzy logic-based image steganography method to ensure medical data security, Computers in biology and medicine, 2015, 67, 172-183
[160] Dadgostar H., Afsari F., Image steganography based on interval-valued intuitionistic fuzzy edge detection and modified LSB, Journal of information security and applications, 2016, 30, 94-104
[161] Li L., Luo B., Li Q., Fang X., A color Images steganography method by multiple embedding strategy based on Sobel operator, In IEEE International Conference on Multimedia Information Networking and Security, 2009, 2, 118-121
[162] Kumar S., Singh A., Kumar M. Information hiding with adaptive steganography based on novel fuzzy edge identification. Defence Technology, 2019, 15(2), 162-169
[163] Lee C. F., Chang C. C., Xie X., Mao K., Shi R. H., An adaptive high-fidelity steganographic scheme using edge detection and hybrid hamming codes, Displays, 2018, 53, 30-39
[164] Bai J., Chang, C. C., Nguyen T. S., Zhu C., Liu Y., A high payload steganographic algorithm based on edge detection, Displays, 2017, 46, 42-51
[165] Tseng H. W., Leng H. S., High-payload block-based data hiding scheme using hybrid edge detector with minimal distortion, IET Image Processing, 2014, 8(11), 647-654
[166] Roy R., Sarkar A., Changder S., Chaos based edge adaptive image steganography, Procedia Technology, 2013, 10, 138-146
[167] Modi M. R., Islam S., Gupta P., Edge based steganography on colored images, In International Conference on Intelligent Computing, Springer, Berlin, Heidelberg, 2013, 593-600
[168] Luo W., Huang F., Huang J., Edge adaptive image steganography based on LSB matching revisited, IEEE Transactions on Information Forensics and Security, 2010, 5(2), 201-214
[169] Bassil Y., Image steganography based on a parameterized canny edge detection algorithm, arXiv preprint arXiv:1212.6259, 2012
[170] Islam S., Modi M. R., Gupta P., Edge-based image steganography, EURASIP Journal on Information Security, 2014, 2014(1), 8
[171] Chan C. S., Chang C. Y., Hiding data in parity check bit. In Proceedings of the 4th International Conference on Uniquitous Information Management and Communication, 2010, 52
[172] Afsari F., Eslami E., Eslami P., Interval-valued intuitionistic fuzzy generators: Application to edge detection, Journal of Intelligent & Fuzzy Systems, 2014, 27(3), 1309-1324
[173] Al-Dmour H., Al-Ani A., A steganography embedding method based on edge identification and XOR coding, Expert systems with Applications, 2016, 46, 293-306
[174] Chen W. J., Chang C. C., Le T. H. N., High payload steganography mechanism using hybrid edge detector, Expert Systems with applications, 2010, 37(4), 3292-3301
[175] Jung K. H., Yoo K. Y., Data hiding using edge detector for scalable images, Multimedia tools and applications, 2014, 71(3), 1455-1468
[176] Alam S., Ahmad T., Doja M. N., A Novel Edge Based Chaotic Steganography Method Using Neural Network, In Proceedings of the 5th International Conference on Frontiers in Intelligent Computing: Theory and Applications, Springer, Singapore, 2017, 467-475
[177] Islam S., Gupta P., Robust edge based image steganography through pixel intensity adjustment, In IEEE International Conference on High Performance Computing and Communications, (HPCC, CSS, ICESS), 2014, 771-777
[178] Hong W., Adaptive image data hiding in edges using patched reference table and pair-wise embedding technique, Information Sciences, 2013, 221, 473-489
[179] Barton J. M., Method and apparatus for embedding authentication information within digital data, U.S. Patent No. 5,646,997, Washington, DC: U.S. Patent and Trademark Office,1997
[180] Tian J., Reversible data embedding using a difference expansion, IEEE transactions on circuits and systems for video technology, 2003, 13(8), 890-896
[181] Alattar A. M., Reversible watermark using the difference expansion of a generalized integer transform, IEEE transactions on image processing, 2004, 13(8), 1147-1156
[182] Kim H. J., Sachnev V., Shi Y. Q., Nam J., Choo H. G., A novel difference expansion transform for reversible data embedding, IEEE Transactions on Information Forensics and Security, 2008, 3(3), 456-465
[183] Jana B., High payload reversible data hiding scheme using weighted matrix, Optik-International Journal for Light and Electron Optics, 2016, 127(6), 3347-3358
[184] Qin C., Chang C. C., Hsu T. J., Reversible data hiding scheme based on exploiting modification direction with two steganographic images, Multimedia Tools and Applications, 2015, 74(15), 5861-5872
[185] Nguyen T. S., Chang C. C., A reversible data hiding scheme based on the Sudoku technique, Displays, 2015, 39, 109-116
[186] Chang C. C., Nguyen T. S., Lin C. C., Reversible data embedding for indices based on histogram analysis, Journal of Visual Communication and Image Representation, 2014, 25(7), 1704-1716
[187] Liu W. L., Leng H. S., Huang C. K., Chen D. C., A block-based division reversible data hiding method in encrypted images, Symmetry, 2017, 9(12), 308
[188] Parah S. A., Ahad F., Sheikh J. A., Loan N. A., Bhat G. M., A New Reversible and high capacity data hiding technique for E-healthcare applications, Multimedia Tools and Applications, 2017, 76(3), 3943-3975
[189] Kumar R., Chand S., A novel high capacity reversible data hiding scheme based on pixel intensity segmentation, Multimedia Tools and Applications, 2017, 76(1), 979-996
[190] Hu J., Li T., Reversible steganography using extended image interpolation technique, Computers & Electrical Engineering, 2015, 46, 447-455

