Image steganography in spatial domain: A survey

Article · March 2018

DOI: 10.1016/j.image.2018.03.012

5 authors, including:

Mehdi Hussain
National University of Sciences and Technology
32 PUBLICATIONS **714** CITATIONS
SEE PROFILE

Ainuddin Wahid
University of Malaya
112 PUBLICATIONS **2,688** CITATIONS
SEE PROFILE

Anthony T. S. Ho
University of Surrey
204 PUBLICATIONS **2,302** CITATIONS
SEE PROFILE

Ki-Hyun Jung
Kyungil University
89 PUBLICATIONS **1,349** CITATIONS
SEE PROFILE

Image Steganography in Spatial Domain: A Survey

Mehdi Hussain[a,b*], Ainuddin Wahid Abdul Wahab[a], Yamani Idna Bin Idris[a], Anthony T. S. Ho[c,d,e], Ki-Hyun Jung [f,*]

[a] *Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur, Malaysia*
[b] *School of Electrical Engineering and Computer Science, National University of Sciences and Technology, Islamabad, Pakistan*
[c] *Department of Computer Science, University of Surrey, Guildford, Surrey, UK*
[d] *Tianjin University of Science and Technology, Tianjin, China*
[e] *China Wuhan University of Technology, Wuhan, China*
[f] *Department of Cyber Security, Kyungil University, Republic of Korea*
[*] *Corresponding authors: mehdi.hussain@seecs.edu.pk, khanny.jung@gmail.com*

ARTICLE INFO

Article history

Keywords:
Image Steganography
Spatial Domain Steganography
Adaptive Steganography
Data Hiding
Security
Digital Spatial Domain

ABSTRACT

This paper presents a literature review of image steganography techniques in the spatial domain for last 5 years. The research community has already done lots of noteworthy research in image steganography. Even though it is interesting to highlight that the existing embedding techniques may not be perfect, the objective of this paper is to provide a comprehensive survey and to highlight the pros and cons of existing up-to-date techniques for researchers that are involved in the designing of image steganographic system. In this article, the general structure of the steganographic system and classifications of image steganographic techniques with its properties in spatial domain are exploited. Furthermore, different performance matrices and steganalysis detection attacks are also discussed. The paper concludes with recommendations and good practices drawn from the reviewed techniques.

1. Introduction

Internet revolution provides the easiness in digital communication; meanwhile, it also becomes a challenge for securing the information over the open network. In order to address the security of information, numerous approaches have been proposed in the field of security systems under information encryption and information hiding as depicted in Fig. 1. Information encryption known as cryptography scrambles the secret message in such a way that it becomes an unintelligent message to eavesdroppers. However, this is always incapable of being encrypted the secret message, it draws attention. Therefore, it is required an invisible communication without noticing to anyone the communication will happen in some cases. This is the reason why information hiding mechanism is needed. Information hiding consists of two subdisciplines, i.e. steganography and watermarking [1]. Both steganography and watermarking are used to hide the secret message and are closely related to each other, but both lies on different objectives. The main concern of steganography is to conceal the existence of communication and protection of secret data. In contrast, watermarking is to protect the integrity of secret data with or without concealing the existence of communication from eavesdroppers. The main purpose of watermarking applications is to protect the intellectual property of the contents. However, Table 1 (an extension of Cheddad et al.) shows basic characteristic between information encryption and information hiding systems.

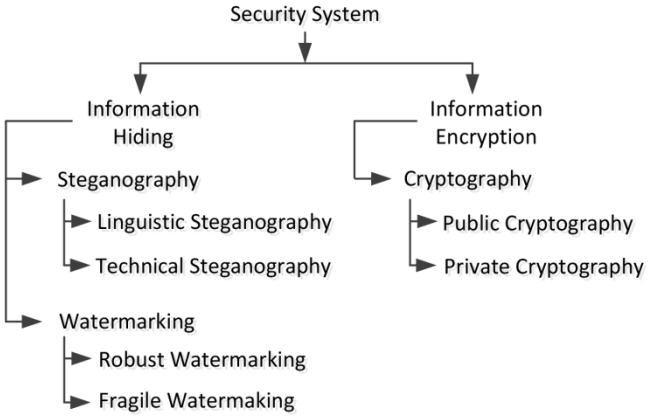

Fig. 1 Basic security system branches (based on Cheddad et al.)

Researchers have shown a great interest in image steganography for last decade. It becomes the most widespread research area due to easy of multimedia content

communication through different low-cost devices (i.e. smart mobiles, IP cameras) and social media applications (i.e. WhatsApp, Facebook). As a result, a user can easily embed/conceal secret information through different steganographic applications.

Usually, image steganography can be categorized into different (spatial and transform) embedding domains detailed in Section 2. We found that most of the surveys are dedicated to general image steganography [2-5]. Moreover, there is a lack of specific domain based comprehensive survey to give exact direction from up to date literature for future researchers in image steganography/steganalysis domain.

The most popular survey available on image steganographic methods was published 6 years ago [2]. In reference to the survey of [2]:

- In Cheddad et al.'s work, the latest cited paper was published in 2009, which means their survey is now 7 years old. Furthermore, more than ~60% of cited papers were before 2007 and 10 years old from now. Therefore, an up-to-date survey was deemed necessary.
- Cheddad et al.'s paper is targeted to current digital image steganographic methods who discussed in Section 1.2 (Ancient steganography), Section 1.3 (The digital era of steganography).
- This paper is totally dedicated to latest image steganographic methods for researchers especially in spatial domain unlike in Cheddad et al. who mentioned very limited in section 3.2 (Steganography in the image spatial domain).
- The classifications in Cheddad et al. paper are limited, i.e. spatial, transform, and adaptive based techniques. This paper proposes different classifications which are based on embedding domain, secret message type, and the image coded format.
- This paper's recommendation can distinguish this initiative from that of Cheddad et al.

Recently, Subhedar et al. [3] survey also focuses on general image steganography. They discussed the fundamental concept, performance evaluation measures and security aspects of the steganographic system, both spatial and transform domains. In reference to the survey of [3]:

- The proposed paper is focused on spatial domain steganography while Subhedar et al.'s work was more emphasized on transform domain steganography.
- In Subhedar et al.'s work published in 2014, very limited spatial domain papers were reviewed and their latest spatial domain cited paper was published in 2013. Therefore, a spatial domain comprehensive and an up-to-date survey is required.
- The image steganographic classifications in Subhedar et al. are also limited like as Cheddad et al., i.e. spatial, transform, model-based approaches.
- The proposed paper's recommendation is more comprehensive and distinctive against Subhedar et al.'s.

Table 1
Comparison between information encryption and information hiding

		Information Encryption	Information Hiding	
		Cryptography	Watermarking	Steganography
Objective		Protection of content	Protect the carrier copyrights	Conceal the existence of communication and secret data
Characteristics	Perceptual Security	No, easy to identify (Visible)	Depends on application (Invisible/Visible)	Hard to identify (Invisible)
	Security of Communication	Depends on confidentiality of Key	Depends on confidentially of embedding technique	Depends on confidentially of embedding technique
	Robustness	Against complexity of ciphering algorithm	Against tampering or removing secret information	Against detection of existence of secret information
	Key requirement	Mandatory	Optional	Application dependent
	Output type	Cipher text/ plain text	Medium dependent Image/Text/Video	Medium dependent Image/Text/Video
	Lifetime of security	Until decryption of cipher text	Until loss of watermark integrity	Until secret information existence exposed
	Medium/Carrier	Digitally represented data	Digital files-text, image, video	Digitally represented data
	Detection and Extraction complexity	Detection easy and complex extraction	Both complex	Both complex
Challenges		Key management, Complexity of encryption algorithm	Robustness	Embedding capacity High Imperceptibility, Robustness

The aim of this paper is to provide up to date spatial domain image steganographic review. Furthermore, we also discuss the existing spatial domain based adaptive embedding approaches and their comparisons in term of strengths and limitations. Also, it is discussed different performance measures matrices and steganographic counterpart as steganalysis attacks. Finally, the proposed recommendations and good practices extracted from the reviewed techniques

will aid researchers to design advanced spatial domain embedding techniques.

The organization of the paper is as follows: Section 2 comprises the general steganography, image steganographic model, and its classifications. The recent literature on the spatial domain is described in Section 3. Section 4 discusses the performance measures methods and Section 5 analyzes the most employed steganalysis methods in the literature. Finally, the recommendations and conclusion are in Section 6.

2. Steganography: A brief review

Steganography is the art and science of using the digital communication object in such a way that it conceals the existence of secret information [6]. The communication object can be any medium/carrier (Fig. 2), device (i.e. smartphone, switch) or service (i.e. browser, Facebook) that utilized for secret communication [7].

Generally, communication mediums/carriers are digital files or data i.e. image, video, text, audio, network protocol and DNA (Fig. 2). Different digital mediums utilize their various characteristics to embed secret information. For example, text steganography uses the line/word shifting encoding [8] and recently utilized emoticons in textual chat to achieve secret communication [9]. In audio steganography, it is generally employed the phase coding, spread spectrum and low-bit encoding for embedding secret information [10]. Secret information can also be embedded into packet payload, packet headers in another medium as network protocol [11], and even utilize the behavior of acknowledgment and retransmission of packets known as retransmission steganography [12]. In DNA-based steganography, the characteristics of randomness in DNA can be employed to embed the secret data, i.e. recently a technique use the numerical mapping table to map the DNA sequence for encoding secret data [13]. In video steganography, the combination of image and audio steganography is often used. It also has more depth to entertain more secret data embedding due to a different combination of images considering the video stream [14]. However, according to [15], the best medium for embedding secret message must possess two features; the medium should be popular and the modification in the cover medium should not be visible to the third party. To the best of our knowledge, in the literature of digital steganography, the image is the most popular medium due to having a high frequency of redundant data and able to conceal the secret data inside together with invisible effects. It is also the focus of this survey.

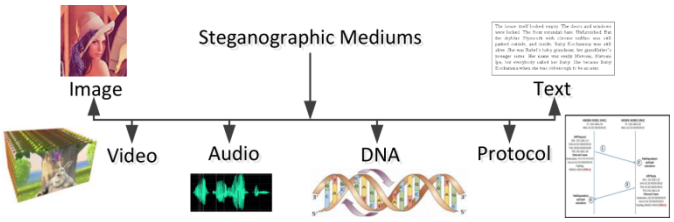

Fig. 2 Steganographic mediums

2.1 Image steganography

In image steganography, the carrier that contains/conceals the secret information is an image. The basic image steganography diagram is shown in Fig. 3. In Fig. 3, the term "cover image" denotes the image which is used to hide the secret data as a payload or "secret message". The "embedding technique" is actually the procedure or algorithm that is used to hide the "secret message" inside the "cover image" namely "stego-image" with optional "stego-key". The optional "stego-key" must be shared with both ends. The "stego-image" denotes the final output image that conceals the secret information. Similarly, the counterpart of embedding can extract the secret information, where "extraction technique" is the process to recover the "secret message" from "stego-image" with optional "stego-key". Furthermore, the counterpart of steganography is "steganalysis" or an attack on steganography. In other words, steganalysis is an art and science of detecting the existence or recovering the secret message from stego images (section 5).

In general, an image steganographic method is evaluated by following key objectives: First, embedding capacity, how maximum the embedding payload can be achieved? Second, visual image quality, how much the stego-image is perceptually identical to its cover image? Third, security, how can a stego-image resist the different steganalysis detection attacks? Therefore, the ideal steganographic method must fulfill the above objectives simultaneously as high capacity, good visual image quality, and undetectability. But most often, high payload steganographic approaches introduce the distortion artifacts in stego-images and that are vulnerable to steganalysis. Moreover, steganographic methods having good visual image quality suffer from the low payload. Therefore, how to achieve simultaneously high payload, good visual quality, and undetectability is a challenging research issue due to the contradictions between them.

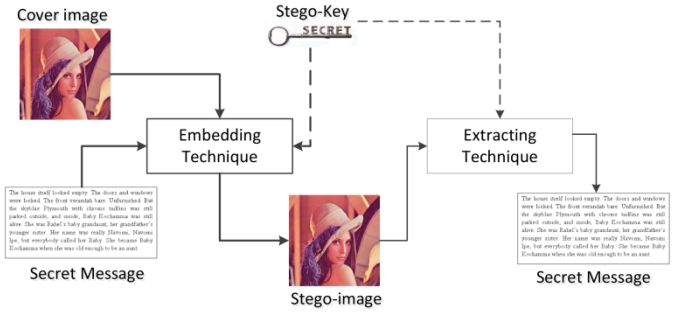

Fig. 3 Images steganographic diagram

In literature, various types of image steganographic methods have been proposed and most of all use a distinct approach to achieve secret data embedding. If we classify them according to model/approach based technique that can be further divided into different types depending on their implementation. Even though it is impossible to classify exactly all of them, we divide them into different categories as shown in Fig. 4. One way is to divide them according to embedding domain, i.e. spatial domain and transform domain adopted by [6]. Furthermore, the adaptive (statistical aware) embedding method can become under the above division

because it can be employed in both spatial and transform domains. Fig. 4(a) shows the classification with their general objectives or goals. Another classification can be based on distinctive steganographic techniques that are specially designed to target coded formats of images, i.e. raw (BMP), compressed (JPEG2000) and encrypted image data (AES-advanced encryption standard) as depicted in Fig. 4 (b). In literature, some of the steganographic techniques are dedicatedly designed with respect to the format/type of secret data (i.e. text, compressed, secret image) to improve the different steganographic objectives. For this Fig. (c), the classification of steganographic techniques based on secret data formats/types is depicted.

From Fig. 4(a), spatial domain directly exploits the cover image data/pixels to conceal the secret information, e.g. substitution of secret bits inside pixel value (detailed in Section 3). In contrast transform domain, the data of the cover image is first converted into other signal/form before applying the embedding process. For example, discrete cosine transformation (DCT) is applied to cover pixels and then the secret data can be embedded into the different coefficient of DCT blocks. Furthermore, the adaptive embedding scheme in Fig. 4 (a) is known as model base or statistical aware information hiding techniques. It is basically interlinked to spatial and transform domain. This type of embedding methods takes the statistical features of the image before embedding the secret information into spatial or transform domain. These statistical features actually dictate where modification takes place in the image for the steganographic purpose [16].

