Received 10 May 2022, accepted 31 May 2022, date of publication 8 June 2022, date of current version 23 June 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3181179

High-Capacity Image Steganography Based on Discrete Hadamard Transform

YING-QIAN ZHANG[1,2,3], **KUAN ZHONG**[1,3], **AND XING-YUAN WANG**[4]

[1]School of Information Science and Technology, Xiamen University Tan Kah Kee College, Zhangzhou 363105, China
[2]School of EEAI, Xiamen University Malaysia, Sepang, Selangor 43900, Malaysia
[3]School of Informatics, Xiamen University, Xiamen 361005, China
[4]Information Science and Technology College, Dalian Maritime University, Dalian 116023, China

Corresponding author: Kuan Zhong (23020191153224@stu.xmu.edu.cn)

This work was supported in part by the Program for New Century Excellent Talents in Fujian Province University, in part by the Natural Science Foundation of Fujian Province of China under Grant 2018J01100, in part by the Zhangzhou Science and Technology Project under Grant ZZ2018J23, and in part by the National Natural Science Foundation of China under Grant 61672124. This work has been co-funded by the European regional development Fund under EU Interreg 2 Seas, CoBra Project Grant 2S04-022 and EU Interreg 2 Seas, SPEED Project Grant 2S04-019.

ABSTRACT High capacity and high imperceptibility are the primary targets for ideal image steganography. For the traditional transform-based schemes, the main challenge is to balance the imperceptibility, hiding capacity, and running efficiency. To obtain a high-quality image in dense embedding, existing high-capacity schemes usually sacrifice running efficiency and security. These disadvantages make the schemes less appealing. In this paper, based on a lightweight transform Discrete Hadamard Transform (DHT), we introduce a simple but high-performance image steganographic model. In the case of only stego-image passed, the experiment results demonstrate that the proposed scheme achieves high imperceptibility and security even in the dense embedding of 8 BPP (Bits Per Pixel). Furthermore, the proposed scheme withstands various tests and shows desirable robustness. The comparative analyses are demonstrated that our scheme is efficient and feasible image steganography.

INDEX TERMS Information security, information hiding, discrete Hadamard transform, image steganography.

I. INTRODUCTION

The rapid development of the Internet has led to an exponential increase in the number of images as an information medium. Owing to inherent properties such as high redundancy and bulk volume, images are a suitable carrier medium for information hiding techniques and thus it has been receiving attention. The information hiding methods can be segregated into two categories: Watermarking and Steganography [1]. Steganography is popular in secret communication and it means concealing a message in the carrier medium and managing to conceal the presence of hidden data during transmission [2], [3]. To provide secure communication, the hidden data must be invisible and able to withstand visual and statistical analysis. The prime goal for Steganography is high imperceptibility and high hiding capacity. In contrast, Watermarking is mainly used in copyright applications and the embedded data can be either visible or invisible. The prime motivation of Watermarking is to generate robust and effective watermarks in the carrier multimedia, the generated watermark should be unalterable by the unauthorized third party. Thus, the main concern of Watermarking is not capacity and imperceptibility but robustness.

The efficiency of the image steganography is usually evaluated by Hiding Capacity (HC), Imperceptibility, robustness, running efficiency, and security [4], [5]. The carrier image without secret data is known as the cover image, and the image with a secret message is named the stego-image. Visual quality is considered to be good when the cover image is indistinguishable from the stego-image by human eyesight. Better visual quality means a lower probability of being detected by the intruder. Besides, the stego-images are possibly subject to various deliberate attacks which aim to detect the existence of secret data [6]. Imperceptibility means the resistance against visual attack or the detection methods based on statistics. Hiding capacity is calculated by the amount of secret data and the cover image: a higher Hiding capacity means more data can be embedded in the cover image. Moreover, since transmitted stego-image possibly undergoes noisy channel, robustness is also a desirable property for image steganography. In summary, an ideal steganographic scheme should satisfy all these criteria. The prime

The associate editor coordinating the review of this manuscript and approving it for publication was Ramakrishnan Srinivasan.

target for a good steganographic model is the imperceptibility and hiding capacity.

A. LITERATURE REVIEW

For the decade years, many image steganography has been introduced and developed. Generally, these schemes can be mainly divided into two categories: spatial domain and transform domain. The common spatial domain approaches include Least Significant Bit (LSB) [7]–[9], Histogram Shifting (HS) [10], and Pixel Value Differencing (PVD) [11]–[13]. In addition, other spatial approaches such as bit flipping are also proposed and developed recently [14], [15].

In the spatial domain schemes, secret data is directly hidden over the pixel values of the cover image. For LSB methods, the least significant bits of pixels in the cover image are discarded and replaced by secret data. And in PVD based methods, the secret message is concealed in the difference value of the consecutive pixels group.

The advantages of spatial domain methods include easy implementation and fast running speed. However, these methods are usually less reliable in robustness and security [16]. It is found that the classic LSB method is vulnerable to RS attack [17]. To increase security, LSB matching (LSBM) is proposed and developed [18]. Unlike the simple LSB substitution, in the LSB matching, the pixel values are increased or decreased randomly by one to match the messages to be hidden. The LSBM reduces the imbalance in the embedding distortion and thus shows higher security in resisting steganographic attacks. Recently, related improved works include dual-layer LSB matching [19], modified LSB matching combined with multi stego-medium [20] and pixel difference [21]. In addition, chaotic systems can also be combined with steganography to achieve better performance. For instance, scheme [22] encrypts the secret message with chaos encryption technology before embedding; scheme [23] utilizes a modified chaotic system to determine embedding locations; scheme [24] and scheme [9] combine the chaotic map system with the optimization algorithms to locate the optimal position and to minimize the distortion of stego-images.

For PVD based methods, the existence of the Fall Off Boundary Problem (FOBP) has attracted the researcher's attention. Scheme [12] avoids the fall off boundary problem and reduces the distortion of the stego-image by utilizing the modulus function with pixel readjustment. Scheme [13] exploits the usage of multi-directional pixel value difference. The scheme improves the performance in Hiding capacity and image quality while avoiding the FOBP and incorrect extraction problem (IEP).

Unlike the spatial domain methods, transform based technology embeds the confidential data in the transformed coefficients. The most commonly used transforms include the Discrete Cosine Transform (DCT) [25], [26], and the Discrete Wavelet Transform (DWT) [27], [28]. Recently, more transform methods including Integer Wavelet Transform (IWT) [29], [30], Complex Wavelet Transform (CWT) [31], and the Dual-Tree Complex Wavelet Transform (DT-CWT) [32], [33] has attracted the researchers' attention. Generally, the existing approaches use different ways to boost efficiency. To improve security, chaotic systems have also been used in transform domain methods [34], [35]. Scheme [34] utilize the modified 3D sine chaotic map to generate the 3D embedding position used in color image steganography; Scheme [35] combines the DCT with a chaotic map and proposes a hybrid method namely Randomly Chaotic Value Differencing (RCVD).

For both spatial based methods and transform based methods, the real challenge is the dense embedding will greatly degrade the similarity of stego-image with cover-image visually and statistically. To achieve high hiding capacity and higher imperceptibility, adaptive steganography is introduced and developed. The core strategy of adaptive steganography is to locate the optimal embedding position and thus produce better quality stego-images. The popular tools that search optimal embedding positions include Genetic algorithm (GA) [36]–[38], Particle Swarm Optimization (PSO) [29], and Ant Colony Optimization (ACO) [39]. Though the adaptive schemes improve the visual quality of the stego-image. the optimization procedure is usually time-consuming and generates extra supporting data such as location position or substitution matrix. For reversibility, supplementary data is required on the receiver side. The scheme [27] utilizes the strategy that matches the most similar cover image coefficient blocks with secret image coefficient blocks. This method achieves high visual quality and offers a good recovery of secret data. And the main disadvantage is that position data is quite considerable. Scheme [33] owns the properties of high capacity and high visual quality. however, it requires the duplicate of the cover image in the extraction stage. The original cover images (images without embedded data) are either sent through a secure channel or are already on the receiver side.

Although the above-mentioned schemes have achieved good results in hiding capacity and image quality, there is still room for improvement, especially in the condition of dense embedding. In addition, most of the methods still suffer from deficiencies in terms of operational efficiency, robustness, and security, especially since most of them do not pass the common robustness tests and security tests. The scheme achieves high capacity, high imperceptibility, high robustness, high running efficiency, and without sending supporting data is rarely reported.

B. RELATED WORK AND MOTIVATION

In the proposed scheme, DHT is adopted for obvious reasons. Compared with other common transforms, DHT is more running efficiently: its operation type only contains addition and subtraction [40]–[42]. Furthermore, compared with DFT, DCT, and DWT, the distortion of cover images caused by embedding is less in DHT [43].

In the existing literature, there are many DHT based watermarking and DHT based image steganography is rarely reported [43]–[46]. These watermarking achieve high robustness but poor hiding capacity. In the existing DHT based image steganography, the work [42] exploits the usage of DHT in the image steganography and introduces several schemes that hide the message in the DHT coefficients. In the scheme, the cover image is split into 8 × 8 non-overlapping blocks and the designed methods use different strategies to hide 1 bit in each block. In the scheme, only the 8 coefficients predefined in the 8 × 8 block are treated as potential embedding positions, which makes the hiding capacity very poor (1024 bits for 256×256 grayscale image). Besides, of all the schemes proposed in the work [42], only scheme (d) and scheme (e) are justified and tested.

To improve the hiding capacity, we consider using more coefficients for improving the hiding capacity. In the proposed scheme, all the coefficients are utilized in the maximum hiding capacity case. Due to the fact of DHT coefficients contains both positive and negative value. To extract the hidden data simply and uniformly, we process the embedding process differently depending on the positivity and negativity of the coefficients. It makes it possible to extract the hidden data at the receiver side without receiving any data even in a different hiding payload. For less distortion and better recovery, Unlike the scheme coding the secret data as a bitstream, we use a pre-defined value to quantize the embedded message and the secret data are embedded as float numbers instead of integer values. The simulation results demonstrate the strategy produces high-quality stego-images while preserving the good similarity of embedded data.