[191] Tang M., Hu J., Song W., Zeng S., Reversible and adaptive image steganographic method, AEU-International Journal of Electronics and Communications, 2015, 69(12), 1745-1754
[192] Sahu A. K., Swain G., High fidelity based reversible data hiding using modified LSB matching and pixel difference, Journal of King Saud University-Computer and Information Sciences, 2019, https://doi.org/10.1016/j.jksuci.2019.07.004 (in press)
[193] Sahu A. K., Swain G., Dual Stego-imaging based Reversible Data Hiding using Improved LSB Matching, International Journal of Intelligent Engineering and Systems, 2019, 12(5), 2019, 63-73
[194] Chang C. C., Lu T. C., A difference expansion oriented data hiding scheme for restoring the original host images, Journal of Systems and Software, 2006, 79(12), 1754-1766
[195] Chang C. C., Kieu T. D., Chou Y. C., Reversible data hiding scheme using two steganographic images, In TENCON, IEEE Region 10 Conference, 2007, 1-4
[196] Wu M. N., Chang C. C., A novel high capacity reversible information hiding scheme based on side-match prediction and shortest spanning path, Circuits, Systems & Signal Processing, 2008, 27(2), 137-153
[197] Li J. J., Lee C. F., Chang C. C., Lin J. Y., Wu Y. H., Reversible Data Hiding Scheme Based on Quad-Tree and Pixel Value Ordering, IEEE Access, 2019, 7, 142947-142962
[198] Lin J. Y., Liu Y., Chang C. C., A real-time dual-image-based reversible data hiding scheme using turtle shells, Journal of Real-Time Image Processing, 2019, 16(3), 673-684
[199] Lin J. Y., Chen Y., Chang C. C., Hu Y. C., Dual-image-based reversible data hiding scheme with integrity verification using exploiting modification direction, Multimedia Tools and Applications, 2019, 1-18. https://doi.org/10.1007/s11042-019-07783-y (in press)
[200] Xie X. Z., Chang C. C., Lin C. C., Lin J. L., A Turtle Shell based RDH scheme with two-dimensional histogram shifting, Multimedia Tools and Applications, 2019, 1-24. https://doi.org/10.1007/s11042-018-7098-7 (in press)
[201] Lu T. C., Tseng C. Y., Wu J. H., Dual imaging-based reversible hiding technique using LSB matching, Signal Processing, 2015, 108, 77-89
[202] Wang W., Ye J., Wang T., Wang W., A high capacity reversible data hiding scheme based on right-left shift, Signal Processing, 2018, 150, 102-115
[203] Wang Y. L., Shen J. J., Hwang M. S., An Improved Dual Image-based Reversible Hiding Technique Using LSB Matching, International Journal of Network Security, 2017, 19(5), 858-862
[204] Ni Z., Shi Y. Q., Ansari N., Su W., (2006). Reversible data hiding, IEEE Transactions on Circuits and Systems for Video Technology, 2006, 16(3), 354-362
[205] Sahu A.K., Swain, G., Reversible Image Steganography Using Dual-Layer LSB Matching, Sensing and Imaging, 2020, 21:1, https://doi.org/10.1007/s11220-019-0262-y (in press)
[206] Wang Y., Cai Z., He W., A New High Capacity Separable Reversible Data Hiding in Encrypted Images Based on Block Selection and Block-Level Encryption, IEEE Access, 2019, 7, 175671-175680
[207] Tai W. L., Yeh C. M., Chang C. C., Reversible data hiding based on histogram modification of pixel differences, IEEE Transactions on Circuits and Systems for video technology, 2009, 19(6), 906-910
[208] Hsiao J. Y., Chan K. F., Chang J. M., Block-based reversible data embedding, Signal Processing, 2009, 89(4), 556-569
[209] Liu Y., Qu X., Xin G., A ROI-based reversible data hiding scheme in encrypted medical images. Journal of Visual Communication and Image Representation, 2016, 39, 51-57
[210] Yao H., Mao F., Tang Z., Qin C., High-fidelity dual-image reversible data hiding via prediction-error shift, Signal Processing, 2019, 170, 107447. https://doi.org/10.1016/j.sigpro.2019.107447 (in press)
[211] Chang C. C., Lin C. C., Chen Y. H., Reversible data-embedding scheme using differences between original and predicted pixel values, IET information security, 2008, 2(2), 35-46
[212] Wang W., A reversible data hiding algorithm based on bidirectional difference expansion, Multimedia Tools and Applications, 2019, 1-24. DOI:10.1007/s11042-019-08255-z (in press)
[213] Jung K. H., High-capacity reversible data hiding method using block expansion in digital images, Journal of Real-Time Image Processing, 2018, 14(1), 159-170
[214] Lu T. C., Chang C. C., Huang Y. H., High capacity reversible hiding scheme based on interpolation, difference expansion, and histogram shifting, Multimedia tools and applications, 2014, 72(1), 417-435
[215] Duan X., Jia K., Li B., Guo D., Zhang E., Qin C., Reversible image steganography scheme based on a U-Net structure, IEEE Access, 2019, 7, 9314-9323
[216] Hong W., Chen T. S., Shiu C. W., Reversible data hiding for high quality images using modification of prediction errors, Journal of Systems and Software, 2009, 82(11), 1833-1842
[217] Pan Z., Hu S., Ma X., Wang L., Reversible data hiding based on local histogram shifting with multilayer embedding, Journal of Visual Communication and Image Representation, 2015, 31, 64-74
[218] Li X., Zhang W., Gui X., Yang B., A novel reversible data hiding scheme based on two-dimensional difference-histogram modification, IEEE Transactions on Information Forensics and Security, 2013, 8(7), 1091-1100
[219] Di F., Zhang M., Liao X., Liu J., High-fidelity reversible data hiding by Quadtree-based pixel value ordering, Multimedia Tools and Applications, 2019, 78(6), 7125-7141
[220] Liao X., Shu C., Reversible data hiding in encrypted images based on absolute mean difference of multiple neighboring pixels, Journal of Visual Communication and Image Representation, 2015, 28, 21-27
[221] Malik A., Sikka G., Verma H. K., An image interpolation based reversible data hiding scheme using pixel value adjusting feature, Multimedia Tools and Applications, 2017, 76(11), 13025-13046
[222] He W., Xiong G., Weng S., Cai Z., Wang Y., Reversible data hiding using multi-pass pixel-value-ordering and pairwise prediction-error expansion, Information Sciences, 2018, 467, 784-799
[223] He W., Zhou K., Cai J., Wang L., Xiong G., Reversible data hiding using multi-pass pixel value ordering and prediction-error expansion, Journal of Visual Communication and Image Representation, 2017, 49, 351-360
[224] Tsai Y. Y., Tsai D. S., Liu C. L., Reversible data hiding scheme based on neighboring pixel differences, Digital Signal Processing, 2013, 23(3), 919-927
[225] Abbasi R., Xu L., Amin F., Luo B., Efficient Lossless Compression Based Reversible Data Hiding Using Multilayered n-Bit Localization, Security and Communication Networks, 2019, https://doi.org/10.1155/2019/8981240 (in press)