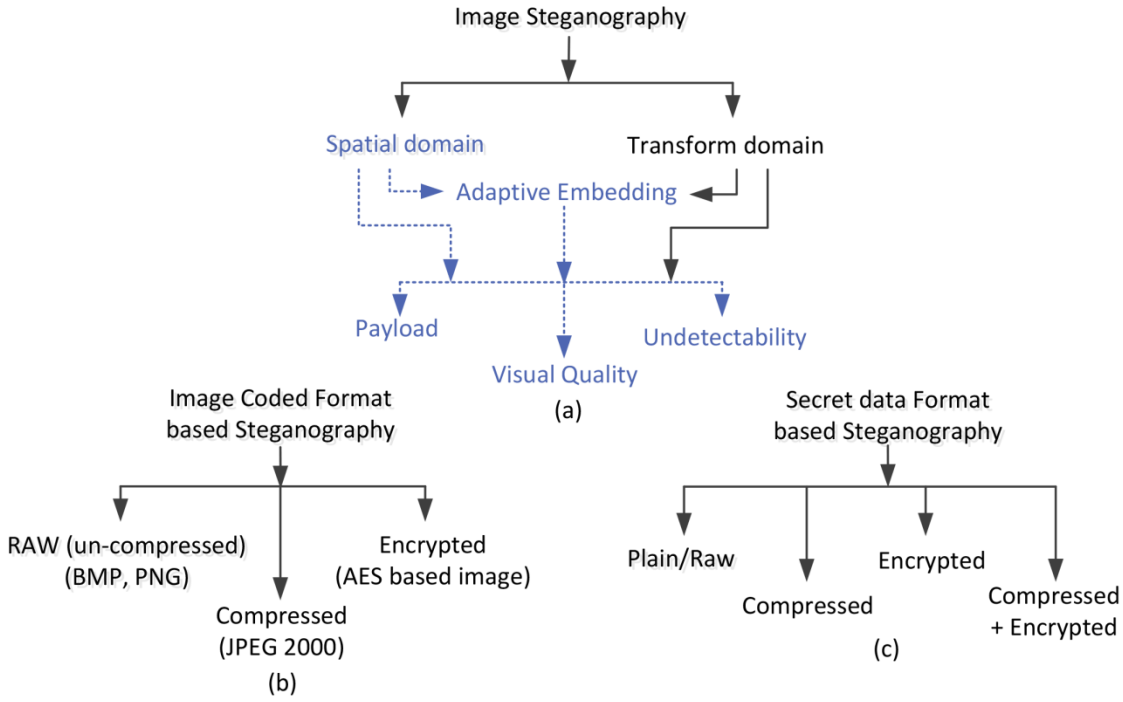

Fig. 4 (a) Image steganographic domains with their targeted goals, (b) Image coded format based embedding techniques, (c) Secret message format based steganographic techniques.

Table 2
The comprehensive comparison of spatial and transform domains with adaptive embedding schemes.

Characteristics	Properties	Spatial Domain	Transform Domain	Adaptive Embedding
System type	-	Simple	Complex	Depends on adaptive algorithm
Format dependency	-	Dependent	Independent	Independent
Pixel Manipulation	-	Direct	Indirect (e.g. in transformed coefficient)	Depends on inline technique
Computational complexity	-	Less computation time	High computational time	Algorithm-dependent
Embedding Capacity	Payload	High	Limited	Varied
Visual Quality	Imperceptibility	High	Less controllable	Highly controllable
Integrity of visual features	Sharpness, blurring, edges	Maintainable	Less maintainable	Maintainable
Robust	Compression, Noise Cropping, Rotating etc.	Highly prone	Less prone	Depends on internal algorithm
Security	Geometric attacks	Vulnerable to geometric attacks	Resistant to geometric attacks	Hard to geometric attacks

Statistical detection attacks analysis	RS, Histogram	Easy to expose/detect	Hard to expose/unsuccessful	Hard to expose/unsuccessful
Non-Structural detection attacks analysis	Feature set, SPAM	Easily detectable	Easily detectable	Difficult/Varied
Target	Capacity Visual quality Undetectability	High High Moderate	Moderate High High	Moderate High High

Spatial domain embedding methods are more popular than transform domain because of easiness in embedding and extraction process but have less robustness. The comprehensive differences between these domains are shown in Table 2. The next section will briefly discuss the highlighting path under spatial domain Fig. 4 (a).

3. Spatial domain image steganography

This section contemplated well-known steganography techniques under the spatial domain and their adaptive steganographic mechanism evolved in recent years. It is also highlighted their merits and challenges with qualitative and quantitative aspects together. In addition, the comprehensive analysis is shown in the form of Table 3. Furthermore, Fig. 9 illustrates the chronology of such spatial steganographic techniques that are focused in this section 3.1 to 3.13. This Fig. also indicates that some steganographic techniques derive other techniques to strengthen their steganographic efficiency in term of capacity, visual quality and security. Similarly, most steganographic methods are evolved as adaptive hybrid embedding techniques to provide better results.

3.1 Least Significant Bit (LSB) based methods

Least significant bit (LSB) [17] steganography is one of the fundamental and conventional method that is capable of hiding larger secret information in a cover image without noticeable visual distortions [18]. It basically works by replacing the LSBs of (randomly or) selected pixels in the cover image with secret message bits. The selection of pixels or the order of embedding may be determined by a stego-key. The basic LSB substitution mechanism is shown in Fig. 5. This section discusses the major variations and combination of LSB based methods in last 5 years.

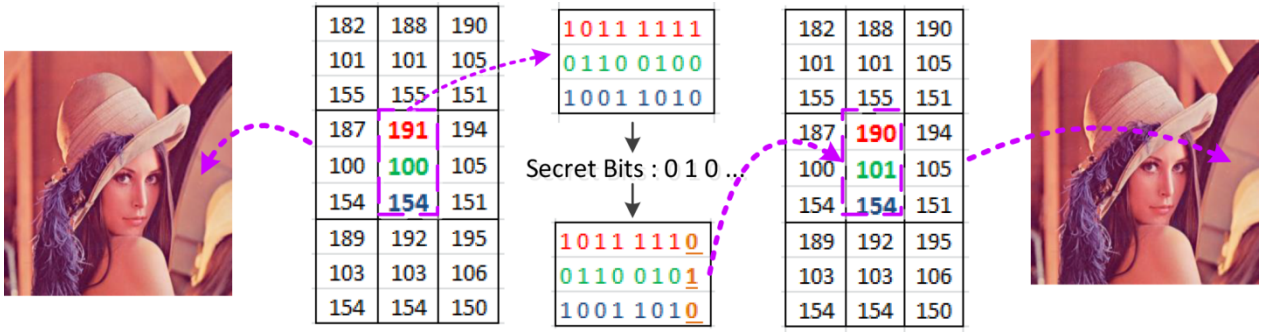

Fig. 5 Basic 1-bit LSB embedding mechanism

With the passage of time, steganographic methods employed a different variation of LSB's pixel or bit-planes. These methods have been developed in an effort to optimized payload while improving visual quality and undetectability due to the simplicity of LSB embedding. Some of them include adaptive LSB substitution based on edges, texture, intensity level, and the brightness of the cover images to estimate the *k* number of LSB for data embedding [19]. Similarly, a different flavor such as optimized LSB substitution using cat swarm strategy [20], LSB substitution with interpolation image [21], and reversible encrypted medical image using LSB substitution [22] exists.

Recently, to improve the visual quality and security against histogram attacks, Saeed et al. [23] proposed ±1 LSB based approach with the 1 bpp embedding capacity. It reduces the probability of changing pixels as 1/3 pixel modification. Due to less modification of stego-pixels, it enhances the visual imperceptibility and also has the resistance against the well-known LSB based detection attacks, i.e. HCF-COM steganalysis. But as compared with other latest LSB based method, the algorithm suffers from the low payload. Another well-known approach LSB+, that resists the histogram detection attacks, where it intentionally embeds some extra bits to make a similar histogram of stego-image with respect to its cover image. However, the LSB+ method still affects the statistical and perceptual characteristics of the cover image. In [24], authors improves the existing LSB+ based method by introducing to identify the sensitive pixels and keep them from extra bit embedding using key lock method, because the extra bits embedding scheme was traced by second order statistics (co-occurrence matrices). The LSB++ method decreases the amount of changes made to the perceptual and statistical attributes of the cover image. This method retains the avoidance of statistical attacks while preserving the histogram and co-occurrence metrics which was caused in extra embedding during LSB+. This technique also could improve the visual quality of peak signal to noise ratio (PSNR). Recently, [25] introduced the LSB based method called as LSB Word-Hunt (LSB WH) which is inspired by the world-hunt puzzle. The motivation of the approach is to reduce the modification per pixel value which indirectly increases the visual quality of stego-image. The

LSB WH approach only resists the statistical chi-square detection attacks.

Different steganographic methods come up with encryption algorithms to improve the security of secret message before embedding process. Amirtharajan et al. in [26] introduced an adaptive LSB method, where the random k-bit embedding approach is used. The cover image is divided into non-overlapping blocks of equal size and the encrypted confidential data are embedded in each block through four different random walks. If any random walk produces minimum degradation for a particular block that is recorded in the same block and kept it as a secret key. As a result, it provides robustness and enhances the quality of the stego-image. Similarly, Muhammad et al. [27] proposed a secure embedding method based on a stego key-directed adaptive LSB substitution with different levels of encryption. Secret information is encrypted by multi-level encryption algorithm (MLEA) before embedding, while the stego key is encrypted using the two-level encryption algorithm. Further, the encrypted data is embedded by adaptive LSB embedding approach depending on red channel, MLEA, and secret data. Experimental results reported that the proposed method achieve a better balance between security and visual quality. Meanwhile, it is lightweight or less computational complex when compared to traditional encryption techniques. Similarly, a three-level-encrypted algorithm (TLEA) using cyclic18 LSB substitution is proposed in [28]. Another three-level encryption algorithm (TLEA), and Morton scanning (MS)-directed least significant bit (LSB) substitution method is proposed [29]. This method employs I-plane of the input image in HSI for secret data embedding using MS-directed LSB substitution method. Furthermore, the secret data is encrypted using TLEA prior to embedding, adding an additional level of security for secure authentication. It is useful for authenticity of visual contents in social networks. In order to reduce the traditional encryption complexity load, [30] divided the gray scale image (secret data) into a different frequency, error and sign matrices. Further, it could be embedded into various cover images using XOR operation of bit-planes between matrixes and cover images. It has less computational complexity than standard encryption to provide confidentiality, but the strength of standard encryption cannot be overlooked. For the reference of an adaptive LSB based technique, Tseng et al. [31] proposed a method using edge characteristics of the cover image, which further incorporated to decide the number of LSB in a pixel. In embedding process, LSB's substitution was applied on edge pixels more than non-edge pixels. It could improve the embedding capacity but not proofed security against steganalysis. Another adaptive LSB based method by Nguyen et al. [32] provided an adaptive multi-bit planes image steganography using block data-hiding (MPBDH) that utilized all types of image regions (smooth or noisy). It employed more than one-bit plane and applied an adaptive complexity threshold to select the complex regions of a cover image for embedding the secret data. The embedding capacity and security performance significantly improved with respect to previous pixel/block-based adaptive LSB methods.

With respect to security or undetectability against modern steganalysis in LSB based method, a state-of-the-art highly undetectable stego (HUGO) embedding method [33] was proposed that is based on LSB matching technique. It consists of a high dimensional image model to calculate the distortion corresponding to a modification of each pixel by ±1. The payload is limited to 1 bpp, but can resist the modern steganalysis detection attacks [34]. Yuan et al. [35] proposed a novel method based on multi-cover adaptive steganography. The secret image embedding is adaptive to the textured regions of different cover images. Secret data embedding is done in LSBs and can be extracted using the XOR based operation. It can resist the modern steganalysis detection attacks such as SPAM features based steganalysis and AUS steganalysis [34, 36]. On the other side, many attempts were tried for increasing the embedded payload while retaining the good visual quality of stego-images in LSB based steganographic methods. Some of them merge the LSB embedding scheme with other techniques to confuse the steganalysis methods. For example, Hussain et al. [37] integrated the adaptive LSB with right most digit replacement (RMDR) technique based on different lower and higher texture regions of the cover image. The substitution of digits instead of bits in the pixel can reduce the risk of RS steganalysis [38] with improved payload and the good visual imperceptibly. But the proposed method cannot resist the modern steganalysis, i.e. SPAM [34] at higher (> 1 bpp) embedding rate. Similarly, another work presented to increase the payload by improving LSB scheme using modulo three strategy in [39]. The two ternary numbers in each pixel can be embedded, which generally modify the two LSB of the pixel that can become the cause of overflow/underflow problems. So a preprocessing of ±1 into the pixel is applied before embedding process. The proposed method improves the embedding capacity while maintaining the similar visual quality (as PSNR value) with respect to 3-bit LSB embedding methods, but it also exposed by modern steganalysis at higher embedding rate due to lack of adaptive embedding characteristics. Furthermore, for more depth on LSB steganography, recently Collins et al. [40] provided a dedicated survey on it.

3.2 *Pixel Value Difference (PVD) based methods*

Although LSB based methods are considered a simple way of information hiding and even very flexible to integrate with other methods, the main disadvantage is that the embedding capacity has a direct relation to visual quality of stego-image. For example, if we try to increase the payload by accommodate maximum level in the LSB of a pixel, it may reduce the overall visual quality of stego-image. To tackle the visual quality issue, Wu and Tsai et al. [41] proposed a steganographic approach based on pixel difference value. The difference value between two neighboring pixels is used to decide how many secret bits should be embedded? In the method, a cover image is partitioned into two non-overlapped consecutive pixels block in a zig-zag direction. Further in each block, the difference value between two pixels is calculated to decide the embedding size of bits, where difference values are grouped into a number of ranges. The selection of range levels or intervals in a range table is based on the human vision's sensitivity. Finally, the difference value is modified with the new difference value along the secret

data. The number of embedding secret data depends on the texture area of an image that actually controlled by range levels of the table. The larger the difference (higher texture), the more secret bits can be embedded into pixel pair. Overall, PVD method embeds a larger secret data into images with higher visual imperceptibility as compared with LSB substitution method. The PSNR value remains above 40 dB and can bypass the RS detection attacks. The major issues of PVD method are remarkable steps in the histogram that reveal the existence of a secret message. Second, the falling-of-boundary procedure is one of the significant problems. The third general image contains more smooth area instead of high texture, so the secret data bits will be hidden in the ranges with a small value. The basic PVD based embedding diagram is illustrated in Fig. 6.

In literature, many works were presented to resolve the PVD limitations and enhance the steganographic objectives. For example, Tri-way PVD [42], PVD with LSB [43, 44], Multi-Pixel Differencing (MPD) [45], Modulus Function (MF) [46-48], block based PVD [49] and various methods discussed in [50-52]. To improve the embedding capacity, [53] combined the PVD method with adaptive LSB substitution and optimal pixel adjustment process. To obtain good visual quality and high payload, Hsiao Shan et al. [54] proposed a multi-way PVD method by combining the tri-way PVD and mode selection process, while this combination improved the visual quality but has low payload when compared with [53]. Mandal et al. [55] proposed an adaptive PVD method with modulus function to resolve the fall-off-boundary conditions, while retaining the similar payload and imperceptibility as original PVD. To utilize the tri-way PVD, Lee et al. [56] proposed a practical embedding of the secret image communication with the combination of compression. The secret image (data) is compressed by JPEG2000 at high compression ratio and embedded by tri-way PVD. After embedding and extraction process the quality of the secret image was degraded due to highly compressed ratio. Further, a residual value coding is proposed to reduce the visual distortion in the recovered secret image. The proposed method provided the secrecy while avoiding the dual statistical detection attacks.