The main contributions of this paper are: 1) this paper introduces an efficient steganographic model. The proposed scheme shows high performance in important criteria including hiding capacity, robustness, and high imperceptibility; 2) compared with other schemes, the proposed scheme improves efficiency by increasing hiding capacity, ease of implementation, and high running efficiency.

The remainder of this paper is organized as follows. In Section II, the Discrete Hadamard Transform is introduced. In Section III, the proposed algorithm is presented. The performance analysis and a comprehensive comparison are reported in Section IV and Section V, respectively. Finally, the conclusions are drawn in Section VI.

II. DISCRETE HADAMARD TRANSFORM

The Hadamard Transform is a generalized form of the Fourier Transform. The Hadamard transform (HT) is a non-sinusoidal, orthogonal transformation that decomposes a signal into a set of orthogonal, rectangular waveforms [47]. Due to the computation being comprised of addition and subtraction, Hadamard Transform is more efficient than the Fast Fourier Transform [48].

To perform DHT on a $N \times N$ matrix where $N = 2^n$, the $N \times N$ Hadamard unitary matrix is generated by the following rule:

$$H_n = H_{n-1} \otimes H_1, \tag{1}$$

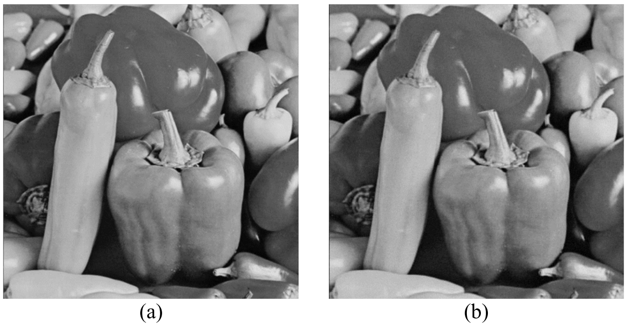


FIGURE 1. Original test image Peppers and the reconstructed Peppers with DHT coefficients values greater than 10 in absolute value. (a) Peppers; (b) reconstructed Peppers.

where H_n represents Hadamard unitary matrix of order n and $\otimes$ denotes Kronecker product of two matrices, and

$$H_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \tag{2}$$

$$H_2 = H_1 \otimes H_1 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}. \tag{3}$$

The orthogonality of the Hadamard unitary matrix is demonstrated as follows:

$$H_n = H_n^{-1} = H_n^T. \tag{4}$$

Thus, the transform core for forward and inverse Hadamard Transform is the same, which simplifies the calculation. The forward Discrete Hadamard Transform for an $N \times N$ matrix X is defined as follows:

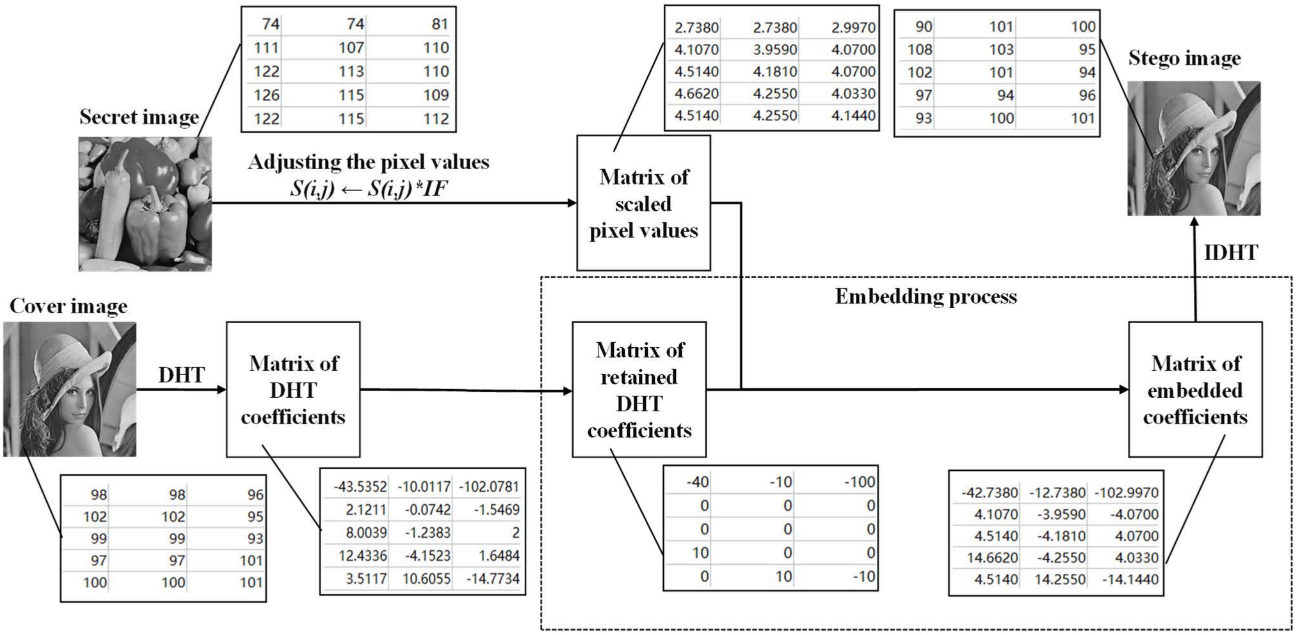
$$Y = \frac{H_n \times X \times H_n}{N}. \tag{5}$$

And the Inverse Discrete Hadamard Transform is calculated by the equation:

$$X = \frac{H_n \times Y \times H_n}{N}. \tag{6}$$

DHT is adopted for the following reasons: 1) easy implementation; 2) simplicity and high running efficiency; 3) moderate energy compacting. The features such as easy implementation and high running efficiency make the DHT more feasible in the application, especially in resource-limited situations [42].

The moderate energy compacting of DHT is shown in Fig. 1: most of the DHT coefficients are in the range of [−10,10]. In the instance, a 512 × 512 test image Peppers is converted to DHT coefficients and only the coefficients with absolute values larger than 10 are retained. The retained coefficients are approximately the top 20 percent of the amplitude of all coefficients. There is no noticeable difference between the two images by the naked human eye. The characteristic of DHT coefficients includes 1) the coefficients include both positive and negative values; 2) the most coefficients are small.


Secret image
Adjusting the pixel values
S(i,j) ← S(i,j)*IF
Matrix of scaled pixel values
Stego image
IDHT
Embedding process
Cover image
DHT
Matrix of DHT coefficients
Matrix of retained DHT coefficients
Matrix of embedded coefficients

74	74	81
111	107	110
122	113	110
126	115	109
122	115	112

2.7380	2.7380	2.9970
4.1070	3.9590	4.0700
4.5140	4.1810	4.0700
4.6620	4.2550	4.0330
4.5140	4.2550	4.1440

90	101	100
108	103	95
102	101	94
97	94	96
93	100	101

98	98	96
102	102	95
99	99	93
97	97	101
100	100	101

-43.5352	-10.0117	-102.0781
2.1211	-0.0742	-1.5469
8.0039	-1.2383	2
12.4336	-4.1523	1.6484
3.5117	10.6055	-14.7734

-40	-10	-100
0	0	0
0	0	0
10	0	0
0	10	-10

-42.7380	-12.7380	-102.9970
4.1070	-3.9590	-4.0700
4.5140	-4.1810	4.0700
14.6620	-4.2550	4.0330
4.5140	14.2550	-14.1440

FIGURE 2. A flowchart of the embedding procedure of the proposed method.

III. THE PROPOSED ALGORITHM

In the proposed scheme, DHT is applied to decompose the carrier image, the transformed coefficients are modified to embed the scaled secret image pixel value. The proposed algorithm consists of two phases: the embedding procedure and the extraction procedure.

A. PSEUDOCODE OF EMBEDDING ALGORITHM

The cover image is expected to be in RGB image format, either grayscale or color. Without loss of generality, suppose the cover image is a $N \times N$ grayscale image C and the secret data is a w $\times$ h grayscale image S (provided $w \leq N$ and $h \leq N$). For color images, the proposed method is applied in each channel separately. Besides, the cover images of size $m \times n\,(m \neq n)$ are also applicable for the algorithm, and can be sliced, trimmed or padded to make the image size meet the requirements. The pseudocode for embedding algorithm is detailed in ***Algorithm* 1**. Fig. 2 plots a flowchart of the embedding algorithm.

1) APPLYING DHT ON THE COVER IMAGE

The cover image C is converted to a $N \times N$ Hadamard coefficients matrix HC by using (5).

2) ADJUSTING THE EMBEDDED DATA

To reduce the distortion caused by embedding, the embedded value should be scaled to a possible range of the coefficient value. The embedded value range is defined as [0,Th] where Th is a predefined threshold value. The original range of pixel values in the secret image is [0,255]. Insert Factor (IF) is required in mapping the intensity of secret pixel values. For all pixel values $S(i,j)$, the intensity mapping is obtained by the formula: $S(i,j) \leftarrow S(i,j) * IF$. The mapped range is $[0, IF{*}255]$. The range $[0, IF{*}255]$ should be within the range [0,Th]. Thus, the theoretical max value $IF_{MAX} = Th/255$. To reduce the round-off error, the chosen IF value is usually smaller than the theoretical max value IF_{MAX}. The influence of parameters IF and Th values are discussed in Section IV.

3) EMBEDDING PROCESS

The secret data should be hidden in the coefficient values, and since the secret data are positive and the Hadamard coefficients contain both positive and negative values, the embedding process needs to be done in different ways depending on the positive and negative values.

