IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 14, 2019, accepted December 5, 2019, date of publication December 17, 2019,
date of current version December 31, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2960254

An Adaptive Image Steganography Method Based on Histogram of Oriented Gradient and PVD-LSB Techniques

MOHAMED ABDEL HAMEED[1], **M. HASSABALLAH**[2], **SALEH ALY**[3,4], **AND ALI ISMAIL AWAD**[5,6,7], **(Senior Member, IEEE)**

[1]Department of Computer Science, Faculty of Computers and Information, Luxor University, Luxor 85951, Egypt
[2]Department of Computer Science, Faculty of Computers and Information, South Valley University, Qena 83523, Egypt
[3]Department of Electrical Engineering, Faculty of Engineering, Aswan University, Aswan 81542, Egypt
[4]Department of Information Technology, College of Computer and Information Sciences, Majmaah University, Majma'ah 11952, Saudi Arabia
[5]Department of Computer Science, Electrical and Space Engineering, Luleå University of Technology, 971 87 Luleå, Sweden
[6]Electrical Engineering Department, Faculty of Engineering, Al-Azhar University at Qena, Qena 83513, Egypt
[7]Centre for Security, Communications and Network Research, University of Plymouth, Plymouth PL4 8AA, U.K.

Corresponding author: M. Hassaballah (m.hassaballah@svu.edu.eg)

This work was supported by the Deanship of Scientific Research at Majmaah University under Project RGP-2019-24.

ABSTRACT Pixel value differencing (PVD) and least significant bit substitution (LSB) are two widely used schemes in image steganography. These two methods do not consider different content in a cover image for hiding the secret data. The content of most digital images has different edge directions in each pixel, and the local object shape or appearance is mostly characterized by the distribution of its intensity gradients or edge directions. Exploiting these characteristics for embedding various secret information in different edge directions will eliminate sequential embedding and improve robustness. Thus, a histogram of oriented gradient (HOG) algorithm is proposed to find the dominant edge direction for each 2 × 2 block of cover images. Blocks of interest (BOIs) are determined adaptively based on the gradient magnitude and angle of the cover image. Then, the PVD algorithm is used to hide secret data in the dominant edge direction, while the LSB substitution is utilized in the other two remaining pixels. Extensive experiments using various standard images reveal that the proposed scheme provides high embedding capacity and better visual quality compared with several other PVD- and LSB-based methods. Moreover, it resists various steganalysis techniques, such as pixel difference histogram and RS analysis.

INDEX TERMS Data hiding, steganography, pixel value differencing, least significant bit, histogram of oriented gradient, HOG.

I. INTRODUCTION

Recently, information hiding has been considered one of the most important issues in human communities because of the increased and urgent demand for data transmission over social networks. The common use of the Internet and cloud services in transmission of a large amount of data over open networks and insecure channels exposes private and secret data to serious situations [1]. Consequently, ensuring that information transmission over the Internet is safe and secure has become crucial [2]. To keep an unauthorized person away from the transmitted information, a variety of data hiding schemes have been introduced [3]; steganography is one of them [4], [5]. Steganography is a mechanism for covert communication that aims to hide secret messages into an ordinary message without drawing suspicion or achieving the least possible statistical detectability. Steganography techniques can be applied for hiding secret information on various types of digital media, such as images, video and audio data, and text [6].

In the digital image domain, several steganography approaches have been proposed. Most of these approaches can hide data bits in the spatial domain within the pixel values of images. In other words, to embed the secret data

The associate editor coordinating the review of this manuscript and approving it for publication was Chien-Ming Chen.

in an image, we directly modify pixel intensity in some way. The majority of these spatial domain steganography approaches are content adaptive [7], [8] in the sense that they perform embedding changes mainly in complex regions of the cover image, which are hard to model by steganalysts [9]. As steganography faces several challenges posed by steganalysis, intending to detect the traces of hidden data, the essential objectives in image steganography are to provide large embedding capacity, good visual quality, and more security against the steganalysis attackers [10].

In this regard, spatial domain image steganography approaches are often suitable for various applications due to their high embedding capacity and low computational complexity. One important steganography scheme in the spatial domain is the PVD method and its variants [11]. Mainly, the PVD-based methods are designed to exploit the characteristics of the human visual system (HVS) for embedding secret data [12], [13], where it utilizes the difference between two consecutive image pixels. The PVD method targets the smooth and edged areas of cover images for low and large embedding capacities, respectively. Thus, it improves visual quality and security [14]. Another spatial domain method is least significant bit (LSB) substitution, which simply replaces the LSBs of the cover image by the secret data bits [15]. The PVD and LSB substitution methods are still widely used because of their large embedding capacity and low computational complexity [16].

The main goal of this study is to hide text as a binary secret message within a cover image in the sense that the image is used to provide safe communication and conceals confidential data within it, where an unauthorized receiver cannot suspect any existence of confidential information. To achieve this goal, this paper proposes a new adaptive steganography method for grayscale images based on finding a set of blocks of interest (BOI) to hide secret data bits in their dominant edge directions. To find the embedding direction in each block, the gradient magnitude is thresholded using an adaptively selected threshold value (T). The embedding regions can be increased or decreased according to the length of the secret message via changing the threshold value (T) and the number of K-bits used in the LSB embedding algorithm. For lower embedding rates, sharper edge regions can only be considered. When the required embedding rate increases, more edge regions can be selected adaptively for data hiding by adjusting the two key parameters (T, K) of the proposed method. A set of experiments is carried out to analyze and test the proposed method with respect to embedding capacity, visual imperceptibility, and security. The visual quality of the stego image is evaluated using two different metrics: the peak signal-to-noise ratio (PSNR) and universal image quality index (Q) [17]. In summary, the main contributions of this work as follows.

- Most kinds of PVD- and LSB-based methods carried out in the field of steganography to date are described and summarized comprehensively. We find that these methods do not consider different content of the cover image for hiding the secret data.
- A new method is proposed based on PVD and LSB, considering the content of digital images, where they have different edge directions in each pixel, and local object shape or appearance is mostly characterized by the distribution of their intensity gradients or edge directions.
- In the proposed method, a histogram of oriented gradient algorithm is introduced to find the dominant edge direction for each 2×2 block of the cover image. Blocks of interest (BOIs) are determined adaptively based on the gradient magnitude and angle of the cover image.
- The PVD algorithm is utilized to hide secret data in the dominant edge direction, while the LSB substitution is utilized in the other two remaining pixels.
- Extensive experiments using a set of standard images reveal that the proposed scheme provides high embedding capacity and better visual quality compared with several PVD- and LSB-based methods. Moreover, it resists steganalysis techniques such as pixel difference histogram and RS analysis.

The rest of the paper is organized as follows. Section II discuses previous studies in image steganography, especially those related to the PVD and LSB methods. Section III presents details of the proposed image steganography method. Experimental results along with analysis and comparisons of the proposed method with the existing PVD and LSB-based methods are provided in Section IV. Finally, conclusions are drawn in Section V.

II. RELATED WORK

A large number of image steganography methods in the spatial domain are introduced in the literature for embedding data securely [18]–[27]. Most of the existing methods in the spatial domain are based on either least significant bit (LSB) substitution [15] or pixel value differencing (PVD) [11]. The LSB-based methods depend on replacing the K least significant bits of each pixel in the cover image with secret k-bits from the secret message. The parameter K used in the LSB embedding scheme is chosen according to the size of the secret message; i.e., a large message requires a large K, while a small message can be embedded using a small K. The major drawback of the traditional LSB algorithm is its uniform embedding at smooth and edge regions [28]. Thus, the visual quality of the cover image is dramatically degraded with increasing K bits. Additionally, the embedding algorithm might be insecure through varied forms of steganalysis attacks [29].

To overcome the limitations of the LSB technique, Mielikainen [30] and Li *et al.* [31] modified the least significant bit (LSB) matching. In [32], to improve the quality of the stego image, a modified method called inverted pattern (IP) LSB substitution was proposed, where each section of secret data was tested to be inverted or noninverted before embedding. Another improved version of the

LSB technique was proposed in [33], which can choose the embedding regions according to the size of the secret data and the difference between two consecutive pixels in the cover image. Deshmukh and Pattewar [34] presented an edge adaptive steganography method based on the LSB substitution, where the secret data were embedded in sharp edge regions of images using an adaptive scheme and the difference between two adjacent image pixels. Muhammad *et al.* [35] proposed a magic least significant bit substitution method (M-LSB-SM) to overcome limitations in terms of security and imperceptibility. However, attempts were made to increase the payload while preserving the reasonable visual quality of stego images in LSB-based methods. For instance, using wavelet packet transformation and a neutrosophic set, a high payload steganography approach was proposed in [36]. The embedding of secret data was performed using the LSB substitution method. The capacity of the hidden secret data improved and provided an acceptable stego image quality, but it has a major drawback of computational complexity in runtime.

Using different directions, Wu and Tsai [11] proposed the PVD method based on the basic principle of human vision systems (HVS) for hiding data in grayscale images, where the cover image was partitioned into 1 × 2 blocks and edge regions in images were employed for hiding more data compared to less embedding data in smooth areas of the cover images. Although this method recovers the low visual quality problems arising from the LSB, its embedding capacity is lower than that of the LSB. To provide better image quality and large embedding capacity, Hong [37] introduced a modified approach using the concept of pixel value differencing combined with a patched reference table (PVD-PRT). Pradhan *et al.* [38] suggested an adaptive PVD scheme with two pixel blocks sizes: 2 × 3 and 3 × 2. Swain [39] proposed a PVD-based technique including two schemes: adaptive and nonadaptive with 1 × 2 overlapping pixel blocks. The adaptive model considers embedding and extraction an adaptive quantization range table and modular arithmetic, while the nonadaptive model considers a fixed quantization range table and addition/difference mechanism.

In the same context, a number of adaptive tri-way PVD methods with block sizes of 2 × 2 was introduced to increase the embedding capacity [40], [41]. A steganography method was suggested by Lee and Chen [42] to achieve high embedding capacity using a modulus function. Another modification using a combination of parity-bit pixel value differences and improved rightmost digit replacement was introduced in [14]. Most of the previously explained PVD-based methods suffer from artificial artifacts resulting from increasing embedding capacity, which is invisible to the human eye but noticeable for steganalysts. A recently proposed method in [43] is a further improvement of the previous adaptive methods. Instead of selecting one common embedding direction for all pixels in the cover image, this method finds different directions for each block to hide secret data. The selective property of the proposed method not only improves the visual quality of the stego image but also increases the embedding capacity. Additionally, Li and He [25] proposed a data hiding algorithm using PVD, modulus function and particle swarm optimization to improve embedding capacity and visual quality.