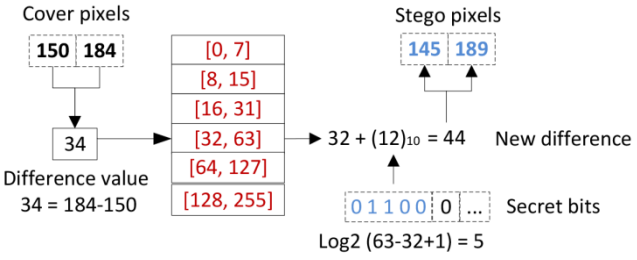

Fig. 6 General pixel values differencing embedding scheme

Balasubramanian et al. [57] proposed an octonary pixel pairing scheme to handle the visual distortion and low payload. The method is based on the principle that edge areas are more tolerable for larger modification than smooth areas, and hence can hold more secret data. So the edge areas are identified first in the region selection phase. Subsequently, the number of bits that can be embedded inside each pixel pair is determined by referring the range table. If the regions are sufficiently large for hiding the given secret message, then secret data is embedded into the selected regions. Otherwise, the smooth regions are utilized for embedding after using all the edge regions. The data hiding is performed as per the octonary PVD scheme. Finally, pixel readjustment was applied to improve the perceptual quality and the statistical undetectability. With similarity, Liu et al. [58] proposed an adaptive PVD based on pixel blocks complexity to improve payload.

In the PVD hybrid method introduced by Shen et al. [59], it combined PVD with modulus function to improve hidden capacity. It fully takes the advantages of correlation of the R, G and B planes in the color image. The number of secret bits is determined by the difference of corresponding G planes pixels. Furthermore, various adjustment processes are applied to maintain the overflow and underflow problems. The proposed method is secured against RS diagram and histogram analysis while provided an acceptable visual quality. But it suffered from low payload against other PVD based methods. Another hybrid PVD with exploiting modification directions (EMD) steganographic method was proposed to improve payload and imperceptibility by Shen et al. [60]. First, a cover image is mapped into a 1D pixels array by Hilbert filling curve instead of conventional zig-zag ordering. Hilbert filling order showed more locality preserving property against raster scan or zig-zag scan orders. It could resolve the overflow/underflow issues and minimize the embedding distortion. Recently, Hernández-Servin et al. [61] introduced a modified version of Tri-way PVD embedding that can remove the extra need of location map for overflow/underflow problem during secret communication. It employed the two embedding approaches, a tri-way for regular secret data embedding and a reversible embedding for location map insertion. Furthermore, G. Swain et al. [62] proposed two adaptive PVD based steganographic solutions that utilized the vertical and horizontal edges. The first approach used the 2x2 pixels blocks and the second one was applied on 3x3 pixels blocks. Both methods are targeted for larger capacity and better visual quality of stego-images.

Recently, I. R. Grajeda-Marín et al. [63] presented another solution to resolve the overflow and underflow problem in the PVD. It focuses on the Tri-way PVD and computes the optimal pixel values for each embedding block. In results, it could resolve the underflow and overflow issues while improving the payload. Khodaei et al. [64] proposed an adaptive hybrid embedding approach based on PVD with LSB methods. It divided the cover image into two pixels blocks, further estimate the difference between these two pixels. The numbers of secret bits are estimated based on difference value and adaptive LSB embedding scheme was employed. The proposed method introduced a readjustment process to keep the difference intact as in cover image pixels. Similarly, G. Swain et al. [65] combined the directional PVD with LSB for the adaptive steganographic method. First, it inserted the k-bits secret data in upper-left pixel from 2x2 pixels block. Next, the PVD embedding process was applied to the upper-left base pixel and other remaining pixels in horizontal and vertical edge directions. It was suggested two embedding techniques, Type 1 and Type 2 to improve PSNR only and PSNR with high payload respectively.

3.3 Exploiting Modification Direction (EMD) based methods

Exploiting modification direction (EMD) is a well-known embedding technique that maintains the high fidelity of stego-images [66] . Generally, the secret digit is transformed by the (2n + 1)-ary system during embedding process in the EMD, where n are the number of cover pixels. The maximum pixel value of distortion range is just (±1). In other words, the EMD utilizes the specific base to determine the local variation of pixel intensity in the image, therefore pixels in high texture areas can embed the more secret message. As results, the EMD can achieve good visual quality when compared with LSB and PVD methods. On the other hand, the maximum capacity of EMD method is up to 1.16 bpp for a number of (n = 2) two pixels, meanwhile, its embedding payload drastically decreases as selected pixels are increased. Therefore, different EMD based methods were proposed to improve the embedding capacity, i.e. [67-71].

In [72], authors came up with proposing of two EMD based embedding techniques called HoEMD and AdEMD to improve payload and imperceptibility. HoEMD concept was to exploit the pixels direction, where the pixels with larger variations has larger directions and may have larger embedding payload. On the other hand, in AdEMD philosophy, the pixels belongs to edge regions may compensate more secret data, but these can be suffered from overflow problem. T. D. Kieu et al. [67] proposed a robust (2n+1)-ary base system on fully exploiting modification direction (FEMD). The FEMD technique improved the embedding capacity from 1 bpp to 4.5 bpp, together with good visual imperceptibility against [66]. It required a search matrix for embedding as an overhead and meanwhile was unable to tackle the overflow conditions as well. K. Wen-Chung et al. [69] resolved the above overflow problem and maintained the embedding capacity. The secret data are embedded directly by formula operations (or without using a lookup matrix) and is known as formula fully exploiting modification directions (FFEMD) method. Similarly, in [68] generalized the exploiting modification direction (GEMD) method presented. The main contribution as the (n+1)-ary binary bits can be embedded into *n* adjacent pixels directly. The experimental results showed it could maintain the embedding payload $(1+\frac{1}{n})$ with adjustable pixels group. In simple, GEMD technique cannot hide more than two secret bits for each pixel; meanwhile it modifies all pixels of the group during secret data embedding. To handle the weakness of pixel modification problem, in [73] W.-C. Kuo et al. proposed a method as Modified Signed-Digit (MSD). It only modifies the n/2 pixels with the value of ±1 range and has 1 bpp payload even increasing n pixels as well. The MSD scheme has resistance against RS steganalysis [38] with good imperceptibility. Another method by W.-C. Kuo et al. [74], a multi-bit encoding function is used to improve further the embedding payload. The proposed method can embed up to $(k+\frac{1}{n})$ on average of each pixel, where k is determined by the number of embedded bits per pixel. It could reduce the overhead of secret data conversion and further provide the flexibility of adjacent pixels relation. Meanwhile, the MSD method maintains the security against RS and bit plain detection analysis, but it suffers from low visual quality when compared with existing EMD based methods because higher embedding capacity reflects in result of lower visual quality. To improve the embedding payload with good imperceptibility, K. Wu et al. [75] proposed a hybrid approach to EMD with LSB and modification of prediction errors (MPE). The method fulfilled the objectives, but it suffered from security such as histogram and RS detection analysis. However, most EMD based methods decided the n-base notation system before embedding procedure in aforementioned methods, it becomes the main disadvantage of their techniques and that should be adaptive introduced in [74].

3.4 Multi-Base Notation System (MBNS) based methods

Another spatial domain embedding method based on multiple base notational systems (MBNS) is introduced to re-express/transform the secret data into the notational system before embedding process. In MBNS based techniques, secret data is converted into symbols and re-expressed in the multiple-base notational system, i.e. binary, decimal, and octroy system. Further, these symbols are embedded into pixels intensities. Generally, the larger notational base symbol indicates the larger embedding rate.

M. Afrakhteh et al. [76] proposed adaptive more surrounding pixels using (A-MSPU) MBNS method, which can improve the visual imperceptibility of MBNS problems. It utilized the edge region pixels with representing the secret data in MBNS that employed either three or four adjacent pixels of a target pixel, while it utilized all eight adjacent neighbored pixels to improve the visual imperceptibility. Similarly, many works were introduced to improve embedding capacity in MBNS based methods. In [77], authors proposed an adaptive steganographic method based on varying-radix numeral system (VRNS). The method decomposed the secret data into numerals that have variable information carrying capacity. This decomposition depends on the cover pixels tolerance to manage maximum adulteration for larger secret data. The experimental results showed the larger payload while maintaining good imperceptibility. Further, it manages to retain security against RS [38] steganalysis, but still embedding payload is limited to other radix based techniques. Therefore, [78] improved the [77] VRNS method by proposing an information hiding using adaptation and radix (AIHR) algorithm. However, from experimental results, this method has larger payload than existing VRNS systems but also has some ambiguity in proposed flow i.e. how sender and receiver will be synchronized with the selection of bases? In AIHR extraction process, again the ambiguity of finding the M, that may lose the integrity to fully recover secret data. Recently, W.-S. Chen et al. [79] proposed a general multiple-base (GMB) secret data embedding method. The secret data bits are converted to M-ary secret digits for pixel-cluster (i.e. n pixels). The M is automatically determined by the input function of the end user. It provides the multi-purpose embedding styles, in result high embedding or high quality of stego-image can be achieved. Furthermore, this method is able to accurately predict the overall capacity and visual quality by mathematical expression without embedding the real secret data inside

images. At lower or 1.0 bpp, GMB method can resist the non-structural SPAM feature based steganalysis and also has resistance against statistical RS steganalysis [38].

3.5 Pixel Pair Matching (PPM) based methods

Another promising steganographic method is based on pixel pair matching (PPM). Usually, these embedding methods utilized the pixel pair $(p_{i,1}, p_{i,2})$ as a reference coordinate to search another coordinate $(p'_{i,1}, p'_{i,2})$ within a predefined neighborhood set of ϕ $(p_{i,1}, p_{i,2})$ to satisfy $f(p'_{i,1}, p'_{i,2}) = \text{SB}$. Where f denoted an extraction function and SB is the secret digit in B-ary notational system. Data embedding scheme is done by replacing $(p_{i,1}, p_{i,2})$ with $(p'_{i,1}, p'_{i,2})$ as shown in Fig. 7.

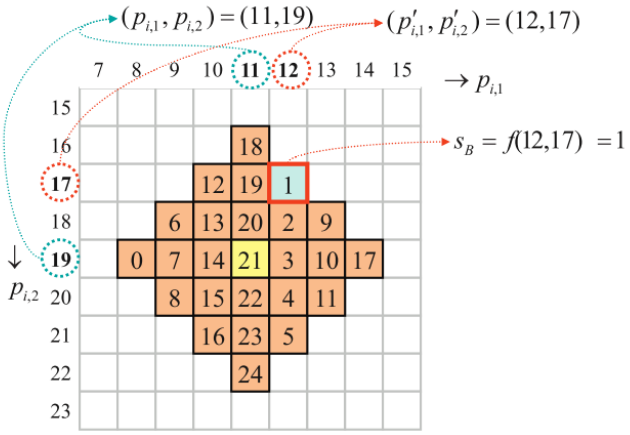

Fig. 7 The neighborhood set ϕ (11,19) [80]

An adaptive pixel pair matching (APPM) method was proposed by W. Hong et al. [81]. Two pixels are scanned as an embedding unit and a designed neighborhood set is specially employed to embed secret message digits. W. Hong [82] introduced the patch reference table (PRT) based embedding with adopting a single reference table (RT). Further, the PVD concept was utilized with PRT method to improve embedding capacity and visual quality. In the method, a special embedding sequence was designed and the number of secret bits to be concealed was estimated by the pixel-value difference. It could retain the histogram, while has limited security (@ 0.5 bpp) against SPAM based steganalysis. In [83], J. Chen proposed a pixel pair matching (PPM) with PVD method, where secret data were embedded adaptively into a pixel pair using two reference tables. The various bits based on the pixel value difference could be concealed in the image. The method reduced the falling off the problem and provided a larger payload with the better visual quality. Further, the proposed method maintained the shape of the histogram of the pixel difference and also showed resistance to chi-square steganalysis.

3.6 *Gray Level Modification (GLM) based methods*

Another spatial domain strategy is a gray level modification (GLM). These types of embedding methods map the secret data by modifying the gray level of pixels (not hide or embed). V. M. Potdar et al. [84] method was based on a mathematical function, where a group of pixels was selected for mapping the secret data inside it. This method utilized the concept of odd and even numbers for mapping, 0 and 1 were mapped with odd and even values respectively for example. The GLM base methods are simple to implement and have minimum computational complexity. However, these methods were unable to resist steganalysis detection attacks. Recently, in [85] authors proposed an RGB image based gray level modification (GLM) and multi-level encryption (MLE) method. This approach encrypts the secret data using MLE algorithm before mapping of GLM. The experimental results depict that the proposed method has less complexity than other standard encrypted steganographic methods. And the method improved the visual quality although it suffered from statistical steganalysis detection attacks.

3.7 Pixel Value Prediction based methods

The prediction based spatial domain embedding gained a lot of attention in recent years. Because the direct altering of pixel values for embedding leads to distortion of visual quality and it causes the low embedding capacity in the case of maintaining good visual quality. Therefore predictive coding technique was proposed to resolve the above problems. In predictive methods, the pixel intensities were predicted through predictor instead of direct modifications. The predicted error values were modified to compensate for secret data. In literature, various predictions based reversible embedding techniques are proposed to improve existing ones.

In [86], Y.-H. Yu et al. proposed a prediction error based image steganographic method to modify the predictive errors. Due to the use of uniform quantization embedding rule, the prediction errors distribution during embedding propagates the visual artifacts that are led to steganalysis. W. Hong et al. [87] proposed an embedding method based on a modification of prediction error (MPE), whereas it modified the histogram of prediction errors to find the vacant position for secret data embedding. The overall visual quality of MPE method guaranteed to above 48 dB, while embedding capacity was also improved by well-known Ni et al. method. H.-C. Wu et al. [88] proposed a predictive coding based reversible embedding technique. The method employed the secret data into compress codes that were utilized during lossless image compression coding. At the predictive coding stage, the proposed method embedded the secret data into error values by referring to a hiding tree. In reverse, secret data can be recovered by referring to the hiding tree at entropy coding stage. This method provided the largest up to 0.0992 bpp embedding payload. Recently, [75] utilized the MPE method with other steganographic LSB and EMD methods to improve the hidden capacity. To obtain the higher embedding capacity, [89] introduced a multiple predictor base data embedding method. This multiple predictor's mechanisms is basically the extension of MPE approach to embed the secret data without adding any predictor overhead. During embedding process, the selection of accurate predictor depended on the history of the predictor. The proposed method showed the improvement in embedding payload and visual quality, while its security was not evaluated by any steganalysis approach.

3.8 Histogram based methods

Histogram based data hiding is another commonly used steganographic technique. The histogram shifting is considered the most efficient histogram based embedding schemes and it has following phases. First, it finds the peak and zero points in a cover image, whereas the bins are shifted with one level between the zero and peak points for emptying peak points. In the second phase, the secret bits are concealed by predefined adjustments in new peak point and the empty point.

In P. Tsai et al. [90] embedding scheme, a cover image was divided into 5x5 non-overlapped image blocks. In each block, the center pixel is treated as a base pixel for linear prediction process, whereas the other (remaining) pixels in the block are processed by linear prediction to generate the residual values. The histogram of residual was employed by histogram shifting to store secret data. Furthermore, multiple pairs of the peak and zero points were used the histogram shifting to increase the embedding payload. In another method in [91], a two-dimensional difference histogram modification and difference pair mapping technique was proposed. In the method, a pixel pair selection strategy enhanced the performance of reversible embedding. The pixel pair selection strategy can locate accurately the targeted pixels in smooth regions. Therefore, this strategy performs much better on smooth images than on heavy texture area of images. T.-C. Lu et al. [92] proposed a hybrid steganographic method that is based on histogram shifting with difference expansion and interpolation technique. In here, the secret data are embedded in two ways; i.e. concealable pixels and difference of interpolated pixels. Therefore, the proposed method gained a high payload against existing compared methods. In another method by Z. Pan et al. [93], a reversible data embedding technique based on histogram shifting are introduced. The neighboring points of the peak point were used to embed the secret data which is based on histogram shifting, while the peak point remains unchanged. The concept of localization was introduced to generate more peak points in results, its neighboring points were embedded by more secret data. In fact, the localization equally redistributes the greater histogram changes into small changes and keeps the similar histogram to cover histogram. It could improve the embedding payload by exploiting the localization with multilayer embedding. Recently, N.-K. Chen et al. [94] improved the reversible data embedding method with histogram shifting in medical images. Generally, reversible embedding is required an extensive data as a location map for reconstruction of cover images. To reduce the size of location map, the proposed method keeps the information record in just two bits of each block, ultimately it could significantly reduce the size of location map table while achieving an efficient data embedding by histogram shifting.