[226] Tsai P., Hu Y. C., Yeh H. L., Reversible image hiding scheme using predictive coding and histogram shifting, Signal Processing, 2009, 89(6), 1129-1143
[227] Wang J., Ni J., Zhang X., Shi Y. Q., Rate and distortion optimization for reversible data hiding using multiple histogram shifting, IEEE Transactions on Cybernetics, 2016, 47(2), 315-326
[228] Xie X. Z., Chang C. C., Lin C. C., A hybrid reversible data hiding for multiple images with high embedding capacity, IEEE Access, 2019, 10.1109/ACCESS.2019.29 61764 (in press)
[229] Chang C. C., Tseng H. W., A steganographic method for digital images using side match, Pattern Recognition Letters, 2004, 25(12), 1431-1437
[230] Chang C. C., Wu W. C., A novel data hiding scheme for keeping high stego-image quality, In 12th IEEE International Multi-Media Modelling Conference, 2006, 1-8
[231] Chang C. C., Chou Y. C., Kieu T. D., An information hiding scheme using Sudoku, In 3^{rd} IEEE international conference on innovative computing information and control, 2008, 17-27
[232] He M., Liu Y., Chang C. C., He M., A Mini-Sudoku Matrix-Based Data Embedding Scheme With High Payload, IEEE Access, 2019, 7, 141414-141425
[233] Liu Y., Chang C. C., Huang P. C., Security protection using two different image shadows with authentication, Mathematical biosciences and engineering, 2019, 16(4), 1914-1932
[234] Lin C. C., An information hiding scheme with minimal image distortion, Computer Standards & Interfaces, 2011, 33(5), 477-484
[235] Jung K. H., Yoo K. Y., Data hiding method using image interpolation, Computer Standards & Interfaces, 2009, 31(2), 465-470
[236] Xu H., Wang J., Kim H. J., Near-optimal solution to pair-wise LSB matching via an immune programming strategy, Information Sciences, 2010, 180(8), 1201-1217
[237] Xia B. B., Wang A. H., Chang C. C., Liu L., An Image Steganography Scheme Using 3D-Sudoku, Journal of Information Hiding and Multimedia Signal Processing, 2016, 7(4), 836-845
[238] Kuo W. C., Kuo S. H., Wang C. C., Wuu L. C., High capacity data hiding scheme based on multi-bit encoding function, Optik-International Journal for Light and Electron Optics, 2016, 127(4), 1762-1769
[239] Wazirali R., Alasmary W., Mahmoud M. M., Alhindi A., An Optimized Steganography Hiding Capacity and Imperceptibly Using Genetic Algorithms,IEEE Access, 2019, 7, 133496-133508
[240] Nguyen T. D., Arch-Int S., Arch-Int N., An adaptive multi bit-plane image steganography using block data-hiding, Multimedia tools and applications, 2016, 75(14), 8319-8345
[241] Amirtharajan R., Rayappan J. B. B., An intelligent chaotic embedding approach to enhance stego-image quality, Information Sciences, 2012, 193, 115-124
[242] Younus Z. S., Hussain M. K., Image steganography using exploiting modification direction for compressed encrypted data, Journal of King Saud University-Computer and Information Sciences, 2019, https://doi.org/10.1016/j.jksuci.2019.04.008 (in press)
[243] Kuo W. C., Li J. J., Wang C. C., Analysis of overflow in data hiding based on extraction function, Journal of Innovative Technology, 2019, 1(2), 21-25
[244] Kuo W. C., Kuo S. H., Huang Y. C., Data hiding schemes based on the formal improved exploiting modification direction method, Applied Mathematics & Information Sciences Letters, 2013, 1(3), 1-8