Suppose $HC(i,j)$ represents the coefficient in the matrix HC at the position of the i-th row and j-th column. For the DHT coefficient $HC(i,j)$ in the selected embedding region $(1 \leq i \leq w, 1 \leq j \leq h)$:

1) if $0 < HC(i,j) \leq Th$, then $HC(i,j) \leftarrow 0$, else if $Th < HC(i,j)$, then $HC(i,j) \leftarrow HC(i,j) - Th$; for all the $0 < HC(i,j)$, let $HC(i,j) \leftarrow HC(i,j) + S(i,j)$.
2) if $-Th \leq HC(i,j) \leq 0$, then $HC(i,j) \leftarrow 0$, else if $-Th > HC(i,j)$, then $HC(i,j) \leftarrow HC(i,j) + Th$; for all the $HC(i,j) \leq 0$, let $HC(i,j) \leftarrow HC(i,j) - S(i,j)$.

After embedding, the coefficient values still maintain their original positivity and negativity. For all the modified coefficients $HC(i,j)$, the maximum absolute difference with the original coefficient values is within Th.

4) TRANSFORM THE EMBEDDED COEFFICIENTS TO SPATIAL DOMAIN

The stego-image matrix S' is obtained by applying IDHT on the matrix HC. After converting all pixel values in matrix S' into integers. The stego-image S' is produced.

Algorithm 1 Embedding Algorithm

```
Input: Cover Image $C$, Secret Image $S$, Threshold value $Th$, Insert Factor $IF$
 Output: Stego-Image: $S'$
$\begin{bmatrix} w & h \end{bmatrix} \leftarrow Size(S)$
$HC \leftarrow DHT(C)$
for $i \leftarrow 1$ to $w$ do
  for $j \leftarrow 1$ to $h$ do
    $S(i,j) \leftarrow S(i,j) * IF$
    if $HC\ (i,j) > 0$ then
      if $HC\ (i,j) \leq Th$ then
        $HC\ (i,j) \leftarrow 0$
      else
        $HC\ (i,j) \leftarrow HC\ (i,j) - Th$
      $HC\ (i,j) \leftarrow HC\ (i,j) + S(i,j)$
      end if
    else
      if $HC\ (i,j) \geq -Th$ then
        $HC\ (i,j) \leftarrow 0$
      else
        $HC\ (i,j) \leftarrow HC\ (i,j) + Th$
      $HC\ (i,j) \leftarrow HC\ (i,j) - S(i,j)$
      end if
    end if
  end for
end for
$S' \leftarrow IDHT(HC)$
$S' \leftarrow Integer(S')$
return $S'$
```

Algorithm 2 Extracting Algorithm

```
Input: Stego-Image: $S'$, Threshold value $Th$, Insert Factor $IF$
Image size $w$ and $h$
 Output: Recovered image $S$
$HC \leftarrow DHT(S')$
for $i \leftarrow 1$ to $w$ do
  for $j \leftarrow 1$ to $h$ do
    $HC'(i,j) \leftarrow Abs(HC(i,j))$
    if $HC'\ (i,j) \leq Th$ then
      $S'(i,j) \leftarrow HC'(i,j)$
    else
      $IHC\ (i,j) \leftarrow Integer(HC'\ (i,j))$
      $RHC\ (i,j) \leftarrow IHC\ (i,j) - Mod(IHC\ (i,j)\ , Th)$
      $S'(i,j) \leftarrow HC'(i,j) - RHC(i,j)$
    end if
    $S(i,j) \leftarrow S'(i,j)/IF$
  end for
end for
$S \leftarrow Integer(S)$
return $S$
```

B. PSEUDOCODE OF EXTRACTING ALGORITHM

In the extraction procedure, stego-image S', the Threshold value (Th), and Insert Factor (IF) are required. The secret image size w $\times$ h is provided unless the secret image size is the same as the cover image ($w = N$, $h = N$). The pseudocode for the extracting algorithm is detailed in ***Algorithm* 2**. Fig. 3 plots a flowchart of the extracting algorithm.

1) APPLYING DHT ON THE STEGO-IMAGE

The stego-image S' size is $N \times N$, and it is converted to a $N \times N$ Hadamard coefficients matrix HC by using (5).

2) EXTRACTING PROCESS

In the extracting process, the embedded data is extracted from DHT coefficients. The first step of the process is to convert all coefficients to absolute values. In the original coefficient values, coefficient values less than or equal to Th are replaced by secret data. Thus, for the coefficients $\{HC(i,j)|HC(i,j) \leq Th\}$, the secret is extracted directly.

For the DHT coefficient $HC(i,j)$ in the embedded region $(1 \leq i \leq w, 1 \leq j \leq h)$:

1) For all $HC(i,j)$, let $HC(i,j) \leftarrow Abs(HC(i,j))$.
2) If $HC(i,j) \leq Th$, let $S(i,j) \leftarrow HC(i,j)$.
3) Else let $IHC(i,j) \leftarrow Integer(HC(i,j))$, let $RHC(i,j) \leftarrow IHC(i,j) - Mod(IHC(i,j), Th)$, and let $S(i,j) \leftarrow HC(i,j) - RHC(i,j)$.

3) RECOVERING THE EXTRACTED DATA

The retrieved data should be scaled into the range of [0,255], For all values $S(i,j)$, let $S(i,j) \leftarrow S(i,j)/IF$ and then convert the values $S(i,j)$ into integers. The recovered image S is produced.

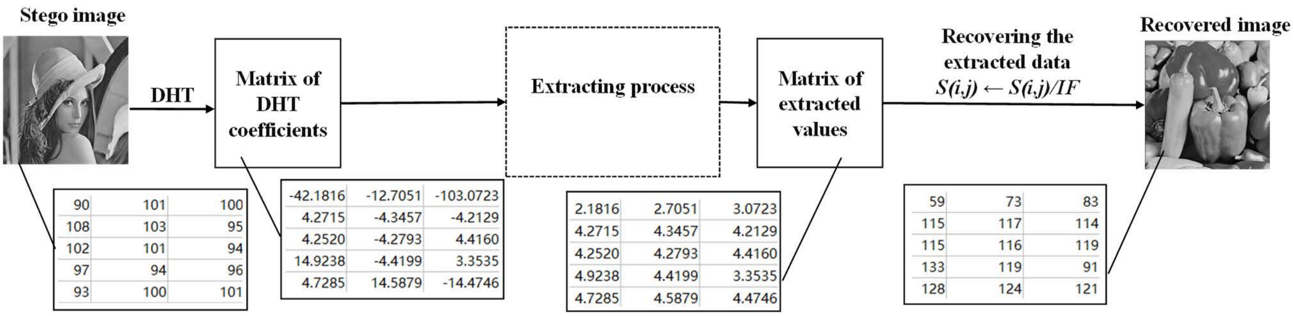
IV. PERFORMANCE ANALYSIS

To validate the proposed scheme, simulation experiment results and corresponding analysis are presented in this section. The experiments are conducted with MATLAB version R2019a on a desktop computer with 8G RAM and Intel (R) Core (TM) i7-7700 CPU (3.6GHZ). In our test, a famous large-scale dataset BOSSBase 1.01 [49] is used. Besides, to facilitate comparison with other well-known methods, the 512×512 pixels gray-scale images including Lena, Baboon, Lake, Jet, House, Peppers, Goldhill, and Boat are selected as test images. As shown in Fig. 4, all of these images quite popular in the research community [7], [29], [36], [45], [50]. In all tests, the retrieved images are Median filtered in the last step of the extraction process.

The performance metrics mentioned in this paper include Hiding Capacity (in BPP) and image quality (PSNR and SSIM).

The Hiding Capacity (HC) evaluates the amounts of bits that can be embedded in the cover image. It can be represented by Bits Per Pixel (BPP) and calculated:

$$HC = \frac{the\ number\ of\ embedded\ \ bits}{the\ number\ of\ pixels\ in\ the\ cover\ image}. \tag{7}$$


Stego image
DHT
Matrix of DHT coefficients
Extracting process
Matrix of extracted values
Recovering the extracted data
$S(i,j) \leftarrow S(i,j)/IF$
Recovered image

90	101	100
108	103	95
102	101	94
97	94	96
93	100	101

-42.1816	-12.7051	-103.0723
4.2715	-4.3457	-4.2129
4.2520	-4.2793	4.4160
14.9238	-4.4199	3.3535
4.7285	14.5879	-14.4746

2.1816	2.7051	3.0723
4.2715	4.3457	4.2129
4.2520	4.2793	4.4160
4.9238	4.4199	3.3535
4.7285	4.5879	4.4746

59	73	83
115	117	114
115	116	119
133	119	91
128	124	121

FIGURE 3. A flowchart of the extracting procedure of the proposed method.

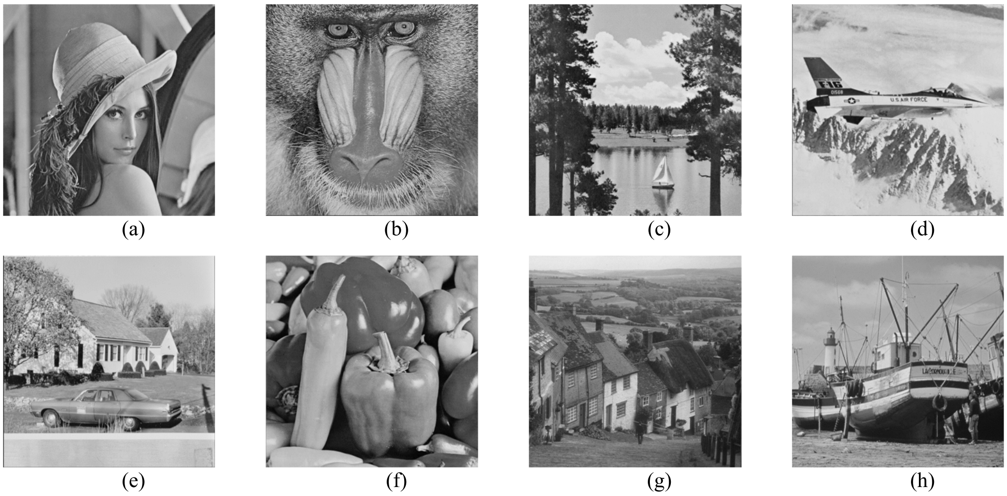


FIGURE 4. 8 classic test images. (a) Lena; (b) Baboon; (c) Lake; (d) Jet; (e) House; (f) Peppers; (g) Goldhill; (h) Boat.