In several other works [44]–[47], a combination of the pixel value differences and adaptive LSB substitution was also introduced to obtain better embedding capacity with a minimum level of distortion and maximum security. For instance, Yang *et al.* [48] presented an adaptive LSB method based on the concept of pixel value differencing, which increases the embedding capacity while maintaining the high quality of the stego image. In [49], the payload was enhanced by dividing the pixels into three nonoverlapping blocks; then, the LSB with optimal pixel adjustment process was applied to the center pixel, while the PVD scheme was employed for embedding on the remaining two pixels of each block. In [50], the pixel difference histogram analysis was avoided by using a combination of the LSB substitution and PVD and by applying the exploiting modification directions (EMD) [51] on 2 × 2 and 3 × 3 pixel blocks.

Despite the fact that the abovementioned methods improved the embedding capacity and security against the histogram analysis, they are subjected to undetectability against the RS steganalysis and incapable of ensuring large embedding capacity with the typical visual quality of stego images. Consequently, there is still room for further research on this topic, especially for finding proper embedding locations in the cover image utilized for imperceptible stego images. We believe that edges and their neighborhood pixels are the most suitable locations for the task.

III. THE PROPOSED STEGANOGRAPHY METHOD

The proposed adaptive steganography scheme consists of two algorithms, one for embedding shown in Fig. 1 and the other for extracting secret data, which is shown in Fig. 2. The embedding algorithm is based on selecting a set of blocks of interest (BOI) using the HOG algorithm to hide secret data in the cover image. HOG computation is considered the key step of the proposed method in which the gradient magnitude and angle are calculated from horizontal and vertical gradient images of the input cover image. Then, the gradient angle is quantized to make all angles fall within a specified fixed range $(1, 2, 3, 4, 5)$, which helps to handle small angle variations. To find the dominant edge direction for each block, the histogram of oriented gradient is calculated over a 2 × 2 block size in the quantized angle image. The block of interest can be selected by thresholding the dominant magnitude value for each block using an adaptive threshold value. For each BOI, we embed secret data in the dominant edge direction using the PVD algorithm and LSB substitution for embedding the other two pixels. The threshold value is computed adaptively according to the length of the secret message to absorb the whole secret message in the candidate blocks of the cover image. The main steps of the proposed

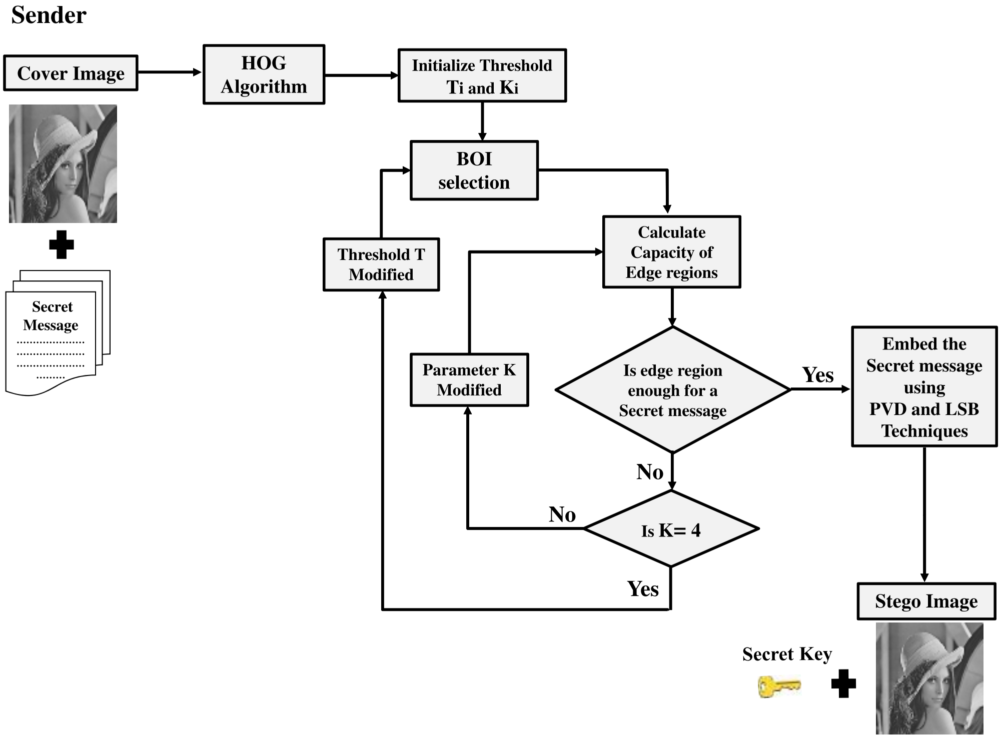

Sender
Cover Image
Secret Message
HOG Algorithm
Initialize Threshold Ti and Ki
BOI selection
Threshold T Modified
Calculate Capacity of Edge regions
Parameter K Modified
Is edge region enough for a Secret message
Yes
Embed the Secret message using PVD and LSB Techniques
No
No
Is K= 4
Yes
Stego Image
Secret Key

FIGURE 1. Flowchart of steps for embedding a secret message using the proposed method.

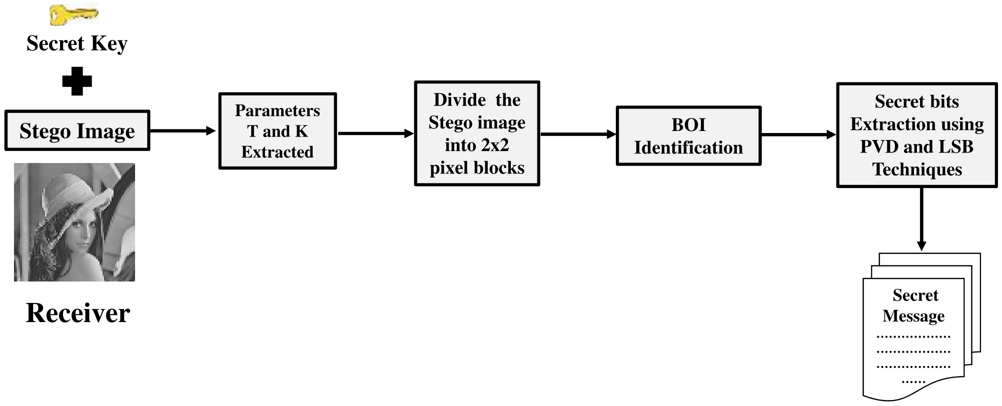

Secret Key
Stego Image
Receiver
Parameters T and K Extracted
Divide the Stego image into 2x2 pixel blocks
BOI Identification
Secret bits Extraction using PVD and LSB Techniques
Secret Message

FIGURE 2. Flowchart of steps for extracting the secret message using the proposed method.

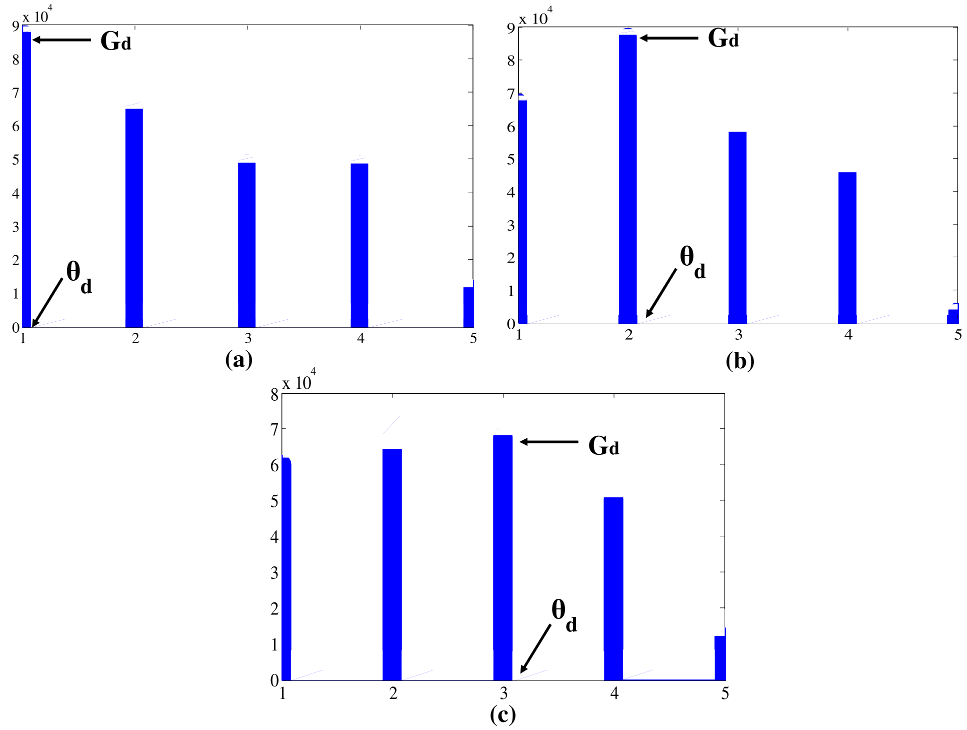
method for the embedding phase and extraction phase are explained in the following.

A. HISTOGRAM OF ORIENTED GRADIENT (HOG)

As a successful edge-based local shape descriptor, HOG [52] was originally used to solve the object detection problem by describing local edge information of objects. A similar idea of HOG is utilized here to find the dominant gradient direction for each block in the cover image. The gradient magnitude values for each pixel are accumulated depending on their corresponding angle. Then, to find the dominant angle θ_d for each block in the cover image, we select the gradient angle corresponding to the maximum accumulated gradient magnitude value G_d as shown in Fig. 3. Based on these criteria, the steps of the algorithm used to find the dominant edge direction are summarized in Algorithm 1. An illustration example of a grayscale image containing different edge directions for each BOI is given in Fig. 4. The three edge directions, horizontal, vertical and diagonal, almost exist and are scattered along all pixels of the cover image.

B. BLOCK OF INTEREST (BOI)

Block of interest (BOI) can be defined as a block that has an accumulated gradient magnitude value greater than a selected



(a)

(b)

(c)

FIGURE 3. Maximum value of G_d and its corresponding θ_d at three dominant directions: (a) Horizontal direction. (b) Diagonal direction. (c) Vertical direction.