[245] Kuo W. C., Wang C. C., Data hiding based on generalised exploiting modification direction method, The Imaging Science Journal, 2013, 61(6), 484–490
[246] Kuo W. C., Kao M. C., A steganographic scheme based on formula fully exploiting modification directions, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2013, 96(11), 2235-2243
[247] Shen S.Y., Huang L.H., A data hiding scheme using pixel value differencing and improving exploiting modification directions, Computers & Security, 2015, 48, 131–141
[248] Liu Y., Yang C., Sun Q., Enhance embedding capacity of generalized exploiting modification directions in data hiding, IEEE Access, 2017, 6, 5374-5378
[249] Kieu T. D., Chang C. C., A steganographic scheme by fully exploiting modification directions, Expert systems with Applications, 2011, 38(8), 10648-10657
[250] Biswas R., Mukherjee I., Bandyopadhyay S. K., Image feature based high capacity steganographic algorithm, Multimedia Tools and Applications, 2019, 1-18. https://doi.org/10.1007/s11042-019-7369-y (in press)
[251] Verma V., Muttoo S. K., Singh V. B., Enhanced payload and trade-off for image steganography via a novel pixel digits alteration, Multimedia Tools and Applications, 2019, 1-20. DOI: 10.1007/s11042-019-08283-9
[252] Vanmathi C., Prabu S., Image Steganography Using Fuzzy Logic and Chaotic for Large Payload and High Imperceptibility, International Journal of Fuzzy Systems, 2018, 20(2), 460-473
[253] Wu K. S., Liao W. D., Lin C. N., Chen T. S., A high payload hybrid data hiding scheme with LSB, EMD and MPE, The Imaging Science Journal, 2015, 63(3), 174-181
[254] Yang C. Y., Wang W. F., Block-based colour image steganography using smart pixel-adjustment, In Genetic and Evolutionary Computing, Springer, Cham, 2015, 145-154
[255] Chen J. A PVD-based data hiding method with histogram preserving using pixel pair matching, Signal Processing: Image Communication, 2014, 29(3), 375-384
[256] Muhammad K., Ahmad J., Farman H., Jan Z., A new image steganographic technique using pattern based bits shuffling and magic LSB for grayscale images, 2016, arXiv preprint arXiv:1601.01386
[257] Thanikaiselvan V., Santosh K., Manikanta D., Amirtharajan R., A new steganography algorithm against chi square attack, Research Journal of Information Technology, 2013, 5, 363-372
[258] Bandyopadhyay D., Dasgupta K., Mandal J. K., Dutta P., Ojha V. K., Snášel V., A Framework of Secured and Bio-Inspired Image Steganography Using Chaotic Encryption with Genetic Algorithm Optimization (CEGAO), In Proceedings of the Fifth International Conference on Innovations in Bio-Inspired Computing and Applications IBICA, Springer, Cham, 2014, 271-280
[259] Sajasi S., Moghadam A. M. E., A high quality image steganography scheme based on fuzzy inference system, In 13th Iranian Conference on Fuzzy Systems (IFSC), 2013, 1-6
[260] Das S., Sharma S., Bakshi S., Mukherjee I., A framework for pixel intensity modulation based image steganography, In Progress in Advanced Computing and Intelligent Engineering, Springer, Singapore, 2018, 3-14
[261] Niimi M., Noda H., Kawaguchi E., Eason R. O., High capacity and secure digital steganography to palette-based images, In Proceedings. International Conference on Image Processing, 2002, 2, II-II
[262] Banik B. G., Bandyopadhyay S. K., Image Steganography using BitPlane complexity segmentation and hessenberg QR method,