Peak Signal to Noise Ratio (PSNR) and Structural Similarity Index Measure (SSIM) evaluate the similarity of two images. These metrics are usually used to measure the distortion in the stego-image caused by the embedding process. When the PSNR value is above 36 dB, the stego-image is indistinguishable from the original image for Human Visual System (HVS) [51]. For an 8-bit grayscale image, the PSNR is calculated:

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right). \tag{8}$$

Mean Squared Error (MSE) is defined as:

$$MSE = \frac{\sum_{i=1}^{N}(p_i - p_i')^2}{N}, \tag{9}$$

where N denotes the number of pixels in the cover image; p_i and p_i' represent the pixel value of the cover image and the stego-image, respectively.

Structural Similarity Index Measure (SSIM) is another metric for measuring the similarity of images. It is defined by:

$$SSIM = \frac{2\mu_x\mu_y + c_1}{\mu_x^2 + \mu_y^2 + c_1}\frac{2\sigma_{xy} + c_2}{\sigma_x^2 + \sigma_y^2 + c_2}, \tag{10}$$

where μ_x and μ_y are the mean value of images x and y. σ_x is the variance of image x, σ_y is the variance of image y, and σ_{xy} is the covariance of x and y. Without loss of generality, the parameters c_1 and c_2 are assigned to $(0.01 \times 255)^2$ and $(0.03 \times 255)^2$, respectively.

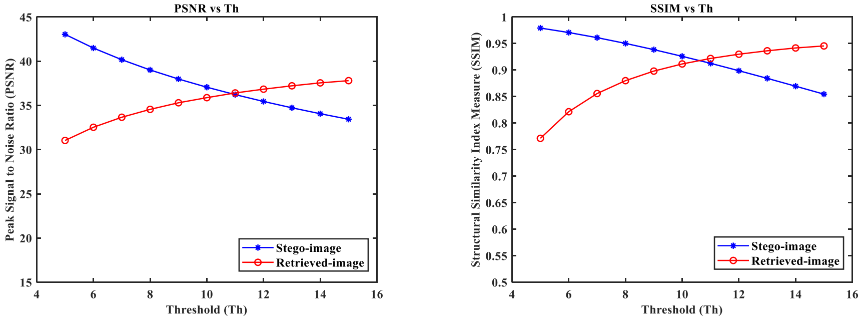
A. INFLUENCE OF PARAMETER ON SIMULATION RESULTS

In the proposed algorithm, the parameters include Th and IF. The scenarios of different parameters are conducted on 8 classical images.

Fig. 5 plots the variations of average PSNR and average SSIM with Th values varying from 5 to 15. In the simulation, the IF values are assigned to the corresponding theoretical max value IF_{MAX}. As shown in Fig. 5, The PSNR values and SSIM values of stego images decline with the Th value increasing. Whereas the PSNR and SSIM values of recovered images rise with the Th value increasing. There is a trade-off between imperceptibility and reversibility.

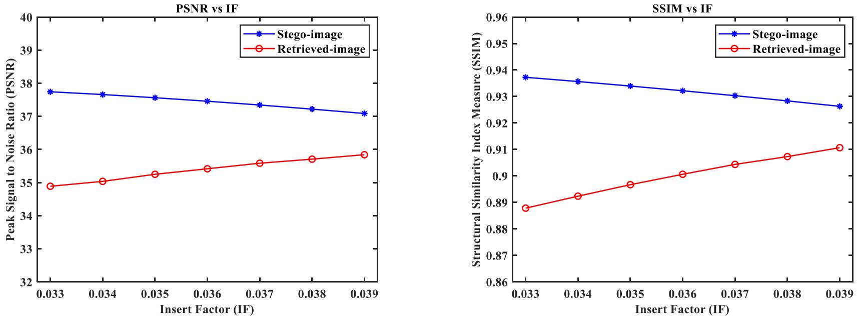
Without loss of generality, in the rest of the experiments, the threshold value Th is assigned to 10. In this case, the PSNR value of the stego images is above 37 dB and the recovered image is about 35 dB.

In the case of Th =10, the theoretical max value for IF is $IF_{MAX} = Th/255 = 10/255 \approx 0.0392$. Fig. 6 plots



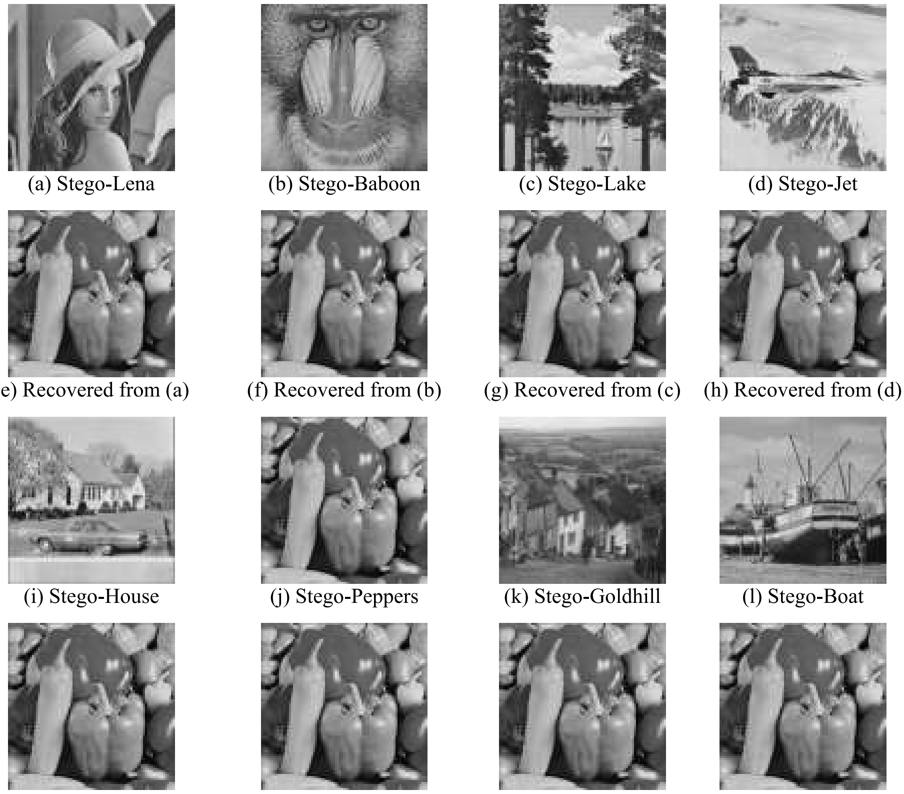
(a) (b)

FIGURE 5. PSNR and SSIM values on different Th values. (a) PSNR vs Th; (b) SSIM vs Th.



(a) (b)

FIGURE 6. PSNR and SSIM values on different IF values. (a) PSNR vs IF; (b) SSIM vs IF.



(a) Stego-Lena (b) Stego-Baboon (c) Stego-Lake (d) Stego-Jet

(e) Recovered from (a) (f) Recovered from (b) (g) Recovered from (c) (h) Recovered from (d)

(i) Stego-House (j) Stego-Peppers (k) Stego-Goldhill (l) Stego-Boat

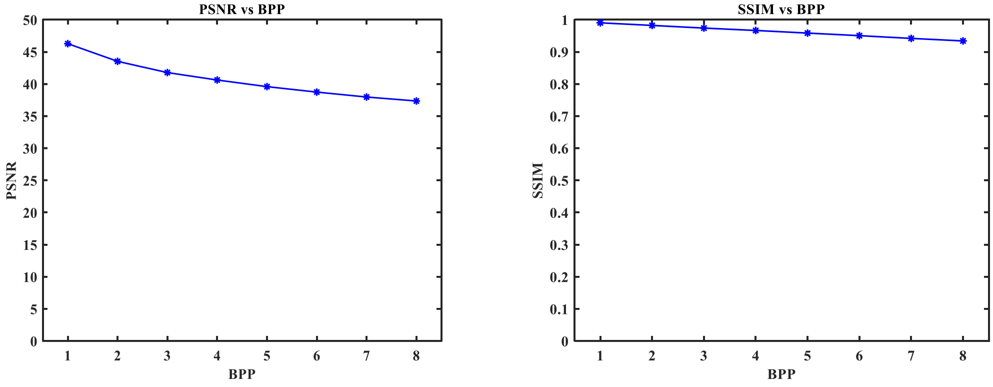
(m) Recovered from (i) (n) Recovered from (j) (o) Recovered from (k) (p) Recovered from (l)

FIGURE 7. Stego-image and Retrieved image for 8 classic test images.

the variations of average PSNR and average SSIM with *IF* values varying from 0.033 to 0.039 and 0.001 as the interval. PSNR values and SSIM values of stego images decline with the *IF* value increasing. Whereas the PSNR and SSIM values of recovered images rise with the *IF* value increasing. Within the range of [0.033,0.039], the higher the *IF* value, the worse

TABLE 1. PSNR and SSIM values for different cover images.