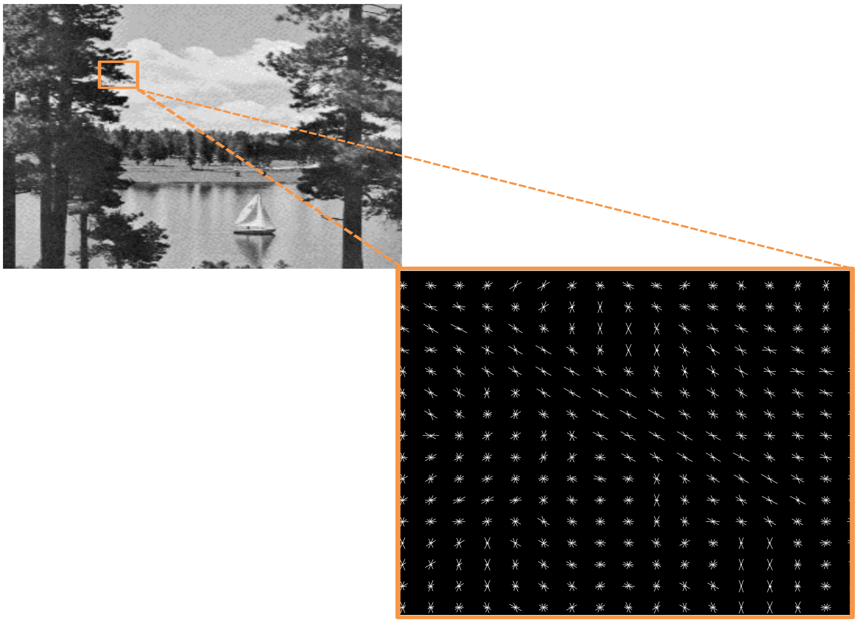


FIGURE 4. Example of BOIs for the Lake cover image containing different edge directions.

threshold parameter (T). To find the BOI in the cover image, the dominant gradient magnitude value for each block is computed by finding the maximum value of the histogram of accumulated gradient magnitude and its associated gradient angle. To avoid blocks containing weak edge information or lying in the smooth regions, the maximum gradient magnitude is thresholded using the T value. This value is adaptively adjusted on the basis of secret message size in such a way that an efficient number of edges in the cover image is selected to embed the whole secret message. An appropriate threshold

Algorithm 1 HOG Computation Steps to Find the BOI During the Embedding Process

```
Input: Input cover image $I$ of size M×N
Output: Histogram of oriented gradients $H$
1: Calculate the gradient of input image in x- and y-directions.
       $$G_x = I * K_x, \quad G_y = I * K_y \quad (1)$$
   where $K_x = [-1 \;\; 1]$, and $K_y = [-1 \;\; 1]^T$
2: The magnitude and edge direction are computed using formula:
       $$G = \sqrt{G_x^2 + G_y^2}, \quad \theta = tan^{-1}(\frac{G_y}{G_x}) \quad (2)$$
3: Normalize the magnitude value to be within the range of $[0 - 1]$ using formula:
       $$G_n = \frac{G}{\max(G)} \quad (3)$$
4: Quantize the angle of edge direction $\theta_q$ according to the quantization ranges given in Fig 5.
5: Divide cover image into a set of $2 \times 2$ nonoverlapping blocks. Then, calculate the HOG using
       $$H_{i,j} = \sum_{x,y \in B(i,j)} s(\theta_q = Q) \quad (4)$$
   where $i = 0, 1, \ldots, M-1$, $j = 0, 1, \ldots, N-1$ and $Q = \{1, 2, 3, 4, 5\}$ are the quantized angle labels and
       $$s(x) = \begin{Bmatrix} G_m, & x \;\; is \;\; true \\ 0, & x \;\; is \;\; false \end{Bmatrix} \quad (5)$$
   where $s(x)$ is an indicator function and $H_{i,j}$ is a function used to accumulate gradient magnitude $G_m$ inside each block $B(i,j)$
```

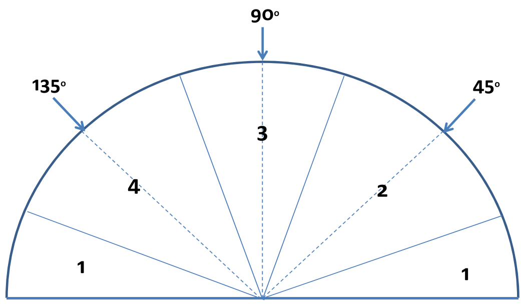


FIGURE 5. Angle quantization range and directions.

value is adaptively searched to find a sufficient number of edge pixels. The threshold value T lies between two values 0 and 1. Let the number of edge pixels returned by the HOG edge detector after thresholding equal N_e. It is quite possible that the number of edge pixels N_e may be less or more than the required number for a specific secret message S_m. Threshold T and K values are gradually increased such that it returns the total number of pixels N_e, which can absorb all embedded bits.

C. EMBEDDING AND EXTRACTING ALGORITHMS

The first stage of the proposed embedding algorithm applies the previously explained HOG scheme on the cover image to determine the BOIs used for embedding. We assume that the top-left pixel in each BOI is a reference edge pixel and that the other pixel is selected according to the dominant edge direction. This direction can be one of three directions, horizontal, vertical or diagonal, according to the maximum value of the histogram of accumulated gradient magnitude, as shown in Fig. 4. For each 2×2 block, two edge pixels are embedded using the PVD method in the dominant direction, while the other two remaining pixels are embedded using the LSB substitution method parametrized by the K value. After the process of embedding the secret message is performed, a secret key results with two parameters (T, K). This key is used later in the extraction phase. The combination of the two data hiding techniques, PVD [11] and LSB [15] in each block is very useful for increasing embedding capacity while good visual quality is acquired. The steps summarized in Algorithm 2 are applied for embedding the input grayscale image. In the extraction phase, the hidden secret data bits can be extracted from the stego image following the pipeline shown in Fig. 2 and via applying steps of the extracting algorithm given in Algorithm 3. Figs. 6 and 7 show an example for embedding and extraction procedures, respectively.

IV. EXPERIMENTAL RESULTS

In this section, we investigate the performance of the proposed steganography scheme by carrying out several experiments. The embedding capacity, visual quality, and security are considered performance measures. The embedding capacity is an important evaluation factor that represents the total number of secret bits that can be embedded in each pixel. The proposed scheme is implemented and tested using MATLAB, and the standard 8-bit grayscale images from the UCID database [53] with a size of 512×512 pixels shown in Fig. 8 are used as cover images.

A. ANALYSIS OF STEGO IMAGES VISUAL QUALITY

In fact, embedding a secret message in a cover image alters it, and there may be some changes in pixel values that affect the visual quality of the stego image. These changes and modifications must be examined since they directly affect the imperceptibility of the final appearance of the stego image. To this end, the peak-signal-to-noise ratio (PSNR) metric is used for measuring the visual quality of the stego image. PSNR is calculated to describe the distortion of the cover images after embedding secret data and evaluating the efficiency of the proposed method. The PSNR measured in decibels (dB) is used as a statistical image quality estimation level to measure the distortion between the cover and stego image. If the PSNR value is greater than 30 dB, the distortion

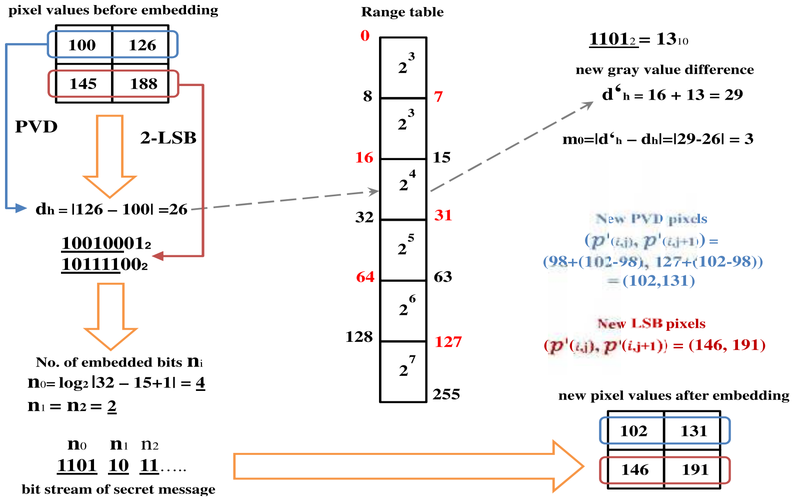


FIGURE 6. Example of the embedding process of the proposed method where T=0.001 and K=2.

```
Algorithm 2 Embedding Algorithm
Input: C cover image sized with $M \times N$ and secret message Sm sized with $N$.
Output: S stego image with size $M \times N$.
  1) Initialize threshold $T$ and $K$ values.
  2) Divide the cover image $C$ into nonoverlapping blocks of $2 \times 2$ pixels.
  3) Calculate HOG for the $C$ image by applying the steps in Algorithm1.
  4) Find the block of interest (BOI), as explained in Section III-B.
  5) For each BOI of the cover image, calculate the difference values for the two edge pixels using one of the following:
       $d_h = |p_{i,j} - p_{i,j+1}|,$
       $d_v = |p_{i,j} - p_{i+1,j}|,$
       $d_d = |p_{i,j} - p_{i+1,j+1}|$        (6)
     where $d_h$, $d_v$ and $d_d$ represent pixel value differences in the horizontal, vertical and diagonal embedding directions, respectively.
  6) Apply the PVD technique to hide secret data in the first two edge pixels of each BOI to modify pixel values according to its dominant angle direction into $(p'_{i,j}, p'_{i,j+1})$, $(p'_{i,j}, p'_{i+1,j})$ and $(p'_{i,j}, p'_{i+1,j+1})$.
  7) For the other two remaining pixels, apply the LSB embedding technique to hide $k$ bits.
  8) Check whether the calculated embedding capacity is less than the required length of the secret message, modify $T$ and $k$ values, then repeat steps (4-8). Otherwise, go to step 9.
  9) Generate stego image $S$ and the secret key.
```

```
Algorithm 3 Extracting Algorithm
Input: S stego image sized with $M \times N$.
Output: Secret message Sm sized with $N$.
  1) Extract the parameter $T$ and $k$ from the secret key.
  2) Calculate HOG for stego image $S$ by applying the steps in Algorithm 1.
  3) Divide stego image $S$ into nonoverlapping blocks of $2 \times 2$ pixels.
  4) For each block in the BOI, the secret bits are extracted using the PVD technique in the dominant edge direction, while the data in the other two pixels are extracted by the LSB technique.
  5) Repeat step 4 for the other two directions, vertical and diagonal, until all secret bits are extracted.
  6) Obtain the secret message via concatenating these extracted bits.
```