In Proceedings of the First International Conference on Intelligent Computing and Communication, Springer, Singapore, 2017, 623-633

[263] Paul G., Davidson I., Mukherjee I., Ravi, S. S., Keyless steganography in spatial domain using energetic pixels, In International Conference on Information Systems Security, Springer, Berlin, Heidelberg, 2017, 134-148

[264] Paul G., Davidson I., Mukherjee I., Ravi S. S., Keyless dynamic optimal multi-bit image steganography using energetic pixels, Multimedia Tools and Applications, 2017, 76(5), 7445-7471

[265] Muhammad K., Ahmad J., Rho S., Baik S. W., Image steganography for authenticity of visual contents in social networks, Multimedia Tools and Applications, 2017, 76(18), 18985-19004

[266] Liao X., Qin Z., Ding L., Data embedding in digital images using critical functions, Signal Processing: Image Communication, 2017, 58, 146-156

[267] Yang C. H., Wang S. J., Weng C. Y., Capacity-raising steganography using multi-pixel differencing and pixel-value shifting operations, Fundamenta Informaticae, 2010, 98(2-3), 321-336

[268] Liao X., Guo S., Yin J., Wang H., Li X., Sangaiah, A. K., New cubic reference table based image steganography, Multimedia Tools and Applications, 2018, 77(8), 10033-10050

[269] Liao X., Yu Y., Li B., Li Z., Qin Z., A new payload partition strategy in color image steganography, IEEE Transactions on Circuits and Systems for Video Technology. 2019, 10.1109/TCSVT.2019.2896270 (in press)

[270] Liao X., Yin J., Two Embedding Strategies for Payload Distribution in Multiple Images Steganography, In IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2018, 1982-1986

[271] Liao X., Yin J., Guo S., Li X., Sangaiah A. K., Medical JPEG image steganography based on preserving inter-block dependencies, Computers & Electrical Engineering, 2018, 67, 320-329

[272] Al-Nofaie S. M. A., Gutub A. A. A., Utilizing pseudo-spaces to improve Arabic text steganography for multimedia data communications, Multimedia Tools and Applications, 2019, 1-49. https://doi.org/10.1007/s11042-019-08025-x (in press)

[273] Al-Nofaie S., Gutub A., Al-Ghamdi M., Enhancing Arabic text steganography for personal usage utilizing pseudo-spaces, Journal of King Saud University-Computer and Information Sciences, 2019, https://doi.org/10.1016/j.jksuci.2019.06 (in press)

[274] Gutub A. A. A., Alaseri K. A., Refining Arabic text stego-techniques for shares memorization of counting-based secret sharing, Journal of King Saud University-Computer and Information Sciences, 2019, https://doi.org/10.1016/j.jksuci.2019.06.014 (in press)

[275] Gutub A., Al-Juaid N., Multi-bits stego-system for hiding text in multimedia images based on user security priority, Journal of Computer Hardware Engineering, 2018, 1(2), 1-9

[276] Liu G., Liu W., Dai Y., Lian S., Adaptive steganography based on block complexity and matrix embedding, Multimedia systems, 2014, 20(2), 227-238