Hiding capacity (BPP)	Cover image (512×512)	PSNR (dB)		SSIM	
		Stego-image	Retrieved image	Stego-image	Retrieved image
8	Lena	37.4676	35.5873	0.9185	0.9045
	Baboon	37.2682	35.5841	0.9713	0.9046
	Lake	37.3695	35.5607	0.9406	0.9042
	Jet	37.2491	35.5890	0.9066	0.9036
	House	37.4131	35.5872	0.9331	0.9048
	Peppers	37.1518	35.5733	0.9067	0.9043
	Goldhill	37.4308	35.5922	0.9418	0.9044
	Boat	37.3879	35.5988	0.9238	0.9044



(a) (b)

FIGURE 8. PSNR and SSIM values on different hiding capacities (in BPP). (a) PSNR vs BPP; (b) SSIM vs BPP.

TABLE 2. PSNR and SSIM values for BOSSBASE images.

Hiding capacity (BPP)	Cover image (512×512)	Average PSNR (dB)		Average SSIM	
		Stego-image	Retrieved image	Stego-image	Retrieved image
8	1000 images	37.3508	35.4717	0.9128	0.9020

the imperceptibility, but the better the quality of the recovered images. To reduce the round off error, we set the *IF* value as 0.037 in the rest experiments.

B. HIDING CAPACITY VERSUS IMPERCEPTIBILITY

Fig. 7 displays the simulation results in 8 different cover images, respectively. The default parameter *IF* and *Th* are assigned to be 0.037 and 10, respectively. There is no difference by naked human eye between the original test cover images and the stego-images. The corresponding quantitative analyses including PSNR and SSIM are shown in Table 1. The PSNR values of the stego-image are larger than 37 dB while the hiding capacity is 8 BPP, and SSIM values are larger than 0.90. The recovered secret image is also of high quality: PSNR values are around 35 dB and SSIM values are around 0.90.

The simulation results on different hiding capacities are plotted in Fig. 8. As shown in the figure, the average PSNR and average SSIM values of the stego-images and cover images both decrease with the hiding capacity increasing from 1 BPP to 8 BPP. It can justify that the imperceptibility of the stego-images is not significantly degraded in the case of high hidden capacity. Even in the max hiding capacity (8 BPP), the PSNR value still maintains above 36 dB (approximately 37 dB). To maximize the use of payload, 8 BPP is recommended in the application.

To further evaluate the influence of different carriers, we conduct the proposed method in a large-scale image dataset: BOSSbase 1.01. The simulation results performed on 1000 images are shown in Table 2. As shown in the Table, the proposed method maintains a stable high performance in the large-scale tests.

Table 3 demonstrates the comparison with other high-capacity schemes. As is shown in the Table, the proposed scheme shows more stability and better performance in both Hiding Capacity (in BPP) and image quality (in PSNR).

To show the proposed method is also applicable for color images, we test the classical color images and the simulation results are shown in Fig. 9. It can be observed that, as with the results of the grayscale images, the color stego-images also show no visible distortion to the naked eye. The PSNR and SSIM values of the stego-image are 36.68 dB and 0.9943, respectively. Besides, the retrieved image also maintains high quality. The corresponding PSNR and SSIM values are 32.74 dB and 0.9847.

TABLE 3. Comparison with existing high capacity image steganographic schemes.

Cover image	Atta *et al.* (2018) [50]		Muhuri *et al.* (2020) [29]		Yu (2015) [7]		Ghasemi *et al.* (2012) [36]		Proposed	
	BPP	PSNR	BPP	PSNR	BPP	PSNR	BPP	PSNR	BPP	PSNR
Lena	3.36	31.27	4	35.69	4.68	30.02	5	32.04	**8**	**37.47**
Baboon	3.34	32.44		36.28	4.64	30.19		32.79		**37.27**
Jet	3.33	31.46		36.60	4.67	30.07		**37.45**		37.25
Boat	-	-		36.44	-	-		31.17		**37.39**
Peppers	3.32	31.72	-	-	4.68	29.98	-	-		**37.15**
Lake	3.35	31.94	-	-	4.66	30.10	-	-		**37.37**

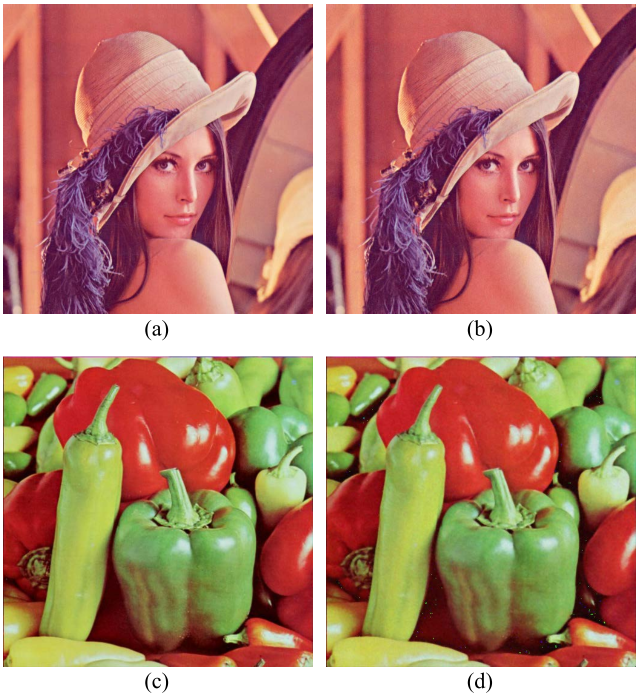

(a) (b) (c) (d)

FIGURE 9. Cover image Lena, secret image Peppers, the corresponding stego-image, and corresponding retrieved image. (a) color-Lena; (b) stego-Lena; (c) color-Peppers; (d) retrieved-Peppers.

C. ROBUSTNESS ANALYSIS

With steganography, robustness refers to the ability to extract hidden data from corrupted stego-files. Unlike watermarking, robustness is not the primary goal of steganography. For watermarking, the stego-files must be able to withstand various deliberate attacks such as rotation, sharpening, etc. For steganography, however, active attack scenarios are not a consideration [6].

Although high robustness to active attacks is not a mandatory requirement for steganography. However, in the real world, the stego-images may encounter some unintended attacks during transmission. The critical secret data may be lost during transmission, thus steganography should maintain robustness against various possible image attacks [32]. We test the proposed method with those possible scenarios such as compression attacks, noise attacks, and cropping attacks. In the test, image Peppers is embedded in Lena, the hiding capacity is 8 BPP.

In the experiments, three common noises: Gaussian White noise, Salt and Pepper noise, and Speckle noise are added to the stego-image, respectively. The simulation results of noise attacks are displayed in Fig. 10. As shown in the picture, retrieved secret images Peppers from stego-image with Gaussian white noise are illustrated in the first row. And the PSNR values are 27.42 dB, 24.99 dB, and 21.02 dB from left to right. In the second row, the PSNR values of the retrieved image are 32.91 dB, 29.82 dB, and 29.09 dB from the stego-image with Salt and Pepper noise. Fig. 10 (g)-(i) displays the retrieved image from stego-images with Speckle noise. The corresponding PSNR values are 30.95 dB, 29.38 dB, and 26.47 dB. Fig. 10 indicates that the proposed scheme owns desirable resistance against various noise attacks.

The retrieved images from stego-images with JPEG compression at different Quality Factors (QF) are plotted in Fig. 11. The PSNR values are 22.15 dB, 16.30dB, and 13.94 dB, respectively. As shown in the picture, the retrieved images still hold a certain degree of similarity at $QF = 85$. This indicates that the proposed method can resist compression attacks to a certain extent.

Stego-image with center cropped is depicted in Fig.12 (a)-(c). The cropping size varies from 32×32, 64×64, and 128×128. The retrieved image Peppers are shown in Fig.12 (d)-(f) And the PSNR values are 22.67 dB, 20.03 dB, and 16.31 dB, correspondingly.

The stego-image with corner cropping is shown in Fig.12 (g)-(i). The cropping size is 32×32, 64×64, and 128×128. Fig.12 (j)-(l) shows the influence of corner cropping. The PSNR values are 33.52 dB, 29.66 dB, and 23.76 dB, respectively. As is shown in Fig.12 (l), in the situation of 128×128 size cropped (6.25% data loss), we successfully retrieve the secret image. The simulation results demonstrate that the proposed scheme owns desirable resistance against the cropping attack.

D. SECURITY ANALYSIS

For steganography, the term "security" indirectly refers to undetectability. Hence a steganographic scheme is considered secure as long as the hidden data is not detectable by statistical means [6]. Those means, also known as steganalysis, refer to the method that aims to detect the presence of secret data based on the modification traces of stego-media [52].

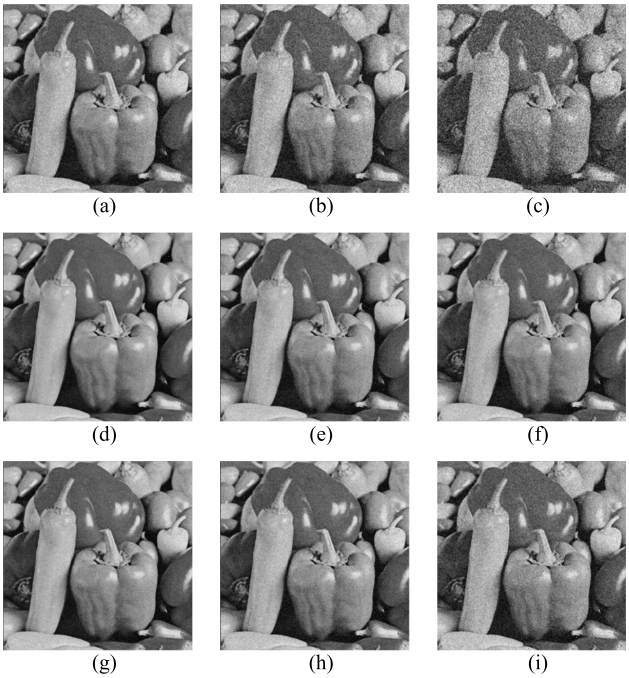


FIGURE 10. Robustness test results against noise attack for extracted image Peppers and carrier image Lena. (a)-(c) are extracted-Peppers from stego-image with zero-mean Gaussian noise. And the variance is (a) 0.00001, (b) 0.00002, and (c) 0.00005. (d)-(f) are extracted-Peppers from stego-image with Salt and Pepper noise. The density is (d) 0.00001, (e) 0.00002, and (f) 0.00005. (g)-(i) are extracted-Peppers from stego-image with Speckle noise. The variance is (g) 0.00001, (h) 0.00002, and (i) 0.00005.