3.9 Edge-base method

One of the prominent embedding strategies in the spatial domain is edge adaptive embedding technique. In the spatial domain, direct modification of pixels yields a visual distortion if these pixels belong to smooth areas in the image. Thus, the edge adaptive embedding schemes are evolved to maintain the minimum visual distortion. Similarly, edge adaptive steganographic methods are favorite to provide high imperceptibility. Fig. 8 shows the canny based edge detector of Lena image that can further efficiently employed by different embedding techniques.

Fig. 8 Lena and its Canny edge based image [95]

W. Luo et al. [96] proposed an edge adaptive steganographic method. The LSBMR is applied for embedding the secret data. The complex and light edge textures regions were selected for larger and smaller embedding payload respectively. The method maintained the visual imperceptibility and security, while it suffered from the low payload. Similarly, authors in [97] proposed a simple and effective embedding method that employed the concept of hybrid edge detection by combining the fuzzy edge and canny edge detectors. However, the underlined embedding was employed by LSB substitution. Furthermore, this technique could provide good visual quality due to considering the HVS principle by edge based embedding and also showed security against statistical steganalysis detection attacks. Meanwhile, the unwanted (n−1) bits modifications of each block were introduced like as the first pixel in each block.

A. Ioannidou et al. [98] introduced a hybrid (as fuzzy and Sobel) edge detector based embedding technique to color images. The method fully utilized the sharp regions of an image for larger embedding payload. It improved the embedding payload while having an overhead as extra logging information was maintained for recovering the secret data in decoding phase. Further logging information was encrypted by Triple-DES algorithm. Unlike [97], the method employed the Sobel edge detector instead of Canny to produce the highest value of PSNR. The overhead was to maintain the two separate additional files, i.e. height, width, and channel modified bits. In addition, the proposed method was not evaluated by steganalysis technique to verify its security level. Further, N. Grover et al. [99] resolved the problem of [98] by incorporating an edge based adaptive embedding for color images to improve the payload. The method improved the security while providing the division of secret data into two different blocks, i.e. edge based and non-edge based blocks for more efficient embedding. R. Roy et al. [100] proposed another edge adaptive technique that combined the matrix encoding and LSBM for embedding in the edge regions of a cover image. This also utilized the cat chaotic mapping to distort the payload. The payload was restorable only by supplying correct key. It was provided high fidelity and imperceptibility, even performed better than LSBR and PVD based techniques, but still suffered from low embedding capacity. Furthermore, M. R. Modi et al. [101] proposed an edge based embedding for color images, where it

utilized the 2-bit LSBM method in embedding process. Canny edge detection technique was applied from one selected R, G, or B channel. Further, the other two channels corresponding to the edge pixels were employed for embedding the secret data. However, the proposed method still suffered from low embedding payload, where the payload was 0.083 bpp for color edge pixel. K.-H. Jung et al. [102] proposed a semi-reversible embedding method, where the image was interpolated and divided into two regions i.e. edge and non-edge. A threshold decided the number of secret bits that were used to embed inside the edge areas. For non-edge areas, the difference between two non-overlapping consecutive pixels was utilized to estimate the number of secret bits for embedding into a pixel. As a result, the embedding capacity was increased, while maintained the good visual quality, but found the lack of steganalysis evaluation to proof its security.

Recently, H. Al-Dmour et al. [95] proposed a method based on combining the edge detection and XOR coding. The proposed method first utilized the sharpest regions of the image and then further gradually moves to the less sharp regions. The proposed method improved the visual imperceptibility. The contribution of edge detection in the approach was to estimate the exact edge intensities for both the cover and stego image before and after hiding the secret data. The edge consistency in both cover and stego image maintained the security against different textural feature steganalysis approaches. Similarly, in [103] authors proposed an edge based secret image embedding method that was employed by canny edge detector with 2k correction (where 2k correction maintained the visual quality). In the technique, a canny edge detector was applied to detect the edge of the cover image and only edge pixels were selected for embedding the secret data. Secondly, a sorting technique was employed to randomize the edge pixels to enhance the security. Further, the Huffman encoding was also applied. An adaptive coherent bit length L was computed and determined by the edge pixels which are further utilized to substitute secret data. Even though the previous works have maintained the good visual quality and capacity, but it could easily be detected by modern steganalysis. In addition, it requires an extensive computation due to encoding phase with respect to other existing spatial domain methods.

3.10 Mapping base methods

In the spatial domain, one way of embedding using mapping/matching of secret data with cover image data were introduced. There are numerous methods available i.e. pixel, block, bit-plane mapping etc. [104] introduced a two-way block matching technique by dividing the cover and secret image into m × n block, where the highest similarity of blocks between the cover and secret images are searched. In next step, the index information of matched and unmatched blocks were compressed and embedded through distributed LSB to provide a less distorted image. Al-Hussaini et al. [105] proposed another type of mapping based method with a pixel to the alphabetic letter, where English alphabets plus some special characters are mapped to the pixel values with the help of mapping table. Meanwhile, matching pattern was maintained and required for extracting. it is considered as a low computational method because of no overhead for texture computation. A. Nag et al. [106] proposed a novel approach based on LSB using X-box mapping, where the unique pattern of different X-boxes was utilized. Four unique X-boxes with different sixteen values (represented by 4-bits) are used and each value was mapped to the four LSBs of the cover image. The security of the proposed method was dependent on mapping rules, which were mandatory to recover the secret data. It could degrade the visual quality due to fixed 4bit LSB substitution. R. Roy et al. [107] proposed an image realization steganographic method with cover-to-secret mapping considering the low embedding rates. This method utilized the concept of Longest Common Subsequence (LCS) to map the secret image to the cover image. Further, the generated map and key should be synchronized with the receiver end to extract the secret image fully. It was based on the simple mapping but had high computation due to LCS mapping nature. And the maintenance of auxiliary information was another overhead of this technique.

In literature, another way of mapping known as direct bit-plane mapping (i.e. binary, Fibonacci, Prime, Natural, Lucas, and Catalan-Fibonacci) is introduced. Recently, A. A. Abdulla et al. [108] introduced a bit plane mapping to improve the visual quality and security. It consists of two phases. First, it reduced the secret data size by proposing a secret image size reduction (SISR) algorithm. Second, the compressed data were embedded through Fibonacci representation in pixel intensities to reduce the embedding distortion of stego pixels. Therefore, the payload and good imperceptibility attained by using bit-plane(s) mapping instead of bit-plane(s) replacement in the embedding process. Another method proposed by A. A. Abdulla et al. [109] is based on the virtual bit plane mapping. The proposed method employed the specific representation to decompose the pixel values into 16 virtual bit planes for embedding process. It could improve the visual quality and embedding payload against existing pixel decomposition based bit plane mapping techniques.

3.11 Pixel/Block indicator base methods

Another strategy in the spatial domain, pixel/block indicator based data embedding schemes are introduced. An RGB based color image consists of 3 bytes including red, green and blue intensities, where one of the RGB channels is used as an indicator and the rest are considered as data channels. A. Gutub et al. [110] proposed a pixel indicator-based method that has a high payload. The proposed method embedded the secret data in one or both of the data channels in a predefined cyclic manner. The experiments showed the better results in term of payload and imperceptibility and also avoided the key exchange overhead for data indicator signaling. In the technique, the payload capacity was totally dependent on a cover image and its indicator bits. In addition, it can hide the fixed number of bits in each pixel, whereas payload was directly affected/degraded the visual quality of the image. In N. Tiwari et al. [111], two embedding techniques were proposed. First, it improved the [110] method by changing the indicator channel for every subsequent pixel to improve the security factor. Second, the random number generator was employed to estimate the secret bits to embed in the LSB of a pixel, where up to 4 LSBs can be embedded

into the data channel. Further, G. Swain et al. [112] introduced a block based RGB indicator data embedding method that divided the image and secret data into each 8 blocks, where user defined key decided the one to one image and secret block mapping or relation. In embedding process, one channel was considered as indicator and others as data channels. The secret data was embedded on LSB by maximum matching portion to reduce the visual distortion in stego-image. Another indicator based steganographic method proposed by P. Mahimah et al. [113] in a zigzag mannered using LSB embedding. It utilized two different indicators based on zigzag traversing. In result, the visual quality and security of secret data were improved. In [114] method, a cover image was scrambled and employed by PVD and adaptive LSB according to blue pixel indicator. The red and green planes were considered as data channels. The proposed method improved the payload and security by scrambling the red and green planes, while visual quality is dependent on embedding capacity. Recently, P. Das et al. [115] proposed an embedding method based on color channel indication. The hiding sequence is controlled by an indicator pattern table, which further indexed by the secret data bits. During embedding phase, indicator and other metadata are embedded inside the cover image as a header that used in recovery phase to blindly recover the secret data. Encryption of secret data and RC4 cipher of the header may increase another layer of security.

3.12 Color Model based methods

Recently, researchers have used correlation of color spaces for embedding purposes. For example, RGB channels, where modification to one channel affects the overall quality of stego-images, which indirectly decreases suitability for steganographic algorithms. Various color spaces are exploited for embedding purposes i.e. RGB, YCbCr, HIS [116, 117]. In [118], Khan et al. proposed an adaptive LSB substitution method using uncorrelated color space, which indirectly increases the imperceptibility while minimizing the chances of detection by the human vision system. First, the cover-image is scrambled to generate an encrypted image, further converted into HSV color space. An ALSB method is then used to embed the data inside the V-plane of HSV color model. Similarly, in [119] presents a novel magic least significant bit substitution method (M-LSB-SM) for RGB images. It employed an achromatic component (I-plane) of the hue-saturation-intensity (HSI) color model with multi-level encryption (MLE) for embedding purposes. This technique improved the visual quality and provides multiple security levels compared to existing methods.

3.13Machine learning base methods

In spatial domain methods, the optimization techniques can be employed to improve the success of embedding algorithms. A steganography method by Tseng et al. [120] was proposed based on OPAP and genetic algorithm (GA). It improved the compatibility of cover and stego images by altering the secret bits. M. Khodaei et al. [121] improved the visual quality by using the LSB substitution, where the GA method was applied as setting parameters of the objective mapping function to obtain the best condition in the distribution of pixels. Similarly, H. R. Kanan et al. [122] proposed a spatial domain GA-based reversible data embedding method with tunable visual quality. This method modeled the hiding process as search and optimization problem. As a result, embedding payload and visual quality were improved. However, the computational complexity was increased and its security was not proved. To obtain larger payload, N. N. El-Emam et al. [123] introduced a steganographic method based on adaptive neural networks (ANN) with modified particle swarm optimization (PSO). The proposed method proved good visual imperceptibility with security and also achieved the high payload shown through experimental results. Another method in [124] proposed a three-phase intelligent technique for color images to improve the visual imperceptibility and embedding payload. The first phase of a learning system (LS) was applied before embedding steps, while the other phases applied after embedding process. The ANN and adaptive GA were applied to estimate the number of embedded secret bits inside the pixels. The results showed that proposed algorithm could embed a larger payload up to 12 bpp with good visual quality. Recently, Ş. Doğan et al. [125] proposed a chaotic maps based method to improve the data hiding technique using GA. In the method, the GA fitness function was selected based on PSNR. Further, the various sizes of secret data were employed into the cover image using random functions and chaotic maps. Meanwhile, the randomness of genetic was performed by using different chaotic maps, i.e. gauss, logistic, tent. Finally, the chaotic maps were considered the fastest than random function for steganographic technique. The aforementioned techniques stand in the row of computationally expensive methods category due to optimization based methods i.e. GA.

Table 3
Performance of recent steganographic techniques

Approach	Reference	Algori-thm	Advantages	Major Challenges	Embedding Capacity (bpp)	Visual Quality (PSNR)	Resistance against Steganalysis
LSB-based	(Chakraborty et al., 2013) [30]	LSB X-OR	• Replacement of encryption in stego-system • Achieved similar payload distortion while reduced computation and time complexities against conventional encryption (i.e. DES, AES) in stego-system	• Maintenance of different matrices • Evaluation of Steganalysis detection attacks missing	NA	NA	NA
LSB-	(Sarreshted	±1 LSB	• Simple implementation.	• Lower embedding capacity	1 bpp	52.90 dB	HCF-COM

based	ari & Akhaee, 2014) [23]		• 1/3 LSB's modified for hiding. • Reduced probability of change per pixel. • High imperceptibility.	compared to existing LSB based method. • Secret key dependency.	(gray)		(normal, calibrated, adjacency)
LSB-based	(Qazanfari & Safabakhsh, 2014) [24]	GLSB++	• Improved visual quality. • Reduced extra bit embedding in existing LSB++ technique. • Secure against Histogram analysis.	• High complexity for the new cover to compute lock key. • Encryption key dependency. • No robustness.	≈ 0.8 bpp (gray)	> 50 dB	Preserve the Histogram, Chi-Square
LSB-based	(Yuan, 2014) [35]	Adaptive ±1 operation LSB	• Utilize multiple covers with location sensitive secret embedding in 2 LSB planes • Not required stego-key at recovering stage. • Less modification per pixel (mpp). • Time efficiency.	• Overhead of multiple cover images for the steganographic process. • Limited embedding capacity even employing multiple covers	NA	≈ 50 dB	SPAM 2nd order with SVM, AUC
LSB-based	(Muhammad et al., 2016) [27]	ALSB-MLEA	• Multi-level encryption applied on stego-key as well as secret data. • Channel indicator based embedding. • Keeps balance between security and imperceptibility. • Light-weight against encryption.	• Limited embedding capacity. • Limited robustness.	≈ 1 bpp	> 45 dB	Histogram, Robustness against salt & pepper noise
LSB-based	(Tavares & Junior, 2016) [25]	LSB-WH	• Based on Word hunt puzzle approach. • Reduced modification of per pixel value. • High imperceptibility.	• Need to test over modern or non-statistical steganalysis	NA	NA	Chi-Square
LSB-based	(Nguyen et al., 2015) [32]	MPBDH	• Block based multi-bit plane adaptive LSB embedding. • Efficient texture complexity levels are computed by an adaptive threshold. • Maximum utilization of all texture regions. • Reduce visual attacks.	• RSA and AES key maintenance dependency for encryption. • No robustness against cropping, compression.	≈ 1.5 bpp (gray)	≈ 46 dB	SPAM with Ensemble Out of Bag (OOB) @ low bpp
PVD-based	(Lee et al., 2012) [56]	PVD-TPVD	• Secret image communication. • Can embed larger secret image than the cover. • TPVD utilized for embedding. • JPEG2000 compression applied on the secret image to reduce size.	• High complexity. • Lack of other statistical analysis.	1.64 bpp (gray)	≈ 40 dB	RS analysis
PVD-based	(Balasubramanian et al., 2014) [57]	Octonary PVD	• Exploited the all eight directions for higher embedding capacity. • Adaptively region based embedding. • Readjustment phase maintains regions after embedding to fully recovery of secret data. • Resistance against various specific and universal statistical steganalysis. • Extensive testing over massive datasets.	• Modern steganalysis evaluation required.	≈ 3.6 bpp (gray)	≈ 40.20 dB	RS analysis, HCF-COM, LSB matching, PVD analysis
PVD-based	(S. Shen et al., 2015) [59]	MF-PVD	• A simple implementation for reversible embedding. • Utilized the correlation of R G B channels. • Resolve the PVD underflow/overflow problem.	• Lack of modern steganalysis. • Limited embedding capacity.	≈ 1.03 bpp (color)	≈ 36 dB	RS analysis, Pixel Difference Histogram
PVD-based	(Hernández-Servin et	PVD-TPVD	• Eliminate the location map of overflow/underflow for TPVD.	• Not discussed any robustness.	≈ 1.55 bpp	≈ 36.25 dB	NA