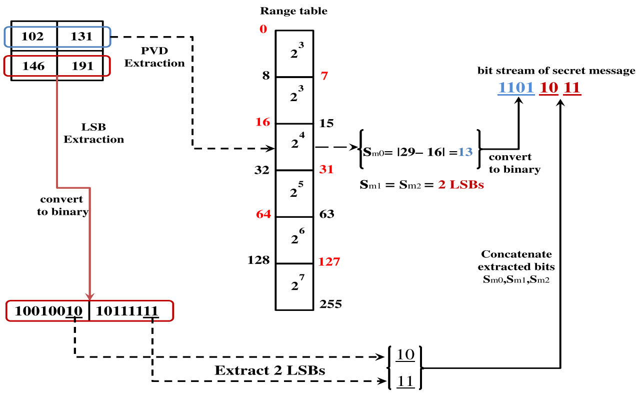


FIGURE 7. Example of the extraction process of the proposed method where T=0.001 and K=2.

of the stego image is undetectable to human vision [42]. That is, a higher value PSNR means a smaller amount of distortion and leads to high visual quality. Meanwhile, a small value of PSNR leads to remarkable changes in stego images that can be easily noticeable by the HVS. The PSNR value between

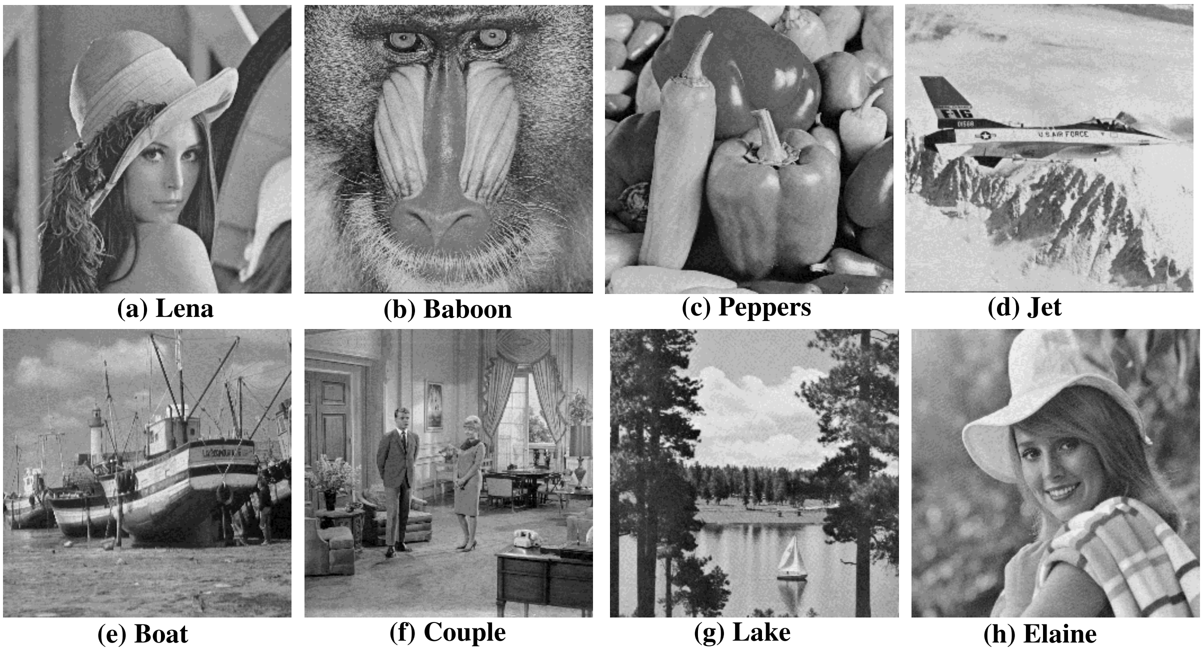


FIGURE 8. Standard 8-bit grayscale image used in experiments as cover images.

the cover image and the stego image is calculated as follows:

$$PSNR = 10\ \log_{10}\frac{255^2}{MSE} \tag{7}$$

where the MSE for images of size $M \times N$ pixels is defined as

$$MSE = \frac{1}{M*N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(C_{ij} - S_{ij})^2. \tag{8}$$

Another more reliable visual quality metric known as the quality index Q [17] is also considered to measure the similarity between cover images and stego images. High values for Q mean that the cover images and stego images are highly correlated, and differences between them are very small. The universal quality index Q can be calculated using

$$Q = \frac{4\sigma_{xy}\bar{x}\bar{y}}{(\sigma_x^2 + \sigma_y^2)[(\bar{x})^2 + (\bar{y})^2)]}. \tag{9}$$

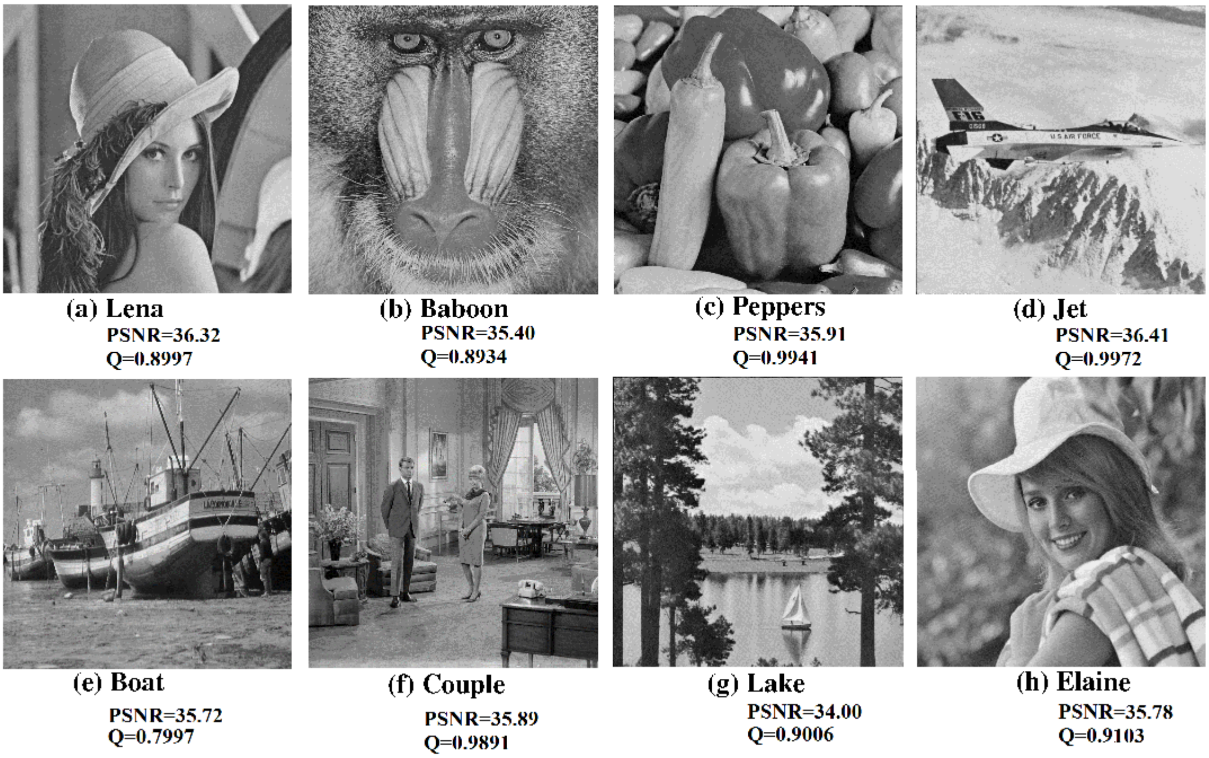
where x, y, $\bar{x}$, and $\bar{y}$ are the value of the pixels in the cover image, the value of the pixels in the stego image, the mean value of x, the mean value of y, and the σ_x^2, σ_y^2 and σ_{xy}^2 are the variance and covariance of x, y and xy images, respectively.

Fig. 9 shows the results of applying the proposed method on the eight stego images shown in Fig 8. It is clear that the visual quality of all stego images at the maximum embedding capacity of 100, 000 bytes did not change considerably by applying the embedding algorithm. The minimum obtained PSNR was 34.00 dB for the lake image, while the minimum quality index Q was 0.7997 for the boat image. Even with these minimum values, the visual quality of these two stego images was still acceptable. Consequently, there were no real observed visual artifacts by human eyes in the stego images due to the embedding process. Thus, the proposed method maintained a higher payload capacity reaching 100, 000 bytes without sacrificing too much imperceptibility or security.

Furthermore, Fig. 10 shows the results of applying the proposed method on eight color images. It is clear that the PSNR benchmark lies between two values 42.86 dB for baboon and 44.91 dB for the lake image. The Q benchmark lay between 0.9925 for baboon and 0.9996 for Lena. However, a higher embedding capacity reaching 100, 000 bytes achieves good imperceptibility and more security. This leads to the exploitation of better visual quality without any detectable changes that can be obtained by HVS.

B. IMPACT OF THRESHOLD ADJUSTING ON EMBEDDING CAPACITY

In this experiment, the effect of changing the threshold value on the embedding capacity is investigated. Fig. 11 illustrates the effects of changing T values in the range from 0.001 to 1 for the baboon cover image on the embedding capacity at $k = 3$. The baboon cover image is chosen for this test as it has a high embedding capacity because it contains rich edges, which results in a large number of BOIs. Obviously, for smaller values of threshold T, the embedding capacity and the number of BOIs increase. Otherwise, the embedding capacity decreases as the value of T increases. Decreasing the value of T allows weak edge pixels to be selected for embedding data while increasing permits only sharp edges to be used for embedding data.