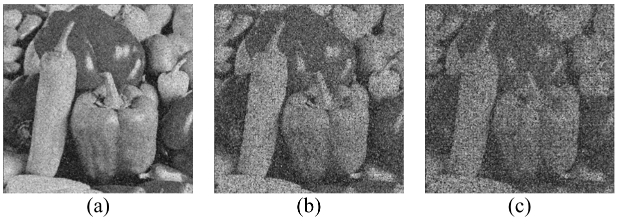


FIGURE 11. Recovered images from stego-images after JPEG compression. (a) QF = 95; (b) QF = 90; (c) QF = 85.

To demonstrate the security of the proposed scheme, we have performed two well-known steganalysis technologies on the proposed scheme: RS attack, and Chi-square attack. In the test, we randomly choose the test image Peppers as the secret image and six test images as the cover images: Lena, Baboon, Lake, Jet, House, and Peppers. Besides, the 1-bit LSB is utilized for comparison. For the LSB method, the secret data is randomly generated and is embedded sequentially. For the proposed scheme, the secret image is resized to meet the requirements of the experimental condition.

As an efficient steganalysis against LSB steganography, RS analysis not only can detect the existence of secret bits but also can estimate the embedding payload [17]. In RS analysis, all the pixels of the image will be divided into disjoint groups. A discrimination function with flipping mask m is designed to capture the smoothness of the group of pixels. And the groups are classified into three groups: regular groups R_m and R_{-m}, singular groups S_m and S_{-m}, and unusable groups.

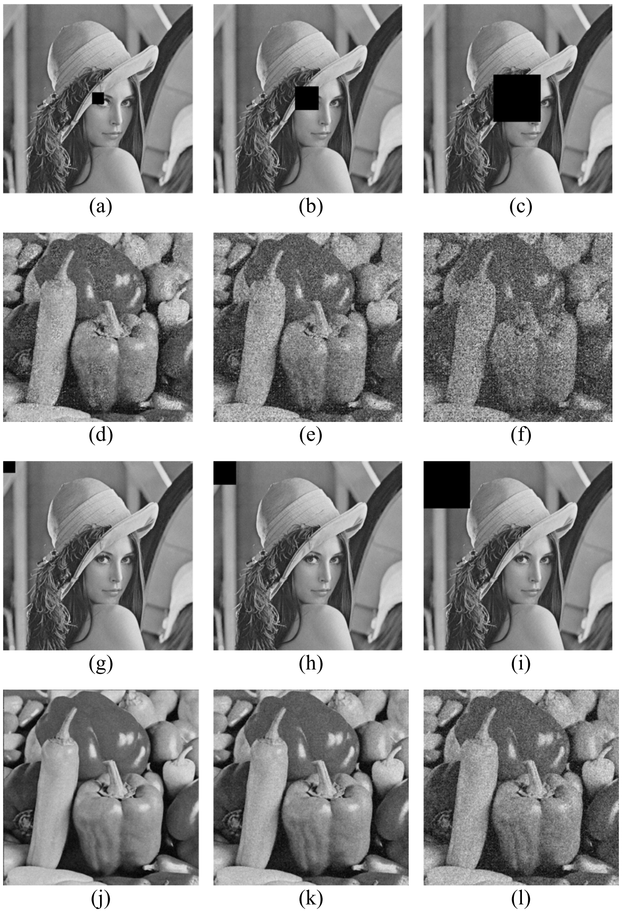
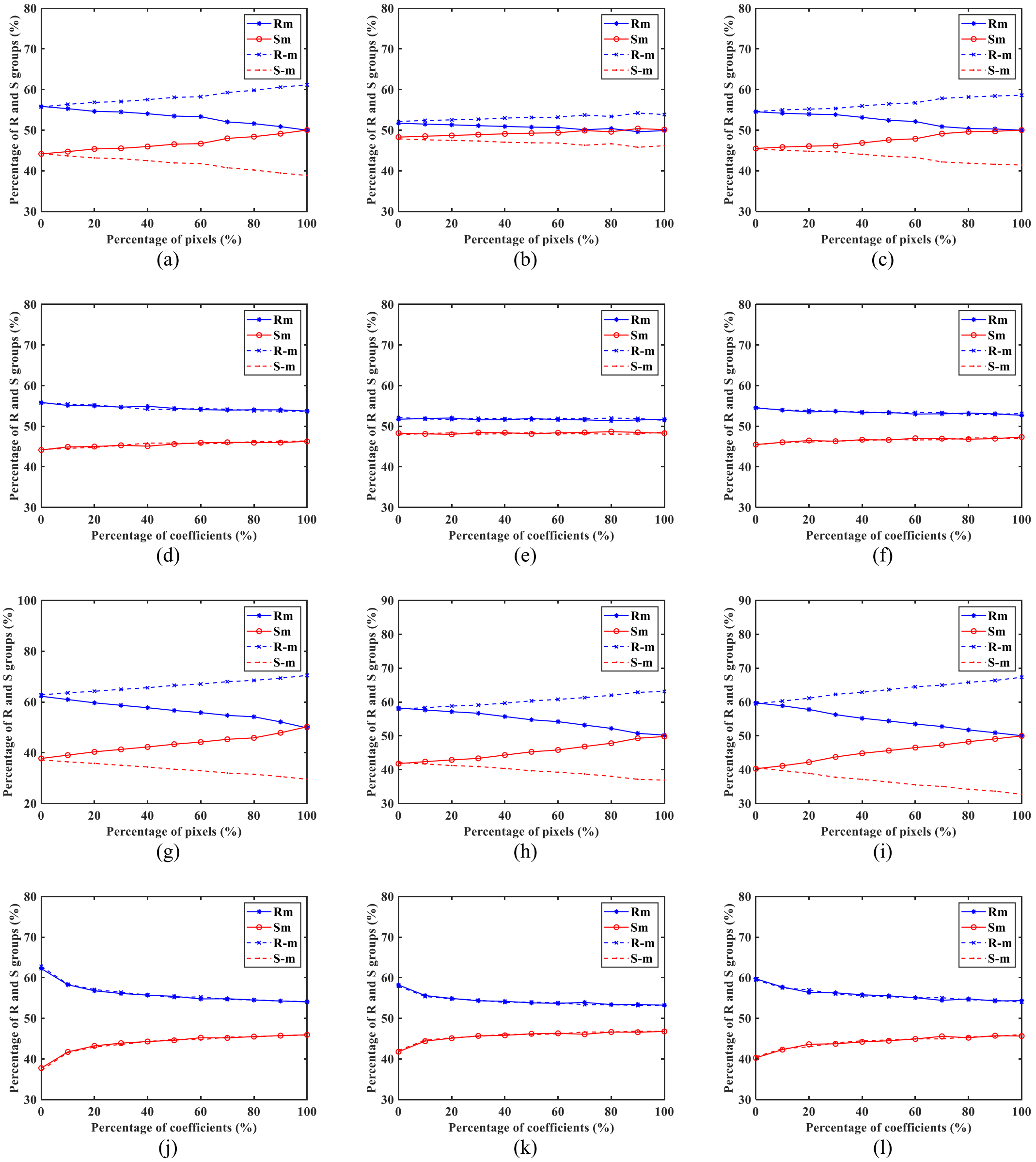


FIGURE 12. Robustness test results against cropping attack for secret image Peppers and carrier image Lena. (a)-(c) are stego-image with center crop by different size, (d)-(f) are corresponding extracted image; (g)-(i) are stego-image with corner crop by different size, (j)-(l) are extracted image from (g)-(i) respectively.

The idea of detection is based on the hypothesis: for a typical natural image (image without any hidden data), R_m is close to R_{-m} and S_m is close to S_{-m} either, i.e., $R_m \cong R_{-m}$ and $S_m \cong S_{-m}$. In contrast, the difference between (R_m, R_{-m}) and (S_m, S_{-m}) of stego-image will increase with the percentage of pixels used in the embedding increasing.

The security of the proposed scheme against RS analysis is shown in Fig.13. The masks used in the test: $m = \{1, 0, 1, 0\}$ and $-m = \{-1, 0, -1, 0\}$. For the RS diagram of the LSB method, the difference of (R_m, R_{-m}) and (S_m, S_{-m}) increase with the percentage of pixels embedded increasing, which means the LSB method is easily detected. In contrast, for the proposed scheme, the difference between R_m and R_{-m} along with the difference between S_m and S_{-m} are both close to zero. It demonstrates that the proposed scheme can resist the RS attack in the various payload.

The Chi-square attack is a statistical analysis method proposed in the work [53]. The fact about 1-bit substitute LSB is found: only the last bits change from either 0 to 1 or 1 to 0. Thus, the sum of frequency for each adjacent two-pixel value is consistent before and after embedding. These two-pixel value pairs are called Pair Of Values (POVs) [54]. For



(a) (b) (c)

(d) (e) (f)

(g) (h) (i)

(j) (k) (l)

FIGURE 13. RS diagrams for six different cover images in LSB scheme and the proposed scheme. (a)-(c) and (g)-(i) are from LSB scheme, (d)-(f) and (j)-(k) are from the proposed scheme. (a) Lena; (b) Baboon; (c) Lake; (d) Lena; (e) Baboon; (f) Lake; (g) Jet; (h) House; (i) Peppers; (j) Jet; (k) House; (l) Peppers.

instance, 0 and 1, 2 and 3, etc. The Chi-square method calculates Chi-square statistics based on the frequency distribution of POVs in the image and produces an embedding probability.