	al., 2015) [61]		• Replace the range table with simple linear function. • A solution of boundary problem.	• Security should be evaluated.			
PVD-based	(Swain, 2015) [62]	Ad-PVD	• Application based adaptive solutions i.e. 1-High payload 2-High visual quality. • Efficient horizontal and vertical edge directions are considered for embedding.	• Lower embedding capacity compared to existing PVD based method.	≈ 1.74 bpp (color)	≈ 46.65 dB	RS, Pixel Difference Histogram
PVD-based	(Grajeda-Marín et al., 2016) [63]	PVD-TPVD	• Skip overflow/underflow problems. • Improved visual quality in TPVD-PVD • 100% utilization of pixels for embedding.	• Lack of security evaluation by steganalysis methods.	≈ 2.14 bpp (gray)	≈ 38.33 dB	NA
EMD-based	(Kieu & Chang, 2011) [67]	FEMD	• Massive improvement in capacity. • Adaptive payload solution. • Exploited eight directions for EMD • Embedding with minimal distortion.	• No handling of an overflow condition. • No evaluation of steganalysis.	1 to 4.5 bpp (gray)	≈ 52 to 31 dB	NA
EMD-based	(H.-M. Sun et al., 2011) [72]	Ad-EMD, HoEMD	• Improved embedding capacity. • Adaptive embedding based on texture. • Resolve the overflow/underflow problem.	• Limited steganalysis evaluation.	2.5 to 3.5 bpp (color)	≈ 43 to 34 dB	Chi-Square
EMD-based	(Wen-Chung & Ming-Chih, 2013)[69]	FFEMD	• Resolve the overflow problem. • Remove the lookup matrix by formula operation. • Less memory and resources required.	• No robustness discussed. • High pixels modification ratio.	NA	NA	NA
EMD-based	(Kuo et al., 2013) [68]	GEMD	• Resolve the extraction function fixed weighting with dynamic modulus table. • Extraction function: lookup & formal form.	• Only two pixels limited relationship in embedding. • All pixels modifications occur.	1.5 bpp	≈ 50.17 dB	NA
EMD-based	(Kuo, Wang, et al., 2016) [73]	MSD	• Reduce the pixel modification ratio (n/2). • Only ± 1 ranges variations. • Maintain the bpp with increasing of n pix.	• Limited embedding capacity	1 bpp	> 52 dB	RS Bit plane attacks
EMD-based	(Kuo, Kuo, et al., 2016) [74]	MBEF	• Flexible adjacent pixel relation, i.e. n • Adaptive embedding capacity, i.e. k bits • Not required secret data conversion. • Handled the overflow/underflow problem	• Lower visual quality against EMD approach i.e. n=2 • Higher embedding capacity reduces the visual quality.	1.25 to 4.5 bpp	≈ 51 to 30 dB	RS analysis, Bit plane attacks
MBNS-based	(Geetha et al., 2011) [77]	VRNS	• Renowned numerical model. • Good visual quality as embedding required minimal visual distortion.	• Not robust against cropping, filtering, compression. • Limited embedding capacity with recent methods.	≈ 1 bpp	≈ 41 dB	RS analysis
MBNS-based	(W.-S. Chen et al., 2016) [79]	GMB	• Adaptive capacity based solution. • Predict the embedding capacity w.r.t to visual quality by mathematical expression. • Content adaptive multi-base embedding. • Increase security by coefficient mapping	• Greater than > 1 bpp, SPAM analysis can be successful. • High complexity.	≈ 1.46 to 3.8 bpp	≈ 50 to 35 dB	RS analysis, Histogram, SPAM analysis
GLM-based	(Muhammad et al., 2015)	GLM-MLE	• High imperceptibility. • Low computation cost by skipping the conventional encryption of the	• Limited embedding payload. • Limited evaluation.	8 KB	≈ 57 dB @ 8 KB	NA

	[85]		secret message. • Multiple levels of security. • Robustness against salt & pepper noise.				
PPM-based	(Hong, 2013) [82]	APPM	• Adaptive to visual quality vs payload. • Special embedding sequences incorporated. • Maintain the statistical image features.	• Limited security (< 0.5) SPAM based analysis. • Reference tables required.	1 to 4 bpp	≈ 52 to 35 dB	RS Histogram, SPAM analysis
PPM-based	(J. Chen, 2014) [83]	PPM-PVD	• Random embedding characteristics. • Reduce falling-off-problem of PVD. • Complex embedding order to enhance security.	• Can be steganalyzed by modern steganalysis. • Reference tables overhead.	≈ 1.3 to 2.53 bpp	≈ 50 to 42 dB	Histogram, Chi-Square
Prediction-based	(Jafar et al., 2015) [89]	MP-MPE	• Improved prediction accuracy by multiple predictors. • No overhead information required for the extraction process. • Improved embedding capacity.	• Limited capacity. • Not evaluated by any steganalysis.	90574 bits	≈ 46 dB	NA
Histogram-based	(Z. Pan et al., 2015) [93]	RDH-HS-ME	• Adaptive approach. • Localization keeps the histogram intact. • Improved capacity with less distortion.	• Low embedding capacity.	< 1 bpp	≈ 30-50 dB	Histogram
Histogram-based	(N.-K. Chen et al., 2016)[94]	RDH-HS	• Reduce the location map size. • Avoid underflow/overflow problem. • Efficient while transmission.	• No robustness discussed.	NA	NA	NA
Edge-based	(Ioannidou et al., 2012) [98]	Hybrid-Edge-ALSB	• Efficient texture evaluation by the hybrid edge detector. • Gradually embedding by sensing the edge regions. • High imperceptibility and capacity.	• Extra logging information required in decoding phase. • No steganalysis evaluated.	1.88 bpp	≈ 44 dB	NA
Edge-based	(H.-W. Tseng & Leng, 2014) [31]	ALSB	• Efficient edge detection by the hybrid fuzzy edge detector. • Adaptive LSB embedding based on block-based edge/texture computation while retaining minimum distortion by MSE.	• Not evaluated by steganalysis • No robustness. • Low embedding rate against recent methods.	≈ 2.41 bpp	≈ 38.18 dB	NA
Edge-based	(Jung & Yoo, 2014)[102]	Edge-Interpolation	• Hybrid approach with interpolation. • Improved embedding capacity.	• Resolution conflict due to interpolation, attraction for the attacker. • No steganalysis evaluation.	≈ 399,115 bits (256x256)	> 35 dB	NA
Edge-based	(Al-Dmour & Al-Ani, 2016)[95]	E-XoR coding	• Can be employed in both spatial and transform domain. • Edge adaptive embedding. • Simple implementation	• Non-adaptive thresholding overhead. • Can be attacked by textural feature analysis.	> 1 bpp	> 40 dB	Histogram, Li110D with SVM
Edge-based	(S. Sun, 2016) [103]	Canny-Huffman	• Improved visual quality and capacity • 2k correction maintains visual quality • Secret image data transform by Huffman encoding to achieve compression and security.	• Encoding complexity. • No robustness.	< 1 bpp	≈ 60 dB	Intact Histogram
Mapping-based	(Roy & Changder, 2014) [107]	LCS	• Limited modification in the cover image. • Embedding capacity can be higher than cover image. • String based mapping.	• Computationally expensive. • Auxiliary and realization information maintenance.	NA	NA	NA
Mapping-	(Alan A	Fibonacc	• Reduce secret data size up to 66% by	• Compression overhead.	465301	> 50	RS and WS

based	Abdulla et al., 2014)[108]	i 3Bit-plane mapping	SISR compression. • Fibonacci embedding reduces the visual distortion effects.	• Modern steganalysis can be attacked. • Eventually low payload.	compressed bits	dB	analysis
Pixel/ Block indicator-based	(Swain & Lenka, 2012) [112]	BI	• Block based channel indicator • Simple to implement. • Use adaptive channel selection.	• Encryption overhead. • Indicator information handling.	240632 compressed bits	> 42.75 dB	NA
Pixel/ Block indicator-based	(Mahimah & Kurinji, 2013) [113]	PI-zigzag	• Use the Zigzag direction of embedding. • Multi-mode of indicators. • Adaptive channel embedding.	• Can be steganalyzed by statistical analysis due to LSB. • Limited embedding capacity.	< 1 bpp	> 50 dB	NA
Color model	(Khan et al. 2015) [118]	HIS-M-LSB-SM	• I-plane of HSI model for embedding. • Multi-level encryption, lightweight • Specific pattern using magic LSB substitution • Reduces processing time.	• Missing of modern steganalysis evaluation.	~8 KB	~47.93 dB	NA
Color model	(Khan et al. 2016) [119]	ALSB	• Image scrambling using a light-weighted image scrambler. • Encryption of sensitive contents using iterative magic matrix-based encryption algorithm.	• Limitation of resiliency of attacks, i.e. compression • Not evaluated any conventional steganalysis	~8 KB	~52.45 dB	NA
ML-based	(Kanan & Nazeri, 2014) [122]	GA	• Adaptive embedding. • Tunable visual quality of stego image. • Lossless secret data embedding.	• Computationally expensive. • Lack of steganalysis evaluation.	0.5 to 3.95 bpp	≈ 34-55 dB	NA
ML-based	El-Emam, 2015) [123]	ANN-MPSO	• Proposed a comprehensive method. • 5 layers of security. • Improved capacity and visual quality.	• NA	Up to 12 bits/pixel (color)	> 55 dB	WFlogSv, WAM, OOB
ML-based	(El-Emam & Al-Diabat, 2015) [124]	ANN-PSO-GA	• Hybrid utilization of ANN with GA • 7 layers of security. • Reduce the number of iterations. • Efficient in training time.	• Extensive computations.	Up to 12 bits/pixel (color)	> 50 dB	Pixel difference histogram, OOB
ML-based	(Doğan, 2016) [125]	ANN-GA GA-Chaotic	• Chaotic map improved GA-based hiding. • Chaotic map results faster than random function.	• NA	NA	> 52 dB	NA
Hybrid	(Jung, 2010) [44]	PVD-ALSB	• Simple implementation. • 3-bit LSB for smooth regions, PVD by modulus function for edge region.	• Lack of steganalysis. • Low visual quality. • No robustness.	3 bpp (gray)	≈ 36.28 dB	NA
Hybrid	(Liao, Wen, & Zhang, 2011) [126]	OPAP-FPVD	• Simple implementation. • Adaptive LSB embedding based on lower (smooth) and higher (edge) levels. • Four pixels difference employing.	• Lack of testing by steganalysis. • Can be steganalyzed by modern steganalysis.	≈ 3.15 bpp (gray)	≈ 39.11 dB	NA
Hybrid	(M Khodaei & Faez, 2012) [53]	SPVD-OPAP	• Improved embedding payload. • Efficient utilization of PVD with ALSB.	• Steganalyzed at higher embedding rate by modern analysis.	> 3.04 bpp (gray)	≈ 38 dB	RS, SPAM feature analysis
Hybrid	(Y.-Y. Tsai, Chen, & Chan, 2014) [127]	LSB-PVD	• Adopted dynamic block division for adjustable embedding rate. • Fully utilized image boundary regions. • Resolve the overflow problem.	• Can be attacked by statistical and non-statistical steganalysis. • Direct embedding of secret data.	≈ 3.08 bpp (gray)	≈ 35.64 dB	NA
Hybrid	(Lu et al., 2014) [92]	RDH-DE-IN-HS	• Hybrid with interpolation. • No peak point searching.	• Limited visual quality. • No robustness.	< 1 bpp	≈ 33 dB	Histogram

			• No compression overhead.				
Hybrid	(S.-Y. Shen & Huang, 2015) [60]	IEMD-PVD	• Efficiently estimate the base digit by PVD for EMD embedding. • Exploit the Hilbert curve traversing for locality preserving and minimal distortion. • Resolve the overflow/underflow problem.	• Limited payload as compared to other EMD based methods. • Can be steganalyzed by modern analysis.	1.53 bpp	≈ 42.46 dB	RS analysis, Pixel Difference Histogram
Hybrid	(K. Wu et al., 2015) [75]	MPE-LSB-EMD	• Hybrid embedding of irreversible & reversible methods. • Balanced steganographic solution; payload vs visual quality. • Application adaptive solution.	• Can be attacked by statistical and non-statistical steganalysis. • Extensive PSNR measuring on every bit of embedding becomes computationally complex.	> 1 bpp	> 35 dB	NA
Hybrid	(Das & Kar, 2015) [115]	PI-LSB-PVD	• Color channel based indicator. • Hiding sequence controlled by pattern table indexed by secret data. • Stego-image itself retained the auxiliary information.	• Encryption header other data overhead. • Cannot resist the structural steganalysis.	2.4 bits per channel (color)	> 39 dB	Histogram analysis
Hybrid	(Hussain et al., 2016) [37]	ALSB-RMDR	• Simple implementation. • Texture complexity exploited to embed RMDR and adaptive LSB. • Closest stego-pixel selection process controls the embedding distortion.	• Less robust against non-statistical steganalysis detection attacks.	3.05 bpp (gray)	39 dB	Bit plane, RS, Difference histogram
Hybrid	(Swain, 2016) [65]	Directional-PVD-ALSB	• Three directional PVD block based embedding. • Adaptive solutions for higher visual quality and higher capacity with good quality. • Integration of ALSB with PVD.	• Step effects as histogram analysis and can expose the secret communication. • Can be attacked by SPAM features based analysis.	≈ 3.03 to 3.17 bpp (color)	≈ 40.44 to 39.29 dB	RS analysis