(a) Lena
PSNR=36.32
Q=0.8997

(b) Baboon
PSNR=35.40
Q=0.8934

(c) Peppers
PSNR=35.91
Q=0.9941

(d) Jet
PSNR=36.41
Q=0.9972

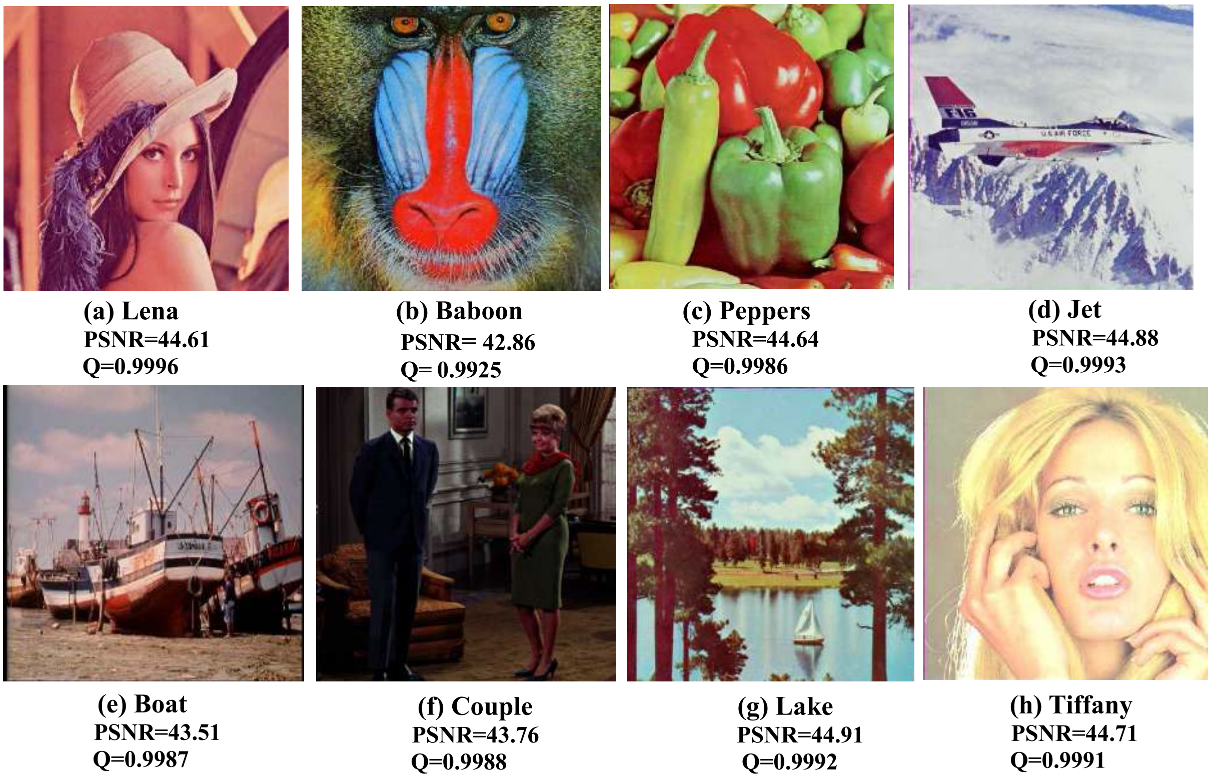
(e) Boat
PSNR=35.72
Q=0.7997

(f) Couple
PSNR=35.89
Q=0.9891

(g) Lake
PSNR=34.00
Q=0.9006

(h) Elaine
PSNR=35.78
Q=0.9103

FIGURE 9. An illustration of the visual quality of stego images using the proposed method at maximum embedding capacity of 100, 000 bytes.



(a) Lena
PSNR=44.61
Q=0.9996

(b) Baboon
PSNR= 42.86
Q= 0.9925

(c) Peppers
PSNR=44.64
Q=0.9986

(d) Jet
PSNR=44.88
Q=0.9993

(e) Boat
PSNR=43.51
Q=0.9987

(f) Couple
PSNR=43.76
Q=0.9988

(g) Lake
PSNR=44.91
Q=0.9992

(h) Tiffany
PSNR=44.71
Q=0.9991

FIGURE 10. An illustration of the visual quality of color stego images using the proposed method.

C. THE EFFECT OF CHANGING K-LSB ON PSNR

Here, we study the impact of changing the k-LSB value over the visual quality metric. Fig. 12 illustrates the obtained results for the effect of changing k values from 0 to 5 using the Lena stego image at a threshold value of $T = 0.001$. The obtained a PSNR value of the Lena stego image is above

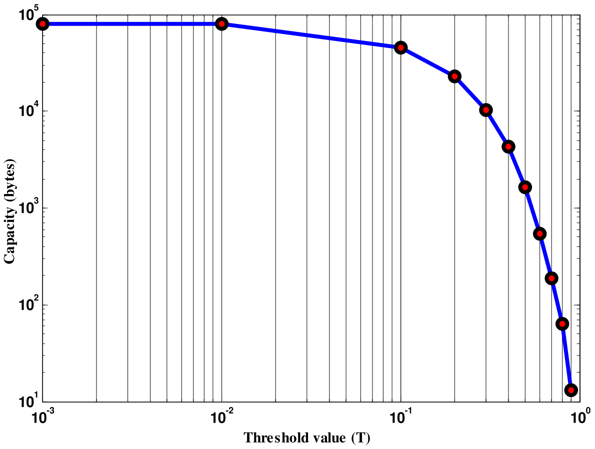


FIGURE 11. The effect of changing threshold value on embedding capacity using the baboon cover image. The horizontal axes are plotted on the log scale to allow a wide span of T values.

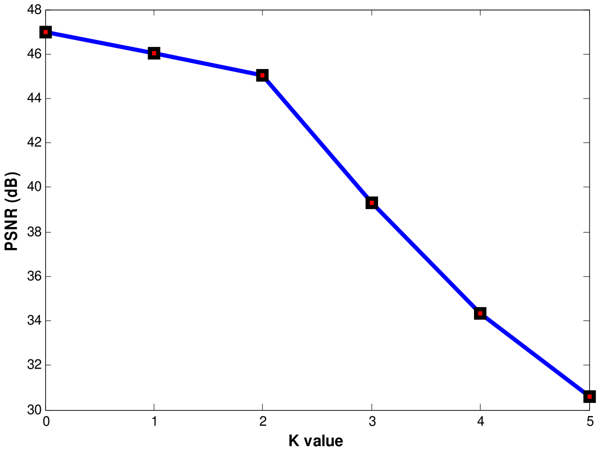


FIGURE 12. Impact of changing the k-LSBs on the PSNR value for the Lena stego image.

34 dB at $k = 4$. This means that the distortion in the stego image resulting from using the proposed method is invisible to the human visual system. Additionally, the obtained results prove that the PSNR value increases as the k value decreases, which leads to high visual quality for the stego images reaching 47.3 dB at $k = 0$. Accordingly, one may conclude that there is a tradeoff between the embedding capacity and PSNR value, which can be controlled by the values of T and k. These values are adaptively calculated in the proposed method, depending on the quantity of data in the secret message. For a small secret message size, T takes a large value, and k takes a small value. To accommodate all data for the large size of the secret message, the value of T is small, and k is large.

D. ANALYSIS OF COMBINING THE PVD AND LSB TECHNIQUES

The importance of combining the PVD and LSB over each block within the proposed method in terms of embedding capacity and the visual quality is examined, where we utilize the PVD and LSB techniques separately in each BOI and compare them. The results reported in Table 1 show the number of BOIs that has been adaptively obtained by adjusting the key parameters (K, T) for using all edge regions to attain maximum embedding capacity. For the first two edge pixels, the BOI with PVD technique is tested along with eight grayscale images. These results show high visual quality with an average PSNR value of 44.97 dB and good average embedding capacity of 208, 549 bits. The other two remaining pixels of the BOI used for hiding the secret message utilizing the LSB technique achieve high embedding capacity with an average value of 385, 358 bits. Additionally, good visual quality is achieved with an average PSNR value of 42.09 dB. Thus, combining the two embedding PVD and LSB techniques in 2 × 2 BOI improves hiding capacity and provides better visual quality without any artificial changes on the stego images that may be recognized by the HVS, leading to more embedding security.

TABLE 1. Results of combining PVD and LSB techniques in terms of embedding capacity and visual quality.

Cover Images 512 × 512	No. of BOIs	BOI with PVD		BOI with LSB	
		Capacity (bits)	PSNR	Capacity (bits)	PSNR
Lena	65,109	203,903	45.58	390,654	41.95
Baboon	65,534	245,568	40.76	393,204	41.86
Peppers	65,458	206,453	45.96	392,748	41.87
Jet	60,518	176,022	45.19	363,108	43.29
Boat	64,199	211,443	45.89	389,226	41.89
Lake	64,613	208,175	45.39	383,808	41.96
Elaine	64,090	198,899	45.31	377,322	42.05
Couple	65,356	217,930	45.67	392,796	41.88
Average	64,360	208,549	44.97	385,358	42.09

E. COMPARISON WITH THE STATE-OF-THE-ART

1) COMPARISON WITH PVD-BASED STEGANOGRAPHY METHODS

The proposed method is compared with popular counterparts spatial PVD-based steganography methods, including Wu and Tsai [11], Wu *et al.* [54], Wang *et al.* [18], Yang *et al.* [19], Liao *et al.* [20], Hussain *et al.* [14], and Li and He [25]. These methods are all spatial domains based on the PVD technique similar to the proposed method. The results of the comparison are given in Table 2, which shows that the proposed method achieves high embedding capacity compared to these seven counterpart methods with an average capacity of 76, 027 bytes. Additionally, the proposed method achieves higher PSNR values than the methods of Wu and Tsai [11], Wu *et al.* [54], Yang *et al.* [19] and Hussain *et al.* [14] resulting in better imperceptibility with an average PSNR of 38.64 dB. Consequently, the proposed method outperforms its PVD-based counterparts with respect to the embedding capacity and image quality. It should be noted that for results given in Table 2, the settings are such that $T_i = 0$, $K_i = 0$, $T = 0.001$, and $K = 3$.

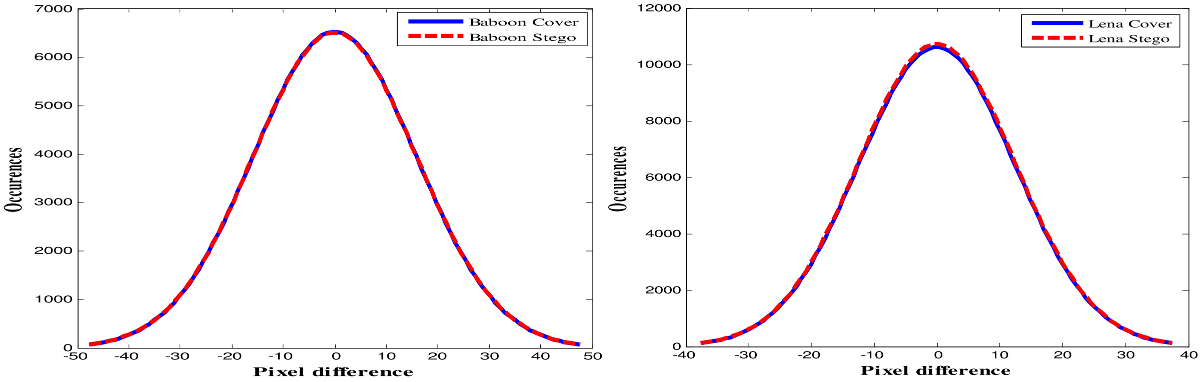


FIGURE 13. Security against PDH analysis at 50% embedding capacity for the baboon and Lena stego images.