The Chi-square attack is performed on the stego-image with different percentages of pixels or coefficients used from 0% to 100%. For each cover image with a different payload, the expected probability of embedding data is depicted in a diagram. The horizontal axis is the percentage of modified pixels or coefficients and the vertical axis is the probability of embedding data. For an ideal scheme, the embedding probability is expected to have a consistent probability with the raw cover image (image without any hidden data).

As is shown in Fig. 14, for most test cases, the embedding probability is near 1 when the percentage of embedded pixels is higher. Thus, the LSB scheme is easily detected. In contrast, for the proposed scheme, the expected probability is consistent with zero in most cases. In a few exceptional cases, the expected probability is higher than the case of 0% embedded data. These cases include the test image Baboon with a modified percentage of 30% and 70%. However, 100% payload is the most commonly used in the application. Hence, we can still conclude that the proposed scheme owns high resistance to the Chi-square attack.

The steganalysis methods are used as the classifier to distinguish the stego-images from normal images (without any data hidden). To better show the performance in security, we draw the Receiver Operating Characteristic (ROC) curves in Fig. 15. ROC curve is a performance measurement for classification problems at various threshold settings. the AUC (Area Under the Curve) represents the degree of differentia-

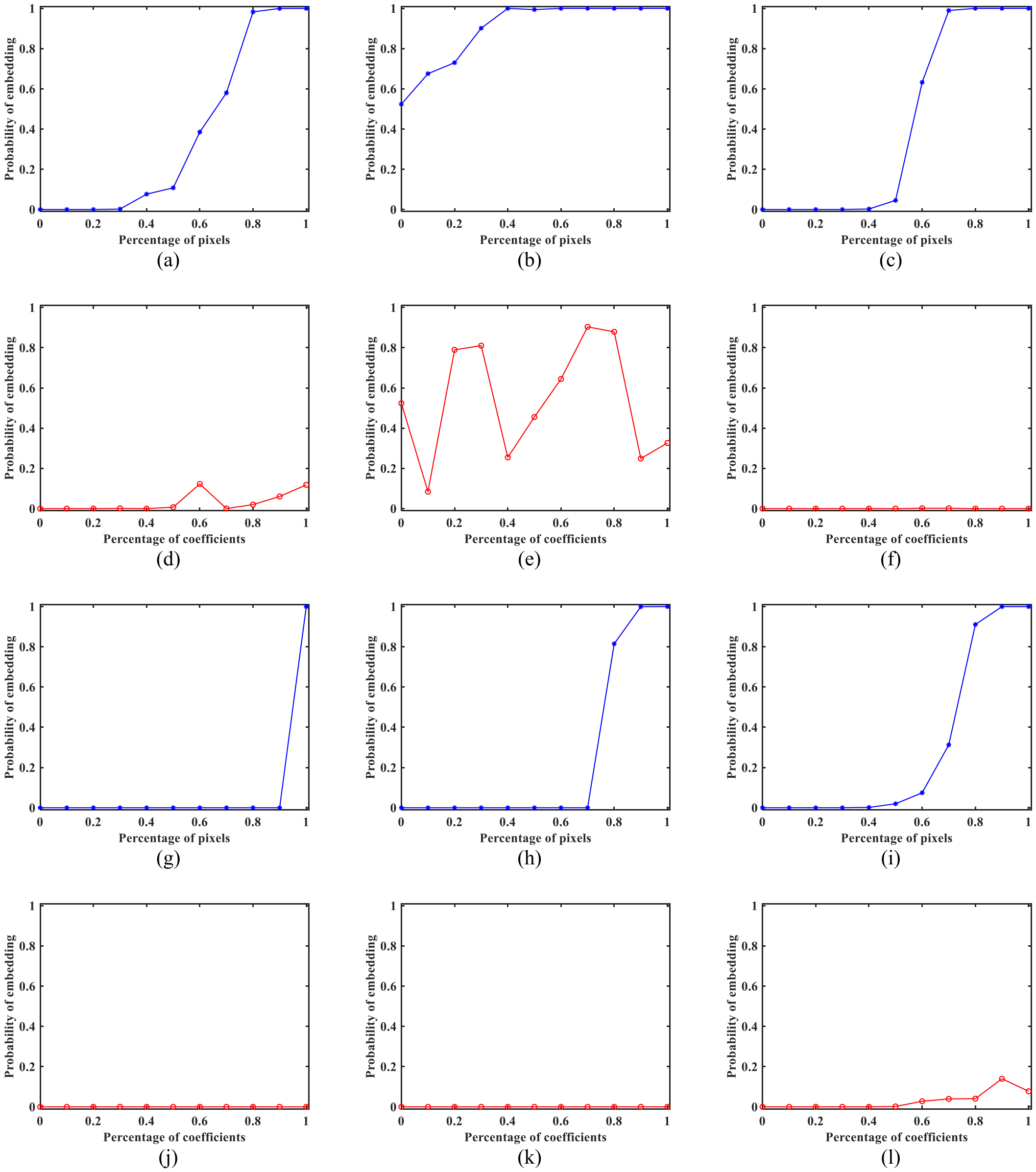


FIGURE 14. Chi-squared embedding probability with different cover and payload. (a)-(c) and (g)-(i) are from LSB scheme. (d)-(f) and (j)-(l) are from the proposed scheme. (a) Lena; (b) Baboon; (c) Lake; (d) Lena; (e) Baboon; (f) Lake; (g) Jet; (h) House; (i) Peppers; (j) Jet; (k) House; (l) Peppers.

bility. the higher the AUC, the better ability of the classifier in prediction. When the AUC is 0.5, it means that the model does not have any category separation capability.

For both ROC curves plotted in Fig. 15, the AUC is relatively small (close to 0.5). This indicates that both methods do not classify effectively, i.e., it is difficult to distinguish stego-images from the normal images. Thus, the proposed scheme shows high security against both attacks.

V. COMPARISON WITH THE RELATED SCHEME

In this section, we provide a comprehensive comparison with related schemes. For comparison, we have considered a lot of related works in the spatial domain and transform domain. Table 4 list a comparative review of the major features of these soft-of-the-art schemes with the proposed scheme. We embed secret data in some famous test images and compare it with other schemes in terms of hiding capacity and visual quality of Stego-image (in PSNR). Besides, other considered properties include robustness, security, and the channel's payload. The property "Channel's payload" refers to the data size that needs to be transferred through the channel to the receiver side. For a fair comparison, the hiding capacity is calculated by the information provided in some works. For the proposed scheme, both the cover image size and secret image size are 512×512. Thus, the hiding capacity of the proposed scheme is 100% or 8 BPP.

Reference [36] proposes a high-capacity scheme based on DWT. The scheme utilizes GA to search for an optimal mapping matrix. Based on the obtained substitution matrix, the secret data is embedded in the less significant

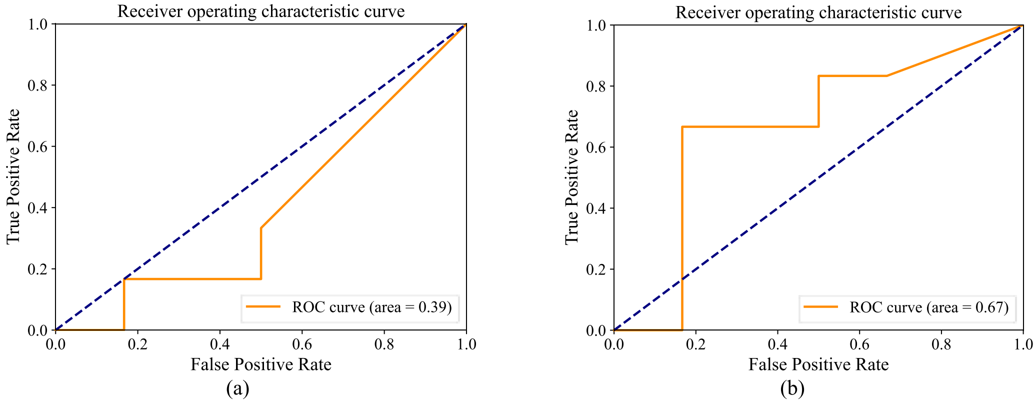


FIGURE 15. ROC curves for RS attack and Chi-square attack. (a) ROC curve for RS attack; (b) ROC curve for Chi-square attack.

TABLE 4. Overall comparison with related image steganographic schemes.

Algorithm	Cover image	Hiding Payload (%)	PSNR	Security	Robustness	Channel's payload
[36] (2011)	Lena Baboon Jet	62.5	32.04 32.79 37.45	Not reported	Not reported	Stego-images and a 4×4 mapping matrix
[38] (2014)	Baboon Jet Peppers	49.4	35.42 34.67 34.93	Not reported	Not reported	Stego-images
[29] (2020)	Lena Baboon Jet	37.5	35.69 36.28 36.60	RS-attack and Chi-square attack	Common image processing	Stego-images
[7] (2015)	Lena Baboon Jet	58.5 58.0 58.4	30.02 30.19 30.07	Not reported	Not reported	Stego-images
[33] (2018)	Lena Baboon	65.9 69.8	43.91 42.17	Not reported	Not reported	Stego-file and cover image
[27] (2018)	Lena Goldhill	25	44.84 43.22	Relative entropy measure	Common image processing	Stego-images and retrieve position (4 positions for a 4×4 block)
The proposed	Lena Baboon Jet Goldhill Peppers	100	37.47 37.27 37.25 37.43 37.15	RS-attack and Chi-square attack	Common image processing	Stego-images

coefficients. and Optimal Pixel Adjust Process (OPAP) is applied to reduce the difference error between stego-image and cover image. Reference [38] introduces another high-capacity scheme based on GA. In this scheme, an optimal chromosome with seven genes is generated by GA, and the mapping rules are defined by the chromosome. Compared with the scheme [36], the search space is less and the scheme also achieves high capacity. Both schemes achieve a high hiding payload. As shown in Table 4, even with the much higher payload, the proposed scheme show superiority over the scheme in visual quality. Besides, the robustness and security are not proven in these methods but our method shows high robustness and high security.