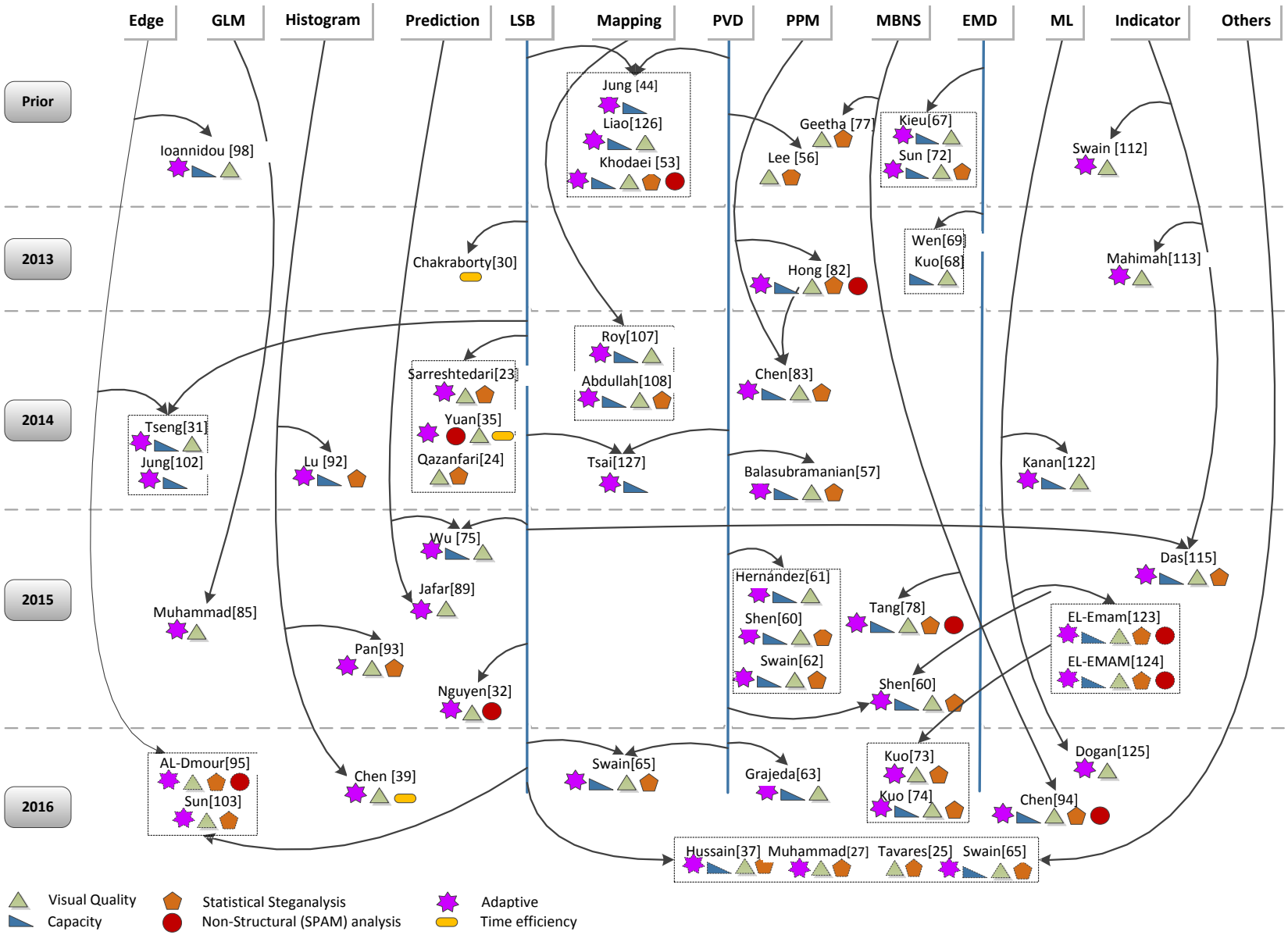

Fig. 9 Chronological orders of spatial domain steganographic techniques with their efficiencies

4. Steganography methods evaluations

The growth of image steganography also raised the significance of evaluation methods. However, the evaluation of a steganographic method is classified into visual quality, embedding payload, robustness, undetectability/security and to some extend computational complexity.

4.1 Visual quality metrics

First, the visual quality analysis, obviously the secret data embedded by any steganographic method altered the visual quality of the cover image that may not easily be noticeable by any human eye. Standard measuring techniques that may estimate or judge the visual modification levels are needed so as to decide whether the steganographic method is perceptual transparent or not. However, in literature various types of visual quality measuring metrics exist for both steganography (i.e. MSE, RMSE, PSNR, WPSNR, Q, SIMM) and watermarking (i.e. IF, NCC), the most frequent are shown in Table 4 with its respective formulas. Furthermore, its detail can be seen from respective references.

Table 4
Most common visual quality analysis matrices

Metric	*Formulas*
Mean Square Error (MSE)	$$\mathbf{MSE} = \frac{1}{\mathbf{H} \times \mathbf{W}} \sum_{i=1}^{H \times W} (\mathbf{C_i} - \mathbf{S_i})^2$$ $\mathbf{C_i}$ = cover pixel value; $\mathbf{S_i}$ = stego pixel value; $\mathbf{H} \times \mathbf{W}$: represent the height and width of cover the image. Lowest values considered good.
Root Mean Square Error (RMSE)	$$\mathbf{RMSE} = \sqrt{\mathbf{MSE}}$$
Signal to Noise Ratio (SNR)	$$\mathbf{SNR} = 10 \times \log_{10}\left(\frac{\sum_{i=1}^{H \times W}(\mathbf{C_i})^2}{\sum_{i=1}^{H \times W}(\mathbf{C_i} - \mathbf{S_i})^2}\right)$$
Peak Signal to Noise Ratio (PSNR)	$$\mathbf{PSNR} = 10 \times \log_{10}\left(\frac{\mathbf{Max}^2}{\mathbf{MSE}}\right)$$ $\mathbf{Max}$ = maximum pixel intensity value that is 255.
Weighted Peak Signal to Noise Ratio (WPSNR)	$$\mathbf{WPSNR} = 10 \times \log_{10}\left(\frac{\mathbf{max}(\mathbf{p}(\mathbf{x},\mathbf{y}))^2}{\mathbf{MSE} \times \mathbf{NVF}}\right)$$ $$\mathbf{NVF} = \mathbf{NORM}\left(\frac{1}{1 \times (\wp_{\mathbf{block}})^2}\right)$$ $\wp_{\mathbf{block}}$ = Standard deviation of luminance of the block pixel. $\mathbf{NVF}$ = Noise visibility function.
Image Quality Index (Q Index) **[128]**	$$\mathbf{Q} = \frac{4 \times (Ó_{YZ}) \times \mathbf{Y}'' \times \mathbf{Z}''}{((Ó_Y)^2 + (Ó_Z)^2)\,[(\mathbf{Y}'')^2 + (\mathbf{Z}'')^2]}$$ $$\mathbf{Y}'' = \frac{1}{N}\sum_{j=1}^{N} \mathbf{Y_j},\ \mathbf{Z}'' = \frac{1}{N}\sum_{j=1}^{N} \mathbf{Z_j}$$ $$(Ó_Y)^2 = \tfrac{1}{N-1}\sum_{j=1}^{N} (\mathbf{Y_j} - \mathbf{Y}'')^2,\ (Ó_Z)^2 = \tfrac{1}{N-1}\sum_{j=1}^{N} (\mathbf{Z_j} - \mathbf{Z}'')^2$$ $$Ó_{YZ} = \frac{1}{N-1}\sum_{j=1}^{N} (\mathbf{Y_j} - \mathbf{Y}'') \times (\mathbf{Z_j} - \mathbf{Z}'')$$
Structural Similarity Index Measure (SSIM) **[129]**	$$\mathbf{SSIM} = \left(\frac{(2 \times \mathbf{C}` \times \mathbf{S}` + \mathbf{K1})(2 \times \mathbf{M_{CS}} + \mathbf{K2})}{(\mathbf{M_C}^2 + \mathbf{M_S}^2 + \mathbf{K2}) \times (\mathbf{C}`)^2 + (\mathbf{S}`)^2 + \mathbf{K1}}\right)$$ Where $\mathbf{C}`$ and $\mathbf{S}`$ are the mean of pixels in image $\mathbf{C}$ and $\mathbf{S}$. $\mathbf{M_C}$ and $\mathbf{M_S}$ are the computed variance of all pixels in both $\mathbf{C}$ and $\mathbf{S}$ images, $\mathbf{M_{CS}}$ is the co-variance between both C and S and K1 and K2 are the constants.
Image Fidelity (IF)	$$\mathbf{IF} = 1 - \left(\frac{\sum_{i=1}^{H \times W}(\mathbf{C_i} \times \mathbf{S_i})^2}{\sum_{i=1}^{H \times W}(\mathbf{C_i})^2}\right)$$
Normalized Cross Correlation (NCC)[130]	$$\mathbf{NNC} = \left(\frac{\sum_{i=1}^{H \times W}(\mathbf{C_i} \times \mathbf{S_i})}{\sum_{i=1}^{H \times W}(\mathbf{C_i})^2}\right)$$

Average Difference (AD) **[131]**	$\mathbf{AD} = \frac{\mathbf{1}}{\mathbf{H} \times \mathbf{W}} \sum_{\mathbf{i=1}}^{\mathbf{H \times W}} (\mathbf{C_i} - \mathbf{S_i})$

4.2 Embedding capacity (EC)

Another steganographic evaluation parameter is the number of secret bits that is embedded per pixel. Ideally, these embedding bits per pixels (bpp) should be as high as possible while maintaining the visual quality and other evaluation parameter factors. It is known as the embedding capacity or embedding payload. The actual measuring of embedding payload is shown in below; W and H are the width and height of the image.

$$\text{EC (bpp)} = \frac{\text{No.of embedding bits}}{\text{W x H}}$$

4.3 Security/Undetectability

Security or undetectability is also considered as a vital evaluation parameter in steganography. Generally, steganographic approaches may suffer from various types of steganalysis detection attacks. Attackers are attracted to retrieve or even detect the existence of secret data bits from the stego-image. The detail of different steganalysis methods is discussed in next section 6.

4.4 Robustness

Usually, robustness is measured in the transform domain, but recently various spatial domain steganographic methods are considered during the designing of an algorithm. The actual term robustness refers the ability of stego-image to retain the secret data even though it is processed by different image processing operations such as noise addition, sharpening, blurring, scaling and rotations, cropping etc. As we observed from some aforementioned spatial domain steganographic techniques, it achieved a very basic level of robustness, i.e. noise addition in [27] method.

4.5 Computational complexity

The term computational complexity in steganographic approaches refers the efficiency of embedding and extraction algorithms with respect to time and operation. The low computational complexity is considered as the ideal. Normally, spatial domain based steganographic methods are simple and less computationally expensive. However, some machine learning based methods require an extensive computational ability due to the nature of embedding based on artificial intelligence algorithms, i.e. GA, ANN.

5. Steganalysis overview

Steganalysis is the art and science of exposing the secret data embedded by steganography [132]. Steganography and steganalysis always remain countermeasure of each other. Whenever an ideal steganographic approach is designed, its countermeasure steganalysis is also developed to analyze or defeat its embedding processes [133]. The actual goal of steganography is defeated if any steganalysis even detects the existence of secret data inside the embedded object. Although the embedding methods are visually transparent to the human eyes in image steganography, still detection attacks are possible in steganalysis. Generally, when steganographic method leaves or introduced various ranges of visual artifacts during embedding process that causes the unusual characteristics variations of the stego-image with respect to visual quality, further steganalysis techniques take the advantages of the unusual image characteristics to detect the existence of secret data inside the stego-image. Usually, steganalysis methods are classified into two major categories, passive steganalysis and active steganalysis [132]. The passive steganalysis identifies the existence or absence of secret data or even just to expose the specific embedding process. The active steganalysis has more depth than passive steganalysis; it can recover or modify the secret data or just to estimate the length of secret data as well. In literature both statistical and non-statistical steganalysis methods exist, some of them are designed to a specific type of embedding steganalysis techniques and others are universal steganalysis. Recently, N. Zaker et al. [134] estimates the secret data using TPVD embedding method as an example of the specific type of steganalysis. An example of universal steganalysis, G. Gul et al. [135] proposed linear dependencies of image rows/columns in local neighborhoods using singular value decomposition. In this section, we are not going in-depth of steganalysis domains, types and any other classifications that can be seen in [136]. Our focus is to discuss some test analysis and detection attacks that are employed frequently in literature for evaluating the security of any steganographic approach. The following section shows the basic tests and analysis techniques.

5.1 Visual steganalysis

The perceptual invisibility is one of the most significant requirements of any steganographic method. After embedding, some salient visual artifacts are invisible because of the limited human vision system. Therefore, different visual quality metrics are applied to estimate the visual quality measures (see section IV.*A*). Generally, most common MSE, PSNR, SSIM, Q index metrics are utilized in literature to evaluate the visual transparency.

5.2 Statistical steganalysis

Statistical steganalysis exploits the structural characteristics of images to detect unusual features that are caused by any steganographic method. There are various types of statistical analysis, i.e. histogram analysis, bit plane analysis, sample pair analysis as Chi-Square, and RS analysis methods that can easily expose the existence of secret data and even estimate secret data size.

5.2.1 Histogram based analysis

Histogram analysis is also considered as the effective testing of a stego-image. The histograms of cover and stego-images are compared to identify the pixels distribution or unusual shapes monitored due to embedding algorithm. Mostly, PVD based steganographic methods are evaluated by different variations of histogram analysis i.e. pixel difference

histogram analysis, Histogram Characteristic Function-Center Of Mass (HCF-COM) analysis [137].

5.2.2 RS steganalysis

Regular and Singular analysis known as RS analysis method was designed to detect the random LSB embedding methods [38]. The method is employed the small alteration in LSB of pixels and utilized these alterations and a discrimination function to classify these pixels into regular and singular groups. The frequency of these groups identifies the length of the secret message in stego-images. In literature, numerous steganographic techniques are evaluated by RS steganalysis to prove their security or undetectability.

5.2.3 Chi-Square analysis

The chi-square attack method is based on statistical analysis of Pairs of Values (PoVs) that are exchanged during secret data embedding. The method was designed to detect the LSB based embedding [138]. Numbers of embedding method are detected by Chi-Square steganalysis attacks.

5.2.4 Bit Plane analysis

Generally, each bit plane of an image has a correlation with other neighboring bit planes. After applying steganographic method, it may change the correlation and that can be visible to bit plane analysis. The bit plane analysis is strongly evaluated by substitution based embedding techniques.

5.3 Non- Structural steganalysis

In non-structural steganalysis, the feature extractor is utilized to model the cover image and further estimate the distortion between cover and stego-image to detect the embedding secret data. The selection of features set can be specific as steganographic oriented or universal feature set. Generally, a machine learning based classifier trains the feature set in such a way that learns the differences of features between larger dataset of cover and stego-images. The most prominent non-structural steganalysis is subtractive pixel adjacency matrix (SPAM) and spatial rich model (SRM) that are considered the better probability of steganalysis for stego image [36, 139]. The steganalyzer is utilized the support vector machine (SVM) or ensemble classifier by supervised training for classification phase. In literature, numerous types of feature based steganalysis exist [140, 141].