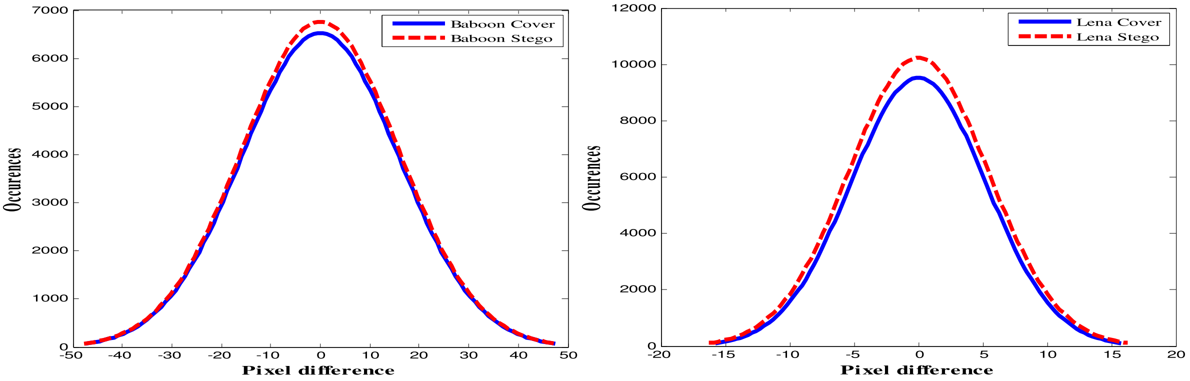


FIGURE 14. Security against PDH analysis at 100% embedding capacity for the baboon and Lena stego images.

TABLE 2. Performance comparison of the proposed method and other PVD-based methods.

Cover Images	Wu and Tsai [11]		Wu et al. [54]		Wang et al. [18]		Yang et al. [19]		Liao et al. [20]		Mehdi et al. [14]		Li and He [25]		Proposed Method	
512 × 512	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR
Lena	51,219	38.94	66,064	38.80	6,402	44.10	70,217	38.24	70,217	41.48	70,402	39.09	70,217	42.74	74,800	39.61
Baboon	57,146	33.43	68,007	33.33	7,143	40.30	86,466	32.24	86,466	35.61	78,972	35.06	86,466	36.63	79,848	36.01
Peppers	50,907	37.07	66,032	37.50	6,363	43.30	70,281	38.42	70,281	41.28	70,321	39.30	70,281	42.45	74,987	39.89
Jet	51,224	37.42	66,256	37.63	6,217	45.20	69,154	39.18	69,154	42.06	66,716	41.19	69,154	43.23	75,321	39.43
Boat	52,635	34.89	66,622	35.01	6,579	42.10	74,623	36.17	74,623	39.29	73,130	37.49	74,623	39.41	76,084	38.34
Lake	52,923	35.07	67,032	36.63	6,170	44.60	71,165	36.90	71,165	40.37	71,232	39.06	71,165	40.29	76,375	38.06
Elaine	50,807	36.07	65,032	37.01	6,384	44.80	72,125	37.20	72,125	40.17	72,075	39.14	72,125	41.22	74,345	39.51
Couple	51,604	38.81	66,167	39.07	6,450	43.50	72,266	37.02	72,266	40.06	72,213	37.75	72,266	41.14	76,459	38.27
Average	52,308	36.46	66,402	36.87	6,464	43.49	73,287	36.92	73,287	40.04	71,883	38.51	73,287	40.89	76,027	38.64

2) COMPARISON WITH PVD-LSB-BASED METHODS

In the proposed method, the PVD technique is utilized to hide secret data bits in the dominant edge direction, while the LSB substitution technique is used to embed secret bits in the other two remaining pixels. Thus, a comparison with other published methods that adapt both PVD and LSB techniques at the same time is required. The results given in Table 3 summarize the required comparison between the proposed method

TABLE 3. Performance comparison of the proposed method and PVD-LSB-based steganography methods.

Cover Images	Yang et al. [48]		Lee and Chen [42]		Khodaei et al. [47]		Proposed Method	
512x512	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR
Lena	98,304	37.91	100,023	37.74	104,878	37.67	104,055	36.32
Baboon	98,304	31.92	100,923	36.05	104,275	35.63	105,880	35.40
Peppers	98,304	37.92	104,504	37.05	102,755	37.13	105,505	35.91
Jet	98,304	37.93	99,979	38.12	104,439	36.02	105,206	36.41
Boat	98,304	36.23	104,351	36.86	104,432	36.80	105,507	35.72
Lake	98,304	36.93	99,321	35.40	103,543	36.04	105,890	35.89
Elaine	98,304	37.89	99,956	37.56	104,726	37.74	105,568	34.00
Couple	98,304	36.13	99,432	36.21	103,543	36.89	105,880	35.78
Average	98,304	36.61	100,591	36.87	104,074	36.74	105,436	35.68

TABLE 4. Performance comparison of the proposed method and other frequency domain methods.

Cover Images	Xuan et al. [55]		Seyyedi and Ivanov [56]		Atta and Ghanbari [36]		Proposed Method	
	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR
Lena	10,688	36.64	50,000	40.54	58,327	44.91	58,416	45.05
Baboon	1,865	32.76	50,000	38.07	60,239	44.59	63,465	41.82
Peppers	8,661	29.11	50,000	40.64	58,040	45.03	58,603	45.65
Jet	11,748	36.30	40,000	40.18	59,133	44.43	59,959	44.77
Boat	N/A	N/A	50,000	39.40	59,482	44.58	59,700	45.70
Couple	10,610	29.83	N/A	N/A	59,255	44.73	60,075	45.95
Average	8,714	32.93	48,000	39.77	59,079	44.71	60,036	44.82

and other well-known PVD-LSB-based methods, namely, Yang *et al.* [48], Lee and Chen [42], and Khodaei *et al.* [47] in terms of hiding capacity and PSNR value. These methods are built on both PVD and LSB techniques for embedding bits in grayscale images. The obtained results confirm that the proposed method is better than the three methods in terms of embedding capacity, with approximately 105, 436 bytes on average. In the context of the visual quality of the stego images, the proposed method performs well, with high values for PSNR reaching 35.68 on average. Clearly, the embedding capacity for the proposed method in all cases is higher than those of Yang *et al.* [48], Lee and Chen [42] and Khodaei *et al.* [47]. It also verifies the effectiveness of the proposed method in preserving visual quality without any detectable changes over the stego images from their original images can be noted by HVS.

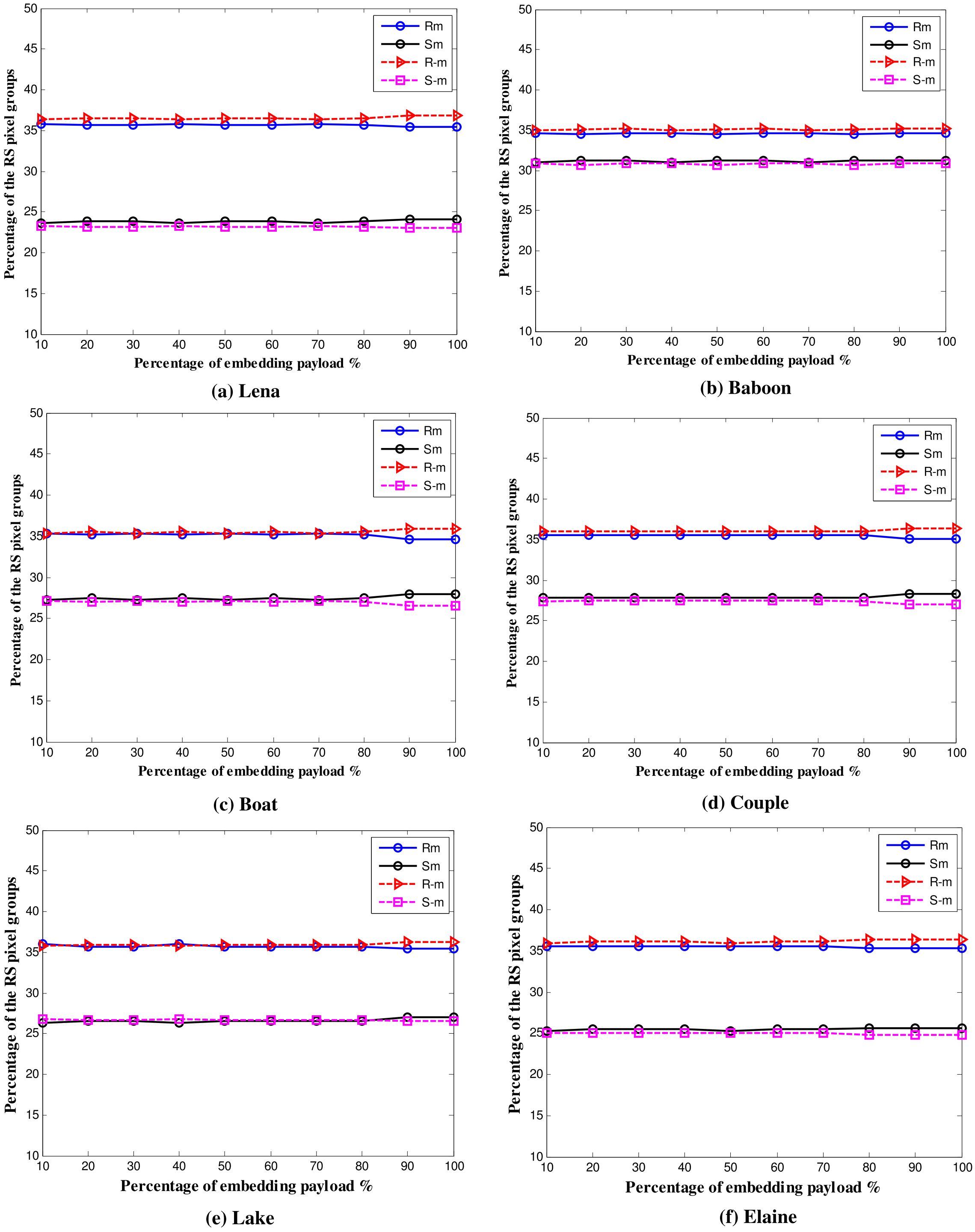
3) COMPARISON WITH NONSPATIAL DOMAIN METHODS

However, although the proposed method belongs to the spatial domain methods, it is also compared with other nonspatial (i.e., frequency domain) methods. Thus, two wavelet-based steganography methods are considered: Schaefer and Stich [55] and Seyyedi and Ivanov [56], as well as one of the most recent data hiding techniques Atta and Ghanbari's [36] method, which is based on wavelet packet transformation and a neutrosophic set using the LSB substitution technique. The results of this experiment are reported in Table 4. The proposed method achieves high embedding capacity and better quality compared with the average capacity and PSNR of 60, 036 bytes and 44.82 dB, respectively. As reported in Table 4, the variations between capacity and PSNR values among different cover images are caused by the texture type and the number of edge pixels available for embedding secret data bits. Thus, T and K values are initialized and modified adaptively. The settings for results given in Table 4 are $T_i = 0$, $K_i = 0$, T=0.01, and $K = 2$.