[277] Sun H. M., Weng C. Y., Lee C. F., Yang C. H., Anti-forensics with steganographic data embedding in digital images, IEEE Journal on selected areas in Communications, 2011, 29(7), 1392-1403

[278] Kuo W. C., Wang C. C., Hou H. C., Signed digit data hiding scheme, Information Processing Letters, 2016, 116(2), 183-191

[279] Hong W., Chen T. S., A novel data embedding method using adaptive pixel pair matching, IEEE transactions on information forensics and security, 2011, 7(1), 176-184

[280] Muhammad K., Ahmad J., Farman H., Jan Z., Sajjad M., Baik S. W., A Secure Method for Color Image Steganography using Gray-Level Modification and Multi-level Encryption, Transactions on Internet and Information Systems, 2015, 9(5), 1938-1962

[281] Kanan H. R., Nazeri B., A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm, Expert Systems with Applications, 2014, 41(14), 6123-6130

[282] El-Emam N. N., New data-hiding algorithm based on adaptive neural networks with modified particle swarm optimization, Computers & Security, 2015, 55, 21-45

[283] Chakraborty S., Jalal A. S., Bhatnagar C., Secret image sharing using grayscale payload decomposition and irreversible image steganography, Journal of Information Security and Applications, 2013, 18(4), 180-192

[284] Roy, R. Laha, S., Optimization of Stego Image retaining secret information using Genetic Algorithm with 8-connected PSNR, Procedia Computer Science, 2015, 60, 468-477

[285] Chang C. C., Liu Y., Nguyen T. S., A novel turtle shell based scheme for data hiding, In 2014 tenth international conference on intelligent information hiding and multimedia signal processing, 2014, 89-93

[286] Hamzah A. A., Khattab S., Bayomi H., A linguistic steganography framework using Arabic calligraphy, Journal of King Saud University-Computer and Information Sciences, 2019, https://doi.org/10.1016/j.jksuci.2019.04.015 (in press)

[287] Liu X., Lin C. C., Muhammad K., Al-Turjman F., Yuan S. M., Joint Data Hiding and Compression Scheme Based on Modified BTC and Image Inpainting, 2019, IEEE Access, 7, 116027-116037

[288] Muhammad K., Steganography: A Secure way for Transmission in Wireless Sensor Networks, 2015, arXiv preprint arXiv:1511.08865

[289] Muhammad K., Ahmad J., Farman H., Zubair M., A novel image steganographic approach for hiding text in color images using HSI color model, 2015, arXiv preprint arXiv:1503.00388

[290] Pan J. S., Li W., Yang C. S., Yan L. J., Image steganography based on subsampling and compressive sensing, Multimedia Tools and Applications, 2015, 74(21), 9191-9205

[291] Liu Y., Zhao H., Liu S., Feng C., Liu S., A robust and improved visual quality data hiding method for HEVC, IEEE Access, 2018, 6, 53984-53997

[292] Li N., Hu J., Sun R., Wang S., Luo Z., A high-capacity 3d steganography algorithm with adjustable distortion, IEEE Access, 2017, 5, 24457-24466

[293] Luo J., Zhou R. G., Luo G., Li Y., Liu G., Traceable Quantum Steganography Scheme Based on Pixel Value Differencing, Scientific reports, 2019, 9(1), 1-12.

[294] Liao X., Chen G., Yin J., Content-adaptive steganalysis for color images, Security and Communication Networks, 9(18), 2016, 5756-5763

[295] Liao X., Chen G., Li Q., Liu J., Improved WOW adaptive image steganography method, In International Conference on Algorithms and Architectures for Parallel Processing, Springer, Cham, 2015, 695-702

[296] Kaur M., Juneja M., Adaptive Block Based Steganographic Model with Dynamic Block Estimation with Fuzzy Rules, In Innovations in Computer Science and Engineering, Springer, Singapore, 2017, 167-176

[297] Muhammad K., Sajjad M., Mehmood I., Rho S., Baik S. W., A novel magic LSB substitution method (M-LSB-SM) using multi-