6. Conclusion

This paper has presented a comprehensive survey of steganographic methods in spatial domain in recent years. The basic difference between cryptography, steganography and watermarking was discussed. The architecture of steganography with different cover objects was presented and special attention was given to spatial domain based image steganography. The comparison of existing embedding methods in spatial domain was described and highlighted their advantages and challenges in the form of tabular and graphical representation. Furthermore, the most widely used steganographic performance evaluation metrics with steganalysis were discussed. Based on the aforementioned review, the following recommendations may help researchers in spatial image steganographic domain.

i. *Compound of steganography with cryptography*: Secret data encryption before embedding adds an additional layer of security. If the steganographic algorithm is exposed by steganalysis, the attacker still has to break the encryption to recover the secret data [119, 142].

ii. *Secured lightweight encryption based steganographic techniques:* As we observed most of the aforementioned steganographic techniques, it can be exposed by modern steganalysis. However, protecting secret data by conventional encryption is expensive, it is needed to design a lightweight encryption to protect secret data and is considered for resource inexpensiveness aspect [27, 108].

iii. *Integration of reversible and irreversible techniques:* Successive reversible along irreversible embedding may increase the payload and security of secret data itself. The same pixels can be recursively employed by different irreversible and reversible techniques at the same time and it will be difficult for an attacker to recover the secret data i.e. [143].

iv. *Hybrid steganographic techniques*: Multiple steganographic methods may increase the data security and even may confuse the specific steganalysis techniques. Furthermore, the strength and weakness of existing techniques may be exploited to design a better steganographic technique. Hybrid steganographic may become a good line of protection [37, 53].

v. *Location sensitive embedding:* Recently, location sensitive embedding known as adaptive steganographic techniques are evolved in order to improve payload, to minimize distortion, or to take a dynamic decision on special data during the steganographic process. This type of steganographic still needs more exploration to be mature with respect to modern steganalysis [35, 67].

vi. *Universal image Steganography:* The study shows that most existing steganographic techniques are format/type and domain dependents. Universal image steganographic techniques should be explored and designed without respect to domain/type. Furthermore, these may provide better resistance to detection attacks and even can be employed by the independence of domain limitations. In literature, limited work found in this direction i.e. [95].

vii. *Minimize the additive noise distortion function:* In steganographic techniques, it can be resisted to the modern steganalysis detection attacks. Generally, modern steganalysis computes the distinctive features of cover and stego-images to differentiate their types. Mostly, distinctive features are generated by additive noise in stego-images. Still needs some efforts to explore and minimize additive noise in designing new steganographic techniques[57, 144].

viii. *Cover-less and key-less secret extraction*: Cover-less and key-less extraction mean the ability to recover secret data from stego-image without employing the original cover image or stego-key. In case the original cover is required in extraction algorithm means that the cover image must be sent that will become suspicious. Similarly, the effort of sending stego-key may be alarming. Therefore, blind (without cover and key) extraction enhances the security of steganographic algorithm [145].

ix. *Significance of smooth texture area*: It is shown that most of the efforts are done in highly textured areas due to less suspiciousness for human vision and even for steganalysis. Meanwhile, the smooth texture areas are neglected by steganographic techniques. Can a linear or gradually variation in smooth texture areas with secret data resist the human vision and steganalysis attacks?

x. *Multi-purpose steganographic techniques*: Many steganographic algorithms were designed to perform a single-purpose, aiming either high imperceptibility or high payload. A multi-purpose steganographic style may reduce the complexity of the algorithm and simplify the implementation intricacy. Most importantly, real-time applications may take benefit from these advantages when developing multi-purpose steganographic algorithms [79].

An ideal image steganography method should provide higher embedding payload, high visual imperceptibility, and resistance against statistical and non-structural steganalysis detection attacks. But there is as such no existence of an ideal steganographic method in reality. All of the aforementioned techniques had strengths and limitations that depend on the adopted algorithm and the type of their applications. Therefore, the significance of an embedding algorithm depends on the given application.

Acknowledgments: The work was supported by the National University of Science and Technology, Islamabad, Pakistan under faculty development program abroad (grant number 0972/F008/HRD/FDP-14/); the Ministry of Education, Malaysia under the University of Malaya (High Impact Research Grant UM.C/625/1/HIR/MoE/FCSIT/17); and the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (No. 2015R1D1A1A01058019).

REFERENCE

[1] F.A. Petitcolas, R.J. Anderson, M.G. Kuhn, Information hiding-a survey, Proceedings of the IEEE, 87 (1999) 1062-1078.

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

[3] M.S. Subhedar, V.H. Mankar, Current status and key issues in image steganography: A survey, Computer science review, 13 (2014) 95-113.

[4] M.C. Trivedi, S. Sharma, V.K. Yadav, 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, ACM, 2016, pp. 84.

[5] S.N. Kishor, G.K. Ramaiah, S. Jilani, A review on steganography through multimedia, in: Research Advances in Integrated Navigation Systems (RAINS), International Conference on, IEEE, 2016, pp. 1-6.

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

[7] W. Mazurczyk, L. Caviglione, Steganography in modern smartphones and mitigation techniques, IEEE Communications Surveys & Tutorials, 17 (2015) 334-357.

[8] A.M. Alattar, O.M. Alattar, Watermarking electronic text documents containing justified paragraphs and irregular line spacing, in: Electronic Imaging 2004, International Society for Optics and Photonics, 2004, pp. 685-695.

[9] Y. Liu, T. Yang, G. Xin, Text Steganography in Chat Based on Emoticons and Interjections, Journal of Computational and Theoretical Nanoscience, 12 (2015) 2091-2094.

[10] F. Djebbar, B. Ayad, K.A. Meraim, H. Hamam, Comparative study of digital audio steganography techniques, EURASIP Journal on Audio, Speech, and Music Processing, 2012 (2012) 1-16.

[11] S.J. Murdoch, S. Lewis, Embedding covert channels into TCP/IP, in: International Workshop on Information Hiding, Springer, 2005, pp. 247-261.

[12] W. Mazurczyk, M. Smolarczyk, K. Szczypiorski, Retransmission steganography and its detection, Soft Computing, 15 (2011) 505-515.

[13] K.N. Santoso, L. Suk-Hwan, W.-J. Hwang, K. Ki-Ryong, Information Hiding in Noncoding DNA for DNA Steganography, IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, 98 (2015) 1529-1536.

[14] M.M. Sadek, A.S. Khalifa, M.G. Mostafa, Video steganography: a comprehensive review, Multimedia tools and applications, 74 (2015) 7063-7094.

[15] E. Zielińska, W. Mazurczyk, K. Szczypiorski, Trends in steganography, Communications of the ACM, 57 (2014) 86-95.

[16] M. Kharrazi, H.T. Sencar, N. Memon, Performance study of common image steganography and steganalysis techniques, Journal of Electronic Imaging, 15 (2006) 041104-041104-041116.

[17] C.-K. Chan, L.-M. Cheng, Hiding data in images by simple LSB substitution, Pattern recognition, 37 (2004) 469-474.

[18] B. Li, J. He, J. Huang, Y.Q. Shi, A survey on image steganography and steganalysis, Journal of Information Hiding and Multimedia Signal Processing, 2 (2011) 142-172.

[19] H. Yang, X. Sun, G. Sun, A high-capacity image data hiding scheme using adaptive LSB substitution, Radioengineering, 18 (2009) 509-516.

[20] Z.-H. Wang, C.-C. Chang, M.-C. Li, Optimizing least-significant-bit substitution using cat swarm optimization strategy, Information Sciences, 192 (2012) 98-108.

[21] K.-H. Jung, K.-Y. Yoo, Steganographic method based on interpolation and LSB substitution of digital images, Multimedia Tools and Applications, 74 (2015) 2143-2155.

[22] Y. Liu, X. Qu, G. Xin, A ROI-based reversible data hiding scheme in encrypted medical images, Journal of Visual Communication and Image Representation, 39 (2016) 51-57.

[23] S. Sarreshtedari, M.A. Akhaee, One-third probability embedding: a new±1 histogram compensating image least significant bit steganography scheme, IET image processing, 8 (2014) 78-89.

[24] K. Qazanfari, R. Safabakhsh, A new steganography method which preserves histogram: Generalization of LSB++, Information Sciences, 277 (2014) 90-101.
[25] J.R.C. Tavares, F.M.B. Junior, Word-Hunt: A LSB Steganography Method with Low Expected Number of Modifications per Pixel, IEEE Latin America Transactions, 14 (2016) 1058-1064.
[26] R. Amirtharajan, J.B.B. Rayappan, An intelligent chaotic embedding approach to enhance stego-image quality, Information Sciences, 193 (2012) 115-124.
[27] K. Muhammad, J. Ahmad, N.U. Rehman, Z. Jan, M. Sajjad, CISSKA-LSB: color image steganography using stego key-directed adaptive LSB substitution method, Multimedia Tools and Applications, (2016) 1-30.
[28] K. Muhammad, M. Sajjad, S.W. Baik, Dual-level security based cyclic18 steganographic method and its application for secure transmission of keyframes during wireless capsule endoscopy, Journal of medical systems, 40 (2016) 114.
[29] K. Muhammad, J. Ahmad, S. Rho, S.W. Baik, Image steganography for authenticity of visual contents in social networks, Multimedia Tools and Applications, (2017) 1-20.
[30] S. Chakraborty, A.S. Jalal, C. Bhatnagar, Secret image sharing using grayscale payload decomposition and irreversible image steganography, Journal of Information Security and Applications, 18 (2013) 180-192.
[31] H.-W. Tseng, H.-S. Leng, High-payload block-based data hiding scheme using hybrid edge detector with minimal distortion, IET Image Processing, 8 (2014) 647-654.
[32] T.D. Nguyen, S. Arch-int, N. Arch-int, An adaptive multi bit-plane image steganography using block data-hiding, Multimedia Tools and Applications, (2015) 1-27.
[33] T. Pevný, T. Filler, P. Bas, Using high-dimensional image models to perform highly undetectable steganography, in: International Workshop on Information Hiding, Springer, 2010, pp. 161-177.
[34] T. Pevny, P. Bas, J. Fridrich, Steganalysis by subtractive pixel adjacency matrix, IEEE Transactions on Information Forensics and Security, 5 (2010) 215-224.
[35] H.-D. Yuan, Secret sharing with multi-cover adaptive steganography, Information Sciences, 254 (2014) 197-212.
[36] H. Zhang, X. Ping, M. Xu, R. Wang, Steganalysis by subtractive pixel adjacency matrix and dimensionality reduction, Science China Information Sciences, 57 (2014) 1-7.
[37] M. Hussain, A.W. Abdul Wahab, N. Javed, K.-H. Jung, Hybrid Data Hiding Scheme Using Right-Most Digit Replacement and Adaptive Least Significant Bit for Digital Images, Symmetry, 8 (2016) 41.
[38] J. Fridrich, M. Goljan, R. Du, Reliable detection of LSB steganography in color and grayscale images, in: Proceedings of the 2001 workshop on Multimedia and security: new challenges, ACM, 2001, pp. 27-30.
[39] W.-L. Xu, C.-C. Chang, T.-S. Chen, L.-M. Wang, An improved least-significant-bit substitution method using the modulo three strategy, Displays, 42 (2016) 36-42.
[40] J.C. Collins, S.S. Agaian, Taxonomy for spatial domain LSB steganography techniques, in: SPIE Sensing Technology+ Applications, International Society for Optics and Photonics, 2014, pp. 912006-912006-912015.
[41] D.-C. Wu, W.-H. Tsai, A steganographic method for images by pixel-value differencing, Pattern Recognition Letters, 24 (2003) 1613-1626.
[42] K.-C. Chang, C.-P. Chang, P.S. Huang, T.-M. Tu, A novel image steganographic method using tri-way pixel-value differencing, Journal of multimedia, 3 (2008) 37-44.
[43] H.-C. Wu, N.-I. Wu, C.-S. Tsai, M.-S. Hwang, Image steganographic scheme based on pixel-value differencing and LSB replacement methods, IEE Proceedings-Vision, Image and Signal Processing, 152 (2005) 611-615.
[44] K.-H. Jung, High-capacity steganographic method based on pixel-value differencing and LSB replacement methods, The Imaging Science Journal, 58 (2010) 213-221.
[45] C.-H. Yang, S.-J. Wang, C.-Y. Weng, Capacity-raising steganography using multi-pixel differencing and pixel-value shifting operations, Fundamenta Informaticae, 98 (2010) 321-336.
[46] F. Pan, J. Li, X. Yang, Image steganography method based on PVD and modulus function, in: Electronics, Communications and Control (ICECC), 2011 International Conference on, IEEE, 2011, pp. 282-284.
[47] X. Liao, Q.-y. Wen, Z.-l. Zhao, J. Zhang, A novel steganographic method with four-pixel differencing and modulus function, Fundamenta Informaticae, 118 (2012) 281-289.
[48] X. Liao, Q. Wen, J. Zhang, Improving the Adaptive Steganographic Methods Based on Modulus Function, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 96 (2013) 2731-2734.
[49] C.-H. Yang, C.-Y. Weng, H.-K. Tso, S.-J. Wang, A data hiding scheme using the varieties of pixel-value differencing in multimedia images, Journal of Systems and Software, 84 (2011) 669-678.
[50] M. Hussain, A.W.A. Wahab, N.B. Anuar, R. Salleh, R.M. Noor, Pixel value differencing steganography techniques: Analysis and open challenge, in: Consumer Electronics-Taiwan (ICCE-TW), 2015 IEEE International Conference on, IEEE, 2015, pp. 21-22.
[51] X. Liao, S. Guo, J. Yin, H. Wang, X. Li, A.K. Sangaiah, New cubic reference table based image steganography, Multimedia Tools and Applications, (2017) 1-18.
[52] M. Hussain, A.W.A. Wahab, A.T. Ho, N. Javed, K.-H. Jung, A data hiding scheme using parity-bit pixel value differencing and improved rightmost digit replacement, Signal Processing: Image Communication, 50 (2017) 44-57.
[53] M. Khodaei, K. Faez, New adaptive steganographic method using least significant-bit substitution and pixel-value differencing, IET Image processing, 6 (2012) 677-686.
[54] H.-S. Huang, A combined image steganographic method using multi-way pixel-value differencing, in: Sixth International Conference on Graphic and Image Processing (ICGIP 2014), International Society for Optics and Photonics, 2015, pp. 944319-944319-944315.
[55] J. Mandal, D. Das, Steganography using adaptive pixel value differencing (APVD) of gray images through exclusion of overflow/underflow, arXiv preprint arXiv:1205.6775, (2012).
[56] Y.-P. Lee, J.-C. Lee, W.-K. Chen, K.-C. Chang, J. Su, C.-P. Chang, High-payload image hiding with quality recovery using tri-way pixel-value differencing, Information Sciences, 191 (2012) 214-225.
[57] C. Balasubramanian, S. Selvakumar, S. Geetha, High payload image steganography with reduced distortion using octonary pixel pairing scheme, Multimedia Tools and Applications, 73 (2014) 2223-2245.