F. ANALYSIS OF SECURITY AND UNDETECTABILITY

1) SECURITY AGAINST PIXEL DIFFERENCE HISTOGRAM ANALYSIS

The pixel difference histogram (PDH) is one of the steganalysis schemes used to discover embedded secret data in images. Previous related works such as [11], [57] considered the PDH analysis for detecting and analyzing the artifacts resulting from steganography methods. Simply, the PDH calculates differences of neighboring pixels between cover and stego images to detect whether there are secret data in the stego images. The PDH curves for two cover images (left baboon and right Lena) and their stego images using the proposed method at 50% and 100% embedding capacity are depicted in Fig. 13 and Fig. 14, respectively. To target 50% embedding capacity in cover images, two values are set: $T = 0.02$



(a) Lena

(b) Baboon

(c) Boat

(d) Couple

(e) Lake

(f) Elaine

FIGURE 15. The RS analysis graphs of six stego images for the proposed method.

and $K = 2$. For 100% embedding capacity is achieved at $T = 0.0016$ and $K = 3$. Looking closely at both curves of the cover and stego images in Fig. 13 at 50% embedding capacity, they are very similar. This means that histograms can be kept well despite the data hiding process. With increasing embedding capacity reaching the maximum embedding capacity (i.e., 100%), there is a very slight difference between the two curves, as shown in Fig. 14. Nevertheless, the distortion in both the baboon and Lena images is still acceptable after embedding secret data of various sizes reaching the maximum capacity. This confirms that the proposed method resists PDH analysis.

2) SECURITY AGAINST THE STATISTICAL RS STEGANALYSIS

Another powerful steganalytic technique called RS steganalysis [29] is used to examine the security of the proposed method. The RS analysis classifies image pixels into either regular group (R_m or R_{-m}) or singular group (S_m or S_{-m})

TABLE 5. Comparison of computational time (in seconds).

Methods	Embedding time	Extraction time	Total time
Shen and Huang [12]	3.5	2.1	5.6
Wu et al. [54]	3.0	1.9	4.9
Sahu and Swain [26]	2.9	2.0	4.9
Proposed Method	2.5	2.0	4.5
Wu and Tsai [11]	2.3	1.4	3.7

based on a mask $m = [0\ \ 1, 1\ \ 0]$ and $-m = [0\ \ -1, -1\ \ 0]$. Then, the RS analysis technique detects any change in the regular and singular groups with increasing embedding capacity. Hence, the stego image passes the RS steganalysis attack when the difference between the two groups is restricted to a minimum. In other words, when the relative number of R_m is equal to that of R_{-m} and the relative number of S_m is equal to that of S_{-m}. In this context, the RS analysis does not disclose any hidden data if the relation $R_m \cong R_{-m} > S_m \cong S_{-m}$ is valid. Fig. 15 shows the results of the RS steganalysis for six stego images at different values of T, K and various embedding rates. It is very clear for all tested stego images that the relation $R_m \cong R_{-m} > S_m \cong S_{-m}$ is true. That is, the difference between R_m, R_{-m} and S_m, S_{-m} does not change substantially even with increasing embedding capacity to be 100% as illustrated in Fig. 15. Accordingly, the probability of detecting the hidden data is very weak. The results drawn in Fig. 15 prove experimentally that the proposed method resists RS steganalysis attacks well.

G. ANALYSIS OF TIME COMPLEXITY

The software setup used to compute the average time complexity (TC) is MATLAB 2015a on a Windows 10 operating system with a Core i5 processor, 4 GB RAM and a 1 TB hard disk. Table 5 compares the average TC for the proposed method and the existing methods, including Wu and Tsai [11], Wu *et al.* [54], Shen and Huang [12] and Sahu and Swain [26] with respect to the maximum embedding capacity. The embedding and extraction time in Table 5 represents the average time for the eight grayscale images, which are shown in Fig. 8. It can be observed that the proposed method comes after the original PVD method [11], which has the smallest TC with a total time equal to 3.7s compared to other data hiding methods because of its simplicity in the embedding and extraction scheme. The method of Shen and Huang [12] has the highest time in the embedding and extraction process, while the TC for Wu *et al.* [54] and Sahu and Swain [26] are equal with 4.9 s. In this context, the proposed method is better than Wu *et al.* [54], Shen and Huang [12] and Sahu and Swain [26] with a total TC of 4.5 s.

V. CONCLUSION

In this paper, an adaptive data hiding method using a histogram of oriented gradient (HOG) is proposed for embedding secret data into digital images based on PVD-LSB techniques. A set of blocks of interest (BOIs) is determined adaptively using the HOG algorithm depending on the edge content of the cover image. The PVD technique is utilized to hide secret data bits in the dominant edge direction, while the LSB substitution technique is used to embed secret bits in the other two remaining pixels. The proposed method improves the embedding capacity, visual quality, and security of the stego image because it exploits only the edge pixels of the cover image to embed secret data. Additionally, it improves security because it can adaptively embed different numbers of bits for each 2 × 2 block of interest (BOI) in the cover image. The well-known tradeoff between the PSNR value and the hiding capacity can be controlled by increasing or decreasing the threshold value and the number of k-bits used in the LSB according to the length of the secret message. A comparison of the proposed method with other adaptive PVD-LSB-based methods shows that it performs well with respect to embedding capacity, visual quality and imperceptibility. It also improves the visual quality without any intelligible changes to the stego images that can be noticed by the HVS compared to previous spatial domain and frequency domain methods. Furthermore, the obtained results proved that the proposed method is robust against steganalysis techniques such as pixel difference histogram and RS analysis. Moreover, the proposed method can be applied to color images where the embedding capacity for each color channel can be selected adaptively with respect to the highest embedding capacity size to absorb whole secret bits. Finally, it can be concluded that combining PVD-LSB and HOG algorithms can improve the embedding capacity, visual quality and security of traditional PVD and LSB methods.

ACKNOWLEDGMENT

The authors extend their appreciation to the Deanship of Scientific Research at Majmaah University for supporting this work under project number No. RGP-2019-24.

REFERENCES

[1] Z. Wang and X. Zhang, "Secure cover selection for steganography," *IEEE Access*, vol. 7, pp. 57857–57867, 2019.

[2] K.-C. Wu and C.-M. Wang, "Steganography using reversible texture synthesis," *IEEE Trans. Image Process.*, vol. 24, no. 1, pp. 130–139, Jan. 2015.

[3] Z. Qu, Z. Cheng, and X. Wang, "Matrix coding-based quantum image steganography algorithm," *IEEE Access*, vol. 7, pp. 35684–35698, 2019.

[4] T. Denemark and J. Fridrich, "Steganography with multiple JPEG images of the same scene," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 10, pp. 2308–2319, Oct. 2017.

[5] Y. Zhang, X. Luo, Y. Guo, C. Qin, and F. Liu, "Zernike moment-based spatial image steganography resisting scaling attack and statistic detection," *IEEE Access*, vol. 7, pp. 24282–24289, 2019.

[6] X. Qin, B. Li, S. Tan, and J. Zeng, "A novel steganography for spatial color images based on pixel vector cost," *IEEE Access*, vol. 7, pp. 8834–8846, 2019.

[7] M. R. Ogiela and K. Koptyra, "False and multi-secret steganography in digital images," *Soft Comput.*, vol. 19, no. 11, pp. 3331–3339, 2015.

[8] S. Chutani and A. Goyal, "A review of forensic approaches to digital image steganalysis," *Multimedia Tools Appl.*, vol. 78, pp. 18169–18204, Jan. 2019.

[9] T. D. Denemark, M. Boroumand, and J. Fridrich, "Steganalysis features for content-adaptive JPEG steganography," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 8, pp. 1736–1746, Aug. 2016.

[10] M. Liśkiewicz, R. Reischuk, and U. Wölfel, "Security levels in steganography–insecurity does not imply detectability," *Theor. Comput. Sci.*, vol. 692, pp. 25–45, Sep. 2017.

[11] D.-C. Wu and W.-H. Tsai, "A steganographic method for images by pixel-value differencing," *Pattern Recognit. Lett.*, vol. 24, no. 9, pp. 1613–1626, Jun. 2003.

[12] S.-Y. Shen and L.-H. Huang, "A data hiding scheme using pixel value differencing and improving exploiting modification directions," *Comput. Secur.*, vol. 48, pp. 131–141, Feb. 2015.

[13] M. Hussain, A. W. A. Wahab, N. Javed, and K.-H. Jung, "Recursive information hiding scheme through LSB, PVD shift, and MPE," *IETE Tech. Rev.*, vol. 35, no. 1, pp. 53–63, 2018.

[14] M. Hussain, A. W. A. Wahab, A. T. S. Ho, N. Javed, and K. H. Jung, "A data hiding scheme using parity-bit pixel value differencing and improved rightmost digit replacement," *Signal Process., Image Commun.*, vol. 50, pp. 44–57, Feb. 2017.

[15] C.-K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," *Pattern Recognit.*, vol. 37, no. 3, pp. 469–474, Mar. 2004.

[16] S. Sajasi and A. M. E. Moghadam, "An adaptive image steganographic scheme based on noise visibility function and an optimal chaotic based encryption method," *Appl. Soft Comput.*, vol. 30, pp. 375–389, May 2015.

[17] Z. Wang and A. C. Bovik, "A universal image quality index," *IEEE Signal Process. Lett.*, vol. 9, no. 3, pp. 81–84, Mar. 2002.

[18] C.-M. Wang, N.-I. Wu, C.-S. Tsai, and M.-S. Hwang, "A high quality steganographic method with pixel-value differencing and modulus function," *J. Syst. Softw.*, vol. 81, no. 1, pp. 150–158, 2008.