level encryption and achromatic component of an image, Multimedia Tools and Applications, 2016, 75(22), 14867-14893
[298] Zhang X., Wang S., Efficient Steganographic Embedding by Exploiting Modification direction, IEE Communications Letter, 2006, 10(11), 781–783
[299] Kaw J. A., Loan N. A., Parah S. A., Muhammad K., Sheikh J. A., Bhat G. M., A reversible and secure patient information hiding system for IoT driven e-health, International Journal of Information Management, 2019, 45, 262-275
[300] Shafi I., Noman M., Gohar M., Ahmad A., Khan M., Din S., Ahmad J., An adaptive hybrid fuzzy-wavelet approach for image steganography using bit reduction and pixel adjustment, Soft Computing, 2018, 22(5), 1555-1567
[301] El-emam N. N., Embedding a large amount of information using high secure neural based steganography algorithm, International Journal of Information and Communication Engineering, 2008, 4(2), 2
[302] Hameed M. A., Hassaballah M., Aly S., Awad A. I., An Adaptive Image Steganography Method Based on Histogram of Oriented Gradient and PVD-LSB Techniques, IEEE Access, 2019, 7, 185189-185204
[303] Liu Y., Chang C. C., Nguyen T. S., High capacity turtle shell-based data hiding, IET Image Processing, 2016, 10(2), 130-137
[304] Liu L., Chang C. C., Wang A., Data hiding based on extended turtle shell matrix construction method, Multimedia Tools and Applications, 2017, 76(10), 12233-12250
[305] Xie X. Z., Lin C. C., Chang C. C., Data hiding based on a two-layer turtle shell matrix, Symmetry, 2018, 10(2), 47
[306] Chang C. C., Chou Y. C., Kieu T. D., An information hiding scheme using Sudoku, In 3rd international conference on innovative computing information and control, 2008, 1-5. 10.1109/ICICIC.2008.149
[307] Kumar M. S., Mamatha E., Reddy C. S., Mukesh V., Reddy R. D., Data hiding with dual based reversible image using sudoku technique, In 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2017, 2166-2172
[308] Alface P. R., Macq B., From 3D mesh data hiding to 3D shape blind and robust watermarking: A survey, In Transactions on data hiding and multimedia security II, Springer, Berlin, Heidelberg, 2007, 91-115
[309] Thiyagarajan P., Natarajan V., Aghila G., Venkatesan V. P., Anitha R., Pattern based 3D image Steganography, 3D Research, 2013, 4(1), 1
[310] Cayre F., Macq B., Data hiding on 3-D triangle meshes, IEEE Transactions on signal Processing, 2003, 51(4), 939-949
[311] Tsai Y. Y., An adaptive steganographic algorithm for 3D polygonal models using vertex decimation. Multimedia Tools and Applications, 2014, 69(3), 859-876
[312] Ghamizi S., Cordy M., Papadakis M., Traon Y. L., Adversarial Embedding: A robust and elusive Steganography and Watermarking technique, 2019, arXiv preprint arXiv:1912.01487
[313] Kim J., Park H., Park J. I., CNN-based image steganalysis using additional data embedding, Multimedia Tools and Applications, 2019, 1-18. https://doi.org/10.1007/s11042-019-08251-3
[314] Baluja S., Hiding images in plain sight: Deep steganography, In Advances in Neural Information Processing Systems, 2017, 2069-2079
[315] Liu, L., Wang A., Chang C. C., Li, Z., A Secret Image Sharing with Deep-steganography and Two-stage Authentication Based on Matrix Encoding, International Journal of Network Security, 2017, 19(3), 327-334
[316] Zhang R., Dong S., Liu J., Invisible steganography via generative adversarial networks, Multimedia Tools and Applications, 2019, 78(7), 8559-8575
[317] Duan X., Jia K., Li B., Guo D., Zhang E., Qin C., Reversible image steganography scheme based on a U-Net structure, IEEE Access, 2019, 7, 9314-9323
[318] Duan X., Song H., Qin C., Khan M. K., Coverless steganography for digital images based on a generative model, Computers, Materials & Continua, 2018, 55(3), 483-493
[319] Atee H. A., Ahmad R., Noor N. M., Rahma A. M. S., Aljeroudi Y. Extreme learning machine based optimal embedding location finder for image steganography, PloS one, 2017, 12(2), e0170329
[320] Hu D., Wang L., Jiang W., Zheng S., Li B., A novel image steganography method via deep convolutional generative adversarial networks, IEEE Access, 2018, 6, 38303-38314
[321] Wu P., Yang Y., Li X., Stegnet: Mega image steganography capacity with deep convolutional network, Future Internet, 2018, 10(6), 54
[322] Li C., Jiang Y., Cheslyar M., Embedding image through generated intermediate medium using deep convolutional generative adversarial network, Computers, Materials & Continua, 2018, 56(2), 313-324
[323] Husien S., Badi H., Artificial neural network for steganography, Neural Computing and Applications, 2015, 26(1), 111-116
[324] Ghaleb Al-Jbara H. A., Mat-Kiah L. B., Jalab H. A., Increased capacity of image based steganography using artificial neural network, In AIP Conference Proceedings, 2012, 1482(1), 20-25
[325] Zhu J., Kaplan R., Johnson J., Fei-Fei L., Hidden: Hiding data with deep networks, In Proceedings of the European Conference on Computer Vision (ECCV), 2018, 657-672
[326] Qian Y., Dong J., Wang W., Tan T., Deep learning for steganalysis via convolutional neural networks, In Media Watermarking, Security, and Forensics. International Society for Optics and Photonics, 2015, 9409, 94090J
[327] Fridrich J., Kodovsky J., Rich models for steganalysis of digital images, IEEE Transactions on Information Forensics and Security, 2012, 7(3), 868-882
[328] Ye J., Ni J., Yi Y., Deep learning hierarchical representations for image steganalysis, IEEE Transactions on Information Forensics and Security, 2017, 12(11), 2545-2557
[329] Hayes J., Danezis G., Generating steganographic images via adversarial training, In Advances in Neural Information Processing Systems, 2017, 1954-1963
[330] Sharma K., Aggarwal A., Singhania T., Gupta D., Khanna A., Hiding Data in Images Using Cryptography and Deep Neural Network, 2019, arXiv preprint arXiv:1912.10413
[331] Kim D. H., Lee H. Y., Deep Learning-Based Steganalysis Against Spatial Domain Steganography, In European Conference on Electrical Engineering and Computer Science (EECS), 2017, 1-4
[332] Ye J., Ni J., Yi Y., Deep learning hierarchical representations for image steganalysis, IEEE Transactions on Information Forensics and Security, 2017, 12(11), 2545-2557
[333] Ge S., Gao Y., Wang R., Least significant bit steganography detection with machine learning techniques, In Proceedings of the international workshop on Domain driven data mining, 2007, 24-32. https://doi.org/10.1145/1288552.1288556
[334] Berg G., Davidson I., Duan M. Y., Paul, G., Searching for Hidden Messages: Automatic Detection of Steganography, In IAAI, 2003, 51-56