[58] G. Liu, W. Liu, Y. Dai, S. Lian, Adaptive steganography based on block complexity and matrix embedding, Multimedia systems, 20 (2014) 227-238.
[59] S. Shen, L. Huang, Q. Tian, A novel data hiding for color images based on pixel value difference and modulus function, Multimedia Tools and Applications, 74 (2015) 707-728.
[60] S.-Y. Shen, L.-H. Huang, A data hiding scheme using pixel value differencing and improving exploiting modification directions, Computers & Security, 48 (2015) 131-141.
[61] J. Hernández-Servin, J.R. Marcial-Romero, V.M. Jiménez, H. Montes-Venegas, A Modification of the TPVD Algorithm for Data Embedding, in: Mexican Conference on Pattern Recognition, Springer, 2015, pp. 74-83.
[62] G. Swain, Adaptive pixel value differencing steganography using both vertical and horizontal edges, Multimedia Tools and Applications, (2015) 1-16.
[63] I.R. Grajeda-Marín, H.A. Montes-Venegas, J.R. Marcial-Romero, J. Hernández-Servín, G. De Ita, An Optimization Approach to the TWPVD Method for Digital Image Steganography, in: Mexican Conference on Pattern Recognition, Springer, 2016, pp. 125-134.
[64] M. Khodaei, B. Sadeghi Bigham, K. Faez, Adaptive Data Hiding, Using Pixel-Value-Differencing and LSB Substitution, Cybernetics and Systems, (2016) 1-12.
[65] G. Swain, A Steganographic Method Combining LSB Substitution and PVD in a Block, Procedia Computer Science, 85 (2016) 39-44.
[66] X. Zhang, S. Wang, Efficient steganographic embedding by exploiting modification direction, IEEE Communications Letters, 10 (2006) 781-783.
[67] T.D. Kieu, C.-C. Chang, A steganographic scheme by fully exploiting modification directions, Expert systems with Applications, 38 (2011) 10648-10657.
[68] W.-C. Kuo, S.-H. Kuo, Y.-C. Huang, Data hiding schemes based on the formal improved exploiting modification direction method, Appl. Math. Inf. Sci. Lett, 1 (2013) 1-8.
[69] K. Wen-Chung, K. Ming-Chih, A steganographic scheme based on formula fully exploiting modification directions, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 96 (2013) 2235-2243.
[70] X. Liao, Q. Wen, J. Zhang, A novel steganographic method with four-pixel differencing and exploiting modification direction, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 95 (2012) 1189-1192.
[71] X. Liao, Z. Qin, L. Ding, Data embedding in digital images using critical functions, Signal Processing: Image Communication, 58 (2017) 146-156.
[72] H.-M. Sun, C.-Y. Weng, C.-F. Lee, C.-H. Yang, Anti-forensics with steganographic data embedding in digital images, IEEE Journal on Selected areas in Communications, 29 (2011) 1392-1403.
[73] W.-C. Kuo, C.-C. Wang, H.-C. Hou, Signed digit data hiding scheme, Information Processing Letters, 116 (2016) 183-191.
[74] W.-C. Kuo, S.-H. Kuo, C.-C. Wang, L.-C. Wuu, High capacity data hiding scheme based on multi-bit encoding function, Optik-International Journal for Light and Electron Optics, 127 (2016) 1762-1769.
[75] K. Wu, W. Liao, C. Lin, T. Chen, A high payload hybrid data hiding scheme with LSB, EMD and MPE, The Imaging Science Journal, 63 (2015) 174-181.
[76] M. Afrakhteh, S. Ibrahim, Adaptive steganography scheme using more surrounding pixels, in: Computer Design and Applications (ICCDA), 2010 International Conference on, IEEE, 2010, pp. V1-225-V221-229.
[77] S. Geetha, V. Kabilan, S. Chockalingam, N. Kamaraj, Varying radix numeral system based adaptive image steganography, Information Processing Letters, 111 (2011) 792-797.
[78] M. Tang, W. Song, X. Chen, J. Hu, An image information hiding using adaptation and radix, Optik-International Journal for Light and Electron Optics, 126 (2015) 4136-4141.
[79] W.-S. Chen, Y.-K. Liao, Y.-T. Lin, C.-M. Wang, A novel general multiple-base data embedding algorithm, Information Sciences, 358 (2016) 164-190.
[80] W. Hong, T.-S. Chen, C.-W. Luo, Data embedding using pixel value differencing and diamond encoding with multiple-base notational system, Journal of Systems and Software, 85 (2012) 1166-1175.
[81] W. Hong, T.-S. Chen, A novel data embedding method using adaptive pixel pair matching, IEEE transactions on information forensics and security, 7 (2012) 176-184.
[82] W. Hong, Adaptive image data hiding in edges using patched reference table and pair-wise embedding technique, Information Sciences, 221 (2013) 473-489.
[83] J. Chen, A PVD-based data hiding method with histogram preserving using pixel pair matching, Signal Processing: Image Communication, 29 (2014) 375-384.
[84] V.M. Potdar, E. Chang, Grey level modification steganography for secret communication, in: Industrial Informatics, 2004. INDIN'04. 2004 2nd IEEE International Conference on, IEEE, 2004, pp. 223-228.
[85] K. Muhammad, J. Ahmad, H. Farman, Z. Jan, M. Sajjad, S.W. Baik, A secure method for color image steganography using gray-level modification and multi-level encryption, KSII Transactions on Internet and Information Systems (TIIS), 9 (2015) 1938-1962.
[86] Y.-H. Yu, C.-C. Chang, Y.-C. Hu, Hiding secret data in images via predictive coding, Pattern Recognition, 38 (2005) 691-705.
[87] W. Hong, T.-S. Chen, C.-W. Shiu, Reversible data hiding for high quality images using modification of prediction errors, Journal of Systems and Software, 82 (2009) 1833-1842.
[88] H.-C. Wu, H.-C. Wang, C.-S. Tsai, C.-M. Wang, Reversible image steganographic scheme via predictive coding, Displays, 31 (2010) 35-43.
[89] I.F. Jafar, K.A. Darabkh, R.T. Al-Zubi, R.A. Al Na'mneh, Efficient reversible data hiding using multiple predictors, The Computer Journal, (2015) bxv067.
[90] P. Tsai, Y.-C. Hu, H.-L. Yeh, Reversible image hiding scheme using predictive coding and histogram shifting, Signal Processing, 89 (2009) 1129-1143.
[91] X. Li, W. Zhang, X. Gui, B. Yang, A novel reversible data hiding scheme based on two-dimensional difference-histogram modification, IEEE Transactions on Information Forensics and Security, 8 (2013) 1091-1100.
[92] T.-C. Lu, C.-C. Chang, Y.-H. Huang, High capacity reversible hiding scheme based on interpolation, difference expansion, and histogram shifting, Multimedia Tools and Applications, 72 (2014) 417-435.
[93] Z. Pan, S. Hu, X. Ma, L. Wang, Reversible data hiding based on local histogram shifting with multilayer embedding, Journal of Visual Communication and Image Representation, 31 (2015) 64-74.
[94] N.-K. Chen, C.-Y. Su, C.-Y. Shih, Y.-T. Chen, Reversible watermarking for medical images using histogram shifting with location map reduction, in: 2016 IEEE International

Conference on Industrial Technology (ICIT), IEEE, 2016, pp. 792-797.
[95] H. Al-Dmour, A. Al-Ani, A steganography embedding method based on edge identification and XOR coding, Expert systems with Applications, 46 (2016) 293-306.
[96] W. Luo, F. Huang, J. Huang, Edge adaptive image steganography based on LSB matching revisited, IEEE Transactions on information forensics and security, 5 (2010) 201-214.
[97] W.-J. Chen, C.-C. Chang, T.H.N. Le, High payload steganography mechanism using hybrid edge detector, Expert Systems with applications, 37 (2010) 3292-3301.
[98] A. Ioannidou, S.T. Halkidis, G. Stephanides, A novel technique for image steganography based on a high payload method and edge detection, Expert systems with applications, 39 (2012) 11517-11524.
[99] N. Grover, A. Mohapatra, Digital image authentication model based on edge adaptive steganography, in: 2013 2nd International Conference on Advanced Computing, Networking and Security, IEEE, 2013, pp. 238-242.
[100] R. Roy, A. Sarkar, S. Changder, Chaos based edge adaptive image steganography, Procedia Technology, 10 (2013) 138-146.
[101] M.R. Modi, S. Islam, P. Gupta, Edge based steganography on colored images, in: International Conference on Intelligent Computing, Springer, 2013, pp. 593-600.
[102] K.-H. Jung, K.-Y. Yoo, Data hiding using edge detector for scalable images, Multimedia tools and applications, 71 (2014) 1455-1468.
[103] S. Sun, A novel edge based image steganography with 2 k correction and Huffman encoding, Information Processing Letters, 116 (2016) 93-99.
[104] R.-Z. Wang, Y.-S. Chen, High-payload image steganography using two-way block matching, IEEE Signal Processing Letters, 13 (2006) 161-164.
[105] M.A. Al-Husainy, Image steganography by mapping pixels to letters, Journal of Computer science, 5 (2009) 33.
[106] A. Nag, S. Ghosh, S. Biswas, D. Sarkar, P.P. Sarkar, An image steganography technique using X-box mapping, in: Advances in Engineering, Science and Management (ICAESM), 2012 International Conference on, IEEE, 2012, pp. 709-713.
[107] R. Roy, S. Changder, Image realization steganography with LCS based mapping, in: Contemporary Computing (IC3), 2014 Seventh International Conference on, IEEE, 2014, pp. 218-223.
[108] A.A. Abdulla, H. Sellahewa, S.A. Jassim, Stego quality enhancement by message size reduction and fibonacci bit-plane mapping, in: International Conference on Research in Security Standardisation, Springer, 2014, pp. 151-166.
[109] A.A. Abdulla, H. Sellahewa, S.A. Jassim, Steganography based on pixel intensity value decomposition, in: SPIE Sensing Technology+ Applications, International Society for Optics and Photonics, 2014, pp. 912005-912005-912009.
[110] A.A.-A. Gutub, Pixel indicator technique for RGB image steganography, Journal of Emerging Technologies in Web Intelligence, 2 (2010) 56-64.
[111] N. Tiwari, M. Shandilya, Secure RGB image steganography from pixel indicator to triple algorithm-an incremental growth, International Journal of Security and Its Applications, 4 (2010) 53-62.
[112] G. Swain, S.K. Lenka, A better RGB channel based image steganography technique, in: Global Trends in Information Systems and Software Applications, Springer, 2012, pp. 470-478.
[113] P. Mahimah, R. Kurinji, Zigzag pixel indicator based secret data hiding method, in: Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference on, IEEE, 2013, pp. 1-5.
[114] V. Thanikaiselvan, S. Subashanthini, R. Amirtharajan, PVD based steganography on scrambled RGB cover images with pixel indicator, Journal of Artificial Intelligence, 7 (2014) 54.
[115] P. Das, N. Kar, ILSB: Indicator-Based LSB Steganography, in: Intelligent Computing, Communication and Devices, Springer, 2015, pp. 489-495.
[116] K. Muhammad, J. Ahmad, N.U. Rehman, Z. Jan, R.J. Qureshi, A secure cyclic steganographic technique for color images using randomization, arXiv preprint arXiv:1502.07808, (2015).
[117] K. Muhammad, J. Ahmad, H. Farman, M. Zubair, A novel image steganographic approach for hiding text in color images using HSI color model, arXiv preprint arXiv:1503.00388, (2015).
[118] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, S.W. Baik, Image steganography using uncorrelated color space and its application for security of visual contents in online social networks, Future Generation Computer Systems, (2016).
[119] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, S.W. Baik, A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image, Multimedia Tools and Applications, 75 (2016) 14867-14893.
[120] L.-Y. Tseng, Y.-K. Chan, Y.-A. Ho, Y.-P. Chu, Image hiding with an improved genetic algorithm and an optimal pixel adjustment process, in: 2008 Eighth International Conference on Intelligent Systems Design and Applications, IEEE, 2008, pp. 320-325.
[121] M. Khodaei, K. Faez, Image hiding by using genetic algorithm and LSB substitution, in: International Conference on Image and Signal Processing, Springer, 2010, pp. 404-411.
[122] H.R. Kanan, B. Nazeri, A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm, Expert Systems with Applications, 41 (2014) 6123-6130.
[123] N.N. El-Emam, New data-hiding algorithm based on adaptive neural networks with modified particle swarm optimization, Computers & Security, 55 (2015) 21-45.
[124] N.N. El-Emam, M. Al-Diabat, A novel algorithm for colour image steganography using a new intelligent technique based on three phases, Applied Soft Computing, 37 (2015) 830-846.
[125] Ş. Doğan, A new data hiding method based on chaos embedded genetic algorithm for color image, Artificial Intelligence Review, 46 (2016) 129-143.
[126] X. Liao, Q.-y. Wen, J. Zhang, A steganographic method for digital images with four-pixel differencing and modified LSB substitution, Journal of Visual Communication and Image Representation, 22 (2011) 1-8.
[127] Y.-Y. Tsai, J.-T. Chen, C.-S. Chan, Exploring LSB Substitution and Pixel-value Differencing for Block-based Adaptive Data Hiding, IJ Network Security, 16 (2014) 363-368.
[128] Z. Wang, A.C. Bovik, A universal image quality index, IEEE signal processing letters, 9 (2002) 81-84.
[129] Z. Wang, A.C. Bovik, H.R. Sheikh, E.P. Simoncelli, Image quality assessment: from error visibility to structural similarity, IEEE transactions on image processing, 13 (2004) 600-612.
[130] I. Avcibas, N. Memon, B. Sankur, Steganalysis using image quality metrics, IEEE transactions on Image Processing, 12 (2003) 221-229.
[131] R. Kumar, M. Rattan, Analysis of various quality metrics for medical image processing, International Journal of Advanced

Research in Computer Science and Software Engineering, 2 (2012) 137-144.
[132] N.F. Johnson, S. Jajodia, Steganalysis: The investigation of hidden information, in: Information Technology Conference, 1998. IEEE, IEEE, 1998, pp. 113-116.
[133] H. Wang, S. Wang, Cyber warfare: steganography vs. steganalysis, Communications of the ACM, 47 (2004) 76-82.
[134] N. Zaker, A. Hamzeh, A novel steganalysis for TPVD steganographic method based on differences of pixel difference histogram, Multimedia Tools and Applications, 58 (2012) 147-166.
[135] G. Gul, F. Kurugollu, SVD-based universal spatial domain image steganalysis, IEEE Transactions on Information Forensics and Security, 5 (2010) 349-353.
[136] A. Nissar, A. Mir, Classification of steganalysis techniques: A study, Digital Signal Processing, 20 (2010) 1758-1770.
[137] A.D. Ker, Steganalysis of LSB matching in grayscale images, IEEE signal processing letters, 12 (2005) 441-444.
[138] A. Westfeld, A. Pfitzmann, Attacks on steganographic systems, in: International workshop on information hiding, Springer, 1999, pp. 61-76.
[139] J. Fridrich, J. Kodovsky, Rich models for steganalysis of digital images, IEEE Transactions on Information Forensics and Security, 7 (2012) 868-882.
[140] T. Denemark, V. Sedighi, V. Holub, R. Cogranne, J. Fridrich, Selection-channel-aware rich model for steganalysis of digital images, in: 2014 IEEE International Workshop on Information Forensics and Security (WIFS), IEEE, 2014, pp. 48-53.
[141] V. Sedighi, R. Cogranne, J. Fridrich, Content-adaptive steganography by minimizing statistical detectability, IEEE Transactions on Information Forensics and Security, 11 (2016) 221-234.
[142] C.-W. Shiu, Y.-C. Chen, W. Hong, Encrypted image-based reversible data hiding with public key cryptography from difference expansion, Signal Processing: Image Communication, 39 (2015) 226-233.
[143] M. Hussain, A.W.A. Wahab, N. Javed, K.-H. Jung, Recursive Information Hiding Scheme Through LSB, PVD Shift, and MPE, IETE Technical Review, (2016) 1-11.
[144] B. Li, M. Wang, J. Huang, X. Li, A new cost function for spatial image steganography, in: Image Processing (ICIP), 2014 IEEE International Conference on, IEEE, 2014, pp. 4206-4210.
[145] G. Paul, I. Davidson, I. Mukherjee, S. Ravi, Keyless Steganography in Spatial Domain Using Energetic Pixels, in: ICISS, Springer, 2012, pp. 134-148.