[19] C.-H. Yang, S.-J. Wang, and C.-Y. Weng, "Capacity-raising steganography using multi-pixel differencing and pixel-value shifting operations," *Fundam. Inform.*, vol. 98, nos. 2–3, pp. 321–336, 2010.

[20] X. Liao, Q.-Y. Wen, Z.-L. Zhao, and J. Zhang, "A novel steganographic method with four-pixel differencing and modulus function," *Fundam. Inf.*, vol. 118, no. 3, pp. 281–289, 2012.

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

[22] J. Chen, "A PVD-based data hiding method with histogram preserving using pixel pair matching," *Signal Process., Image Commun.*, vol. 29, no. 3, pp. 375–384, Mar. 2014.

[23] K.-H. Jung and K.-Y. Yoo, "High-capacity index based data hiding method," *Multimedia Tools Appl.*, vol. 74, no. 6, pp. 2179–2193, 2015.

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

[25] Z. Li and Y. He, "Steganography with pixel-value differencing and modulus function based on PSO," *J. Inf. Secur. Appl.*, vol. 43, pp. 47–52, Dec. 2018.

[26] A. K. Sahu and G. Swain, "Pixel overlapping image steganography using PVD and modulus function," *3D Res.*, vol. 9, no. 3, p. 40, 2018.

[27] C. Qin, W. Zhang, F. Cao, X. Zhang, and C.-C. Chang, "Separable reversible data hiding in encrypted images via adaptive embedding strategy with block selection," *Signal Process.*, vol. 153, pp. 109–122, Dec. 2018.

[28] T. Pevný, P. Bas, and J. Fridrich, "Steganalysis by subtractive pixel adjacency matrix," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 2, pp. 215–224, Jun. 2010.

[29] J. Fridrich, M. Goljan, and R. Du, "Detecting LSB steganography in color, and gray-scale images," *IEEE Multimedia Mag.*, vol. 8, no. 4, pp. 22–28, Oct./Dec. 2001.

[30] J. Mielikainen, "LSB matching revisited," *IEEE Signal Process. Lett.*, vol. 13, no. 5, pp. 285–287, May 2006.

[31] X. Li, B. Yang, D. Cheng, and T. Zeng, "A generalization of LSB matching," *IEEE Signal Process. Lett.*, vol. 16, no. 2, pp. 69–72, Feb. 2009.

[32] C.-H. Yang, "Inverted pattern approach to improve image quality of information hiding by LSB substitution," *Pattern Recognit.*, vol. 41, no. 8, pp. 2674–2683, 2008.

[33] W. Luo, F. Huang, and J. Huang, "Edge adaptive image steganography based on LSB matching revisited," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 2, pp. 201–214, Jun. 2010.

[34] P. Deshmukh and T. Pattewar, "A novel approach for edge adaptive steganography on LSB insertion technique," in *Proc. IEEE Int. Conf. Inf. Commun. Embedded Syst.*, Feb. 2014, pp. 1–5.

[35] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, and S. W. Baik, "A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image," *Multimedia Tools Appl.*, vol. 75, no. 22, pp. 14867–14893, 2016.

[36] R. Atta and M. Ghanbari, "A high payload steganography mechanism based on wavelet packet transformation and neutrosophic set," *J. Vis. Commun. Image Represent.*, vol. 53, pp. 42–54, May 2018.

[37] W. Hong, "Adaptive image data hiding in edges using patched reference table and pair-wise embedding technique," *Inf. Sci.*, vol. 221, pp. 473–489, Feb. 2013.

[38] A. Pradhan, K. R. Sekhar, and G. Swain, "Adaptive PVD steganography using horizontal, vertical, and diagonal edges in six-pixel blocks," *Secur. Commun. Netw.*, vol. 2017, Aug. 2017, Art. no. 1924618.

[39] G. Swain, "Adaptive and non-adaptive PVD steganography using overlapped pixel blocks," *Arabian J. Sci. Eng.*, vol. 43, no. 12, pp. 7549–7562, 2018.

[40] Y.-P. Lee, J.-C. Lee, W.-K. Chen, K.-C. Chang, I.-J. Su, and C.-P. Chang, "High-payload image hiding with quality recovery using tri-way pixel-value differencing," *Inf. Sci.*, vol. 191, pp. 214–225, May 2012.

[41] K.-C. Chang, C.-P. Chang, P. S. Huang, and T.-M. Tu, "A novel image steganographic method using tri-way pixel-value differencing," *J. Multimedia*, vol. 3, no. 2, pp. 37–44, 2008.

[42] C.-F. Lee and H.-L. Chen, "A novel data hiding scheme based on modulus function," *J. Syst. Softw.*, vol. 83, no. 5, pp. 832–843, 2010.

[43] M. Abdel Hameed, S. Aly, and M. Hassaballah, "An efficient data hiding method based on adaptive directional pixel value differencing (ADPVD)," *Multimedia Tools Appl.*, vol. 77, no. 12, pp. 14705–14723, 2018.

[44] X. Liao, Q.-Y. Wen, and J. Zhang, "A steganographic method for digital images with four-pixel differencing and modified LSB substitution," *J. Vis. Commun. Image Represent.*, vol. 22, no. 1, pp. 1–8, 2011.

[45] P. Thiyagarajan and G. Aghila, "Reversible dynamic secure steganography for medical image using graph coloring," *Health Policy Technol.*, vol. 2, no. 3, pp. 151–161, 2013.

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

[47] M. Khodaei, B. S. Bigham, and K. Faez, "Adaptive data hiding, using pixel-value-differencing and LSB substitution," *Cybern. Syst.*, vol. 47, no. 8, pp. 617–628, 2016.

[48] C. H. Yang, C. Y. Weng, S. J. Wang, and H. M. Sun, "Adaptive data hiding in edge areas of images with spatial LSB domain systems," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 3, pp. 488–497, Sep. 2008.

[49] M. Khodaei and K. Faez, "New adaptive steganographic method using least-significant-bit substitution and pixel-value differencing," *IET Image Process.*, vol. 6, no. 6, pp. 677–686, 2012.

[50] A. Pradhan, K. R. Sekhar, and G. Swain, "Digital image steganography using LSB substitution, PVD, and EMD," *Math. Problems Eng.*, vol. 2018, Sep. 2018, Art. no. 1804953.

[51] C.-F. Lee, C.-C. Chang, and K.-H. Wang, "An improvement of EMD embedding method for large payloads by pixel segmentation strategy," *Image Vis. Comput.*, vol. 26, no. 12, pp. 1670–1676, 2008.

[52] N. Dalal and B. Triggs, "Histograms of oriented gradients for human detection," in *Proc. IEEE Comput. Vis. Pattern Recognit. (CVPR)*, vol. 1, Jun. 2005, pp. 886–893.

[53] G. Schaefer and M. Stich, "UCID: An uncompressed color image database," *Proc. SPIE*, vol. 5307, pp. 472–481, Dec. 2003.

[54] H.-C. Wu, N.-I. Wu, C.-S. Tsai, and M.-S. Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods," *IEE Proc.-Vis., Image Signal Process.*, vol. 152, no. 5, pp. 611–615, Oct. 2005.

[55] G. Xuan, J. Zhu, J. Chen, Y. Q. Shi, Z. Ni, and W. Su, "Distortionless data hiding based on integer wavelet transform," *Electron. Lett.*, vol. 38, no. 25, pp. 1646–1648, Dec. 2002.

[56] S. A. Seyyedi and N. Ivanov, "High payload and secure steganography method based on block partitioning and integer wavelet transform," *Int. J. Secur. Appl.*, vol. 8, no. 4, pp. 183–194, 2014.

[57] X. Zhang and S. Wang, "Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security," *Pattern Recognit. Lett.*, vol. 25, no. 3, pp. 331–339, Feb. 2004.

MOHAMED ABDEL HAMEED received the B.Sc. degree in computer science from the Faculty of Computers and Information, Suez Canal University, Ismailia, Egypt, in 2004, and the M.Sc. degree in computer science from the Faculty of Science, Suez Canal University, in 2012, and the Ph.D. degree in computer science from the Faculty of Science, South Valley University, Egypt, in 2019. He is currently a Lecturer with the Department of Computer Science, Faculty of Computers and Information, Luxor University. He has more than ten years of experience in the field of information technology and network communications. His research interests include data hiding, deep learning, wireless communications, information security, and digital image steganography.

M. HASSABALLAH received the B.Sc. degree in mathematics and the M.Sc. degree in computer science from South Valley University, Egypt, in 1997 and 2003, respectively, and the D.Eng. degree in computer science from Ehime University, Japan, in 2011. He was a Visiting Scholar with the Department of Computer and Communication Science, Wakayama University, Japan, in 2013, and the GREAH Laboratory, Le Havre Normandie University, France, in 2019. He is currently an Associate Professor of computer science with the Faculty of Computers and Information, South Valley University. His research interests include feature extraction, object detection/recognition, artificial intelligence, biometrics, image processing, computer vision, machine learning, and data hiding.

SALEH ALY received the B.Sc. and M.Sc. degrees in electrical and computer engineering from Assiut University, Assiut, Egypt, in 1997 and 2004, respectively, and the Ph.D. degree from the Department of Intelligent Systems, Graduate School of Information Science and Electrical Engineering, Kyushu University, Japan, in 2010. In 2012 and 2014, he was a Visiting Researcher with the Department of Media Science, Nagoya University, and the Department of Computer Science, Tsukuba University, Japan, respectively. He is currently an Associate Professor with the Department of Information Technology, College of Computer and Information Sciences, Majmaah University, and on a leave from the Electrical Engineering Department, Faculty of Engineering, Aswan University, Egypt. His research interests include deep learning, neural networks, pattern recognition, image processing, machine learning, and computer vision.

ALI ISMAIL AWAD (S'11–M'13–SM'17) is currently an Associate Professor (Docent) with the Department of Computer Science, Electrical and Space Engineering, Luleå University of Technology, Luleå, Sweden, where he also serves as a Coordinator of the Master Programme in information security. He is also a Visiting Researcher with the University of Plymouth, U.K. He is also an Associate Professor with the Electrical Engineering Department, Faculty of Engineering, Al-Azhar University at Qena, Qena, Egypt. His research interests include information security, the Internet of Things security, image analysis with applications in biometrics and medical imaging, and network security. He has edited or coedited six books and authored or coauthored several journal articles and conference papers in these areas. He is an Editorial Board Member of the *Future Generation Computer Systems Journal*, *Computers and Security Journal*, the *Internet of Things*, *Engineering Cyber Physical Human Systems Journal*, and *Health Information Science and Systems Journal*.