[335] Wu S., Zhong S. H., Liu Y., Steganalysis via deep residual network, In IEEE 22nd International Conference on Parallel and Distributed Systems (ICPADS), 2016, 1233-1236

[336] Wu S., Zhong S., Liu Y., Deep residual learning for image steganalysis, Multimedia tools and applications, 2018, 77(9), 10437-10453

[337] Zhang Y., Zhang W., Chen K., Liu J., Liu Y., Yu N., Adversarial examples against deep neural network based steganalysis, In Proceedings of the 6th ACM Workshop on Information Hiding and Multimedia Security, 2018, 67-72

[338] Kang S., Park H., Park J. I., CNN-Based Ternary Classification for Image Steganalysis, Electronics, 2019, 8(11), 122

[339] USC-SIPI Image Database. [Online]. Available: http://sipi.usc.edu/database/database.php?volume=misc

[340] http://homepages.inf.ed.ac.uk/rbf/CVonline/Imagedbase.htm

[341] Pevny T., Bas P., Fridrich J., Steganalysis by subtractive pixel adjacency matrix, IEEE Transactions on information Forensics and Security, 2010, 5(2), 215-224

[342] Fridrich J., Kodovsky J., Rich models for steganalysis of digital images, IEEE Transactions on Information Forensics and Security, 2012, 7(3), 868-882

[343] Gutub A., Al-Ghamdi M., Hiding shares by multimedia image steganography for optimized counting-based secret sharing, Multimedia Tools and Applications, 2020, 1-35. DOI: 10.1007/s11042-019-08427-x (in press)

[344] Alanazi N., Khan E., Gutub A., Inclusion of Unicode Standard Seamless Characters to Expand Arabic Text Steganography for Secure Individual Uses, Journal of King Saud University-Computer and Information Sciences. 2020, https://doi.org/10.1016/j.jksuci.2020.04.011 (in press)

[345] Gutub A., Al-Juaid N., Khan E., Counting-based secret sharing technique for multimedia applications, Multimedia Tools and Applications, 2019, 78(5), 5591-5619

[346] Gutub A., Al-Shaarani F., Efficient Implementation of Multi-image Secret Hiding Based on LSB and DWT Steganography Comparisons, Arabian Journal for Science and Engineering, 2020, 1-14. https://doi.org/10.1007/s13369-020-04413-w (in press)

[347] Al-Khodaidi T., Gutub A., Trustworthy Target Key Alteration Helping Counting-Based Secret Sharing Applicability, Arabian Journal for Science and Engineering, 2020, https://doi.org/10.1007/s13369-020-04422-9 (in press)

[348] Al-Juaid N., Gutub A., Combining RSA and audio steganography on personal computers for enhancing security, SN Applied Sciences, 2019, 1(8), 830-841