Reference [29] presents an adaptive steganographic model based on PSO. Based on the idea of the search optimal substitution matrix, the scheme utilizes the coefficients of LH, HL, and HH bands to conceal secret messages. Unlike the scheme, this approach conceals the substitution matrix in the predefined position. Thus, no supporting data needs to be sent via an extra channel. The scheme [29] shows robustness and security against various attacks. However, the disadvantage of the method lies in the time-consuming optimization. Besides, in the case of n = 4, the payload is $256 \times 256 \times 3 \times 4$ and equal to 786432 bits. Considering the used image size is 512×512. Thus, the maximum hiding payload of the scheme is only 37.5%. Compared with the 100% hiding payload of our methods, the payload is poor.

The above-mentioned schemes are all complex and time-consuming. Reference [7] introduces a simple and high-capacity LSB-based scheme. Different from the traditional LSB-based technologies, this model utilizes the Median Edge Detector (MED) to locate the complex area of the cover image. To reduce the sensitivity of HVS, fewer secret data is embedded in the flat area. Besides, OPAP is also applied to reduce image distortion. The proposed scheme shows an edge over the scheme [7] in the hiding capacity, visual quality, robustness, and security.

Reference [33] introduces a scheme based on edge detection over DT-CWT. The cover image is split into non-overlapping blocks and the textured patch will be embedded with more messages. The scheme could produce high-quality stego-images with a high payload. However, the main disadvantage is that a duplicate of the original cover image is required on the receiver side. Scheme [27] utilizes Root Mean Square Method (RMSE) as the criteria to match the block of the secret image with the block of the cover image. However, though the used secret image size is the same as the cover image, only the LL band coefficients are embedded and the hiding payload is only 25%. Even though the scheme is slightly better in terms of image quality, it is safe to say that our method is superior considering that our hiding capacity is four times higher. Moreover, the scheme needs a very considerable retrieve position in the extraction process but our method requires nothing.

From the above discussion, we can conclude that the proposed scheme is efficient image steganography. Compared with the related scheme, the superiority of the proposed one is mainly reflected in the hiding capacity, visual quality, and payload in the channel.

VI. CONCLUSION

This paper presents an efficient image steganographic scheme. As a computationally efficient transform, DHT is adopted to convert the cover image. Based on the nature of DHT coefficients, an efficient embedding strategy based on substitution is utilized in the embedding procedure. In experiments conducted on over 1000 images, the proposed scheme produces high-quality stego-images and retrieved images in the dense embedding of 100%. For robustness, the proposed scheme is tested with cropping attacks, JPEG compression, and three types of noise attacks. For security, the proposed scheme can resist the RS attack and Chi-square attack. Besides, a comparative analysis shows that our scheme achieves good visual quality and higher hiding capacity than the other schemes. Thus, we can conclude that our scheme outperforms other former schemes.

In future work, we will investigate the DHT-based image steganography combined with edge detection technologies.

ACKNOWLEDGMENT

This work has been co-funded by the European regional development Fund under EU Interreg 2 Seas, CoBra Project Grant 2S04-022 and EU Interreg 2 Seas, SPEED Project Grant 2S04-019.

REFERENCES

[1] A. K. Sahu and M. Sahu, “Digital image steganography and steganalysis: A journey of the past three decades,” *Open Comput. Sci.*, vol. 10, no. 1, pp. 296–342, Oct. 2020.

[2] C. Vanmathi and S. Prabu, “Image steganography using fuzzy logic and chaotic for large payload and high imperceptibility,” *Int. J. Fuzzy Syst.*, vol. 20, no. 2, pp. 460–473, Feb. 2018.

[3] A. Gupta and A. Chaudhary, “A Metaheuristic method to hide MP3 sound in JPEG image,” *Neural Comput. Appl.*, vol. 30, no. 5, pp. 1611–1618, Sep. 2018.

[4] M. S. Subhedar and V. H. Mankar, “Current status and key issues in image steganography: A survey,” *Comput. Sci. Rev.*, vols. 13–14, pp. 95–113, Nov. 2014.

[5] M. Dalal and M. Juneja, “Steganography and steganalysis (in digital forensics): A cybersecurity guide,” *Multimedia Tools Appl.*, vol. 80, no. 4, pp. 5723–5771, Feb. 2021.

[6] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Hallorana, “Comprehensive survey of image steganography: Techniques, evaluations, and trends in future research,” *Neurocomputing*, vol. 335, pp. 299–326, Mar. 2019.

[7] Y. Wang, “The LSB-based high payload information steganography,” in *Proc. Int. Conf. Mechatronics, Electron., Ind. Control Eng.*, 2015, pp. 776–779.

[8] 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.

[9] L. Laimeche, A. Meraoumia, and H. Bendjenna, “Enhancing LSB embedding schemes using chaotic maps systems,” *Neural Comput. Appl.*, vol. 32, no. 21, pp. 16605–16623, Nov. 2020.

[10] Y. Jia, Z. Yin, X. Zhang, and Y. Luo, “Reversible data hiding based on reducing invalid shifting of pixels in histogram shifting,” *Signal Process.*, vol. 163, pp. 238–246, Oct. 2019.

[11] F. Pan, J. Li, and X. Yang, “Image steganography method based on PVD and modulus function,” in *Proc. Int. Conf. Electron., Commun. Control (ICECC)*, Sep. 2011, pp. 282–284.

[12] A. K. Sahu and G. Swain, “An optimal information hiding approach based on pixel value differencing and modulus function,” *Wireless Pers. Commun.*, vol. 108, no. 1, pp. 159–174, 2019.

[13] A. K. Sahu, G. Swain, M. Sahu, and J. Hemalatha, “Multi-directional block based PVD and modulus function image steganography to avoid FOBP and IEP,” *J. Inf. Secur. Appl.*, vol. 58, May 2021, Art. no. 102808.

[14] R. Kumar and S. Chand, “A reversible data hiding scheme using bit flipping strategy,” *J. Discrete Math. Sci. Cryptogr.*, vol. 19, no. 2, pp. 331–345, Mar. 2016.

[15] A. K. Sahu, G. Swain, and E. S. Babu, “Digital image steganography using bit flipping,” *Cybern. Inf. Technol.*, vol. 18, no. 1, pp. 69–80, 2018.

[16] R. Chu, X. You, X. Kong, and X. Ba, “A DCT-based image steganographic method resisting statistical attacks,” in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*, May 2004, pp. 953–956.

[17] J. Fridrich, M. Goljan, and R. Du, “Reliable detection of LSB steganography in color and grayscale images,” in *Proc. Workshop Multimedia Secur.*, 2001, pp. 27–30.

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

[19] A. K. Sahu and G. Swain, “Reversible image steganography using dual-layer LSB matching,” *Sens. Imag.*, vol. 21, no. 1, pp. 1–21, Dec. 2020.

[20] G. Swain and A. Sahu, “A novel multi stego-image based data hiding method for gray scale image,” *Pertanika J. Sci. Technol.*, vol. 27, pp. 753–768, May 2019.

[21] A. K. Sahu and G. Swain, “High fidelity based reversible data hiding using modified LSB matching and pixel difference,” *J. King Saud Univ. Comput. Inf. Sci.*, vol. 34, no. 4, pp. 1395–1409, Apr. 2022.

[22] Q. Li, X. Wang, X. Wang, B. Ma, C. Wang, Y. Xian, and Y. Shi, “A novel grayscale image steganography scheme based on chaos encryption and generative adversarial networks,” *IEEE Access*, vol. 8, pp. 168166–168176, 2020.

[23] C. Pak, J. Kim, K. An, C. Kim, K. Kim, and C. Pak, “A novel color image LSB steganography using improved 1D chaotic map,” *Multimedia Tools Appl.*, vol. 79, nos. 1–2, pp. 1409–1425, Jan. 2020.

[24] J. Sun and Y. Song, “Image based information hiding with one-dimensional chaotic systems and particle swarm optimization,” in *Proc. IEEE 11th Int. Conf. Electron. Inf. Emergency Commun. (ICEIEC)*, Jun. 2021, pp. 108–111.

[25] Y. K. Lin, “A data hiding scheme based upon DCT coefficient modification,” *Comput. Standards Int.*, vol. 36, no. 56, pp. 855–862, Sep. 2014.

[26] A. A. Attaby, M. F. M. M. Ahmed, and A. K. Alsammak, “Data hiding inside JPEG images with high resistance to steganalysis using a novel technique: DCT-M3,” *Ain Shams Eng. J.*, vol. 9, no. 4, pp. 1965–1974, Dec. 2018.

[27] V. Kumar and D. Kumar, “A modified DWT-based image steganography technique,” *Multimedia Tools Appl.*, vol. 77, no. 11, pp. 13279–13308, Jun. 2018.

[28] R. Thanki and S. Borra, "A color image steganography in hybrid FRT–DWT domain," *J. Inf. Secur. Appl.*, vol. 40, pp. 92–102, Jun. 2018.

[29] P. K. Muhuri, Z. Ashraf, and S. Goel, "A novel image steganographic method based on integer wavelet transformation and particle swarm optimization," *Appl. Soft Comput.*, vol. 92, Jul. 2020, Art. no. 106257.

[30] A. Miri and K. Faez, "An image steganography method based on integer wavelet transform," *Multimedia Tools Appl.*, vol. 77, no. 11, pp. 13133–13144, Jun. 2018.

[31] S. Singh and T. J. Siddiqui, "Robust image steganography using complex wavelet transform," in *Proc. IMPACT*, 2013, pp. 56–60.

[32] I. J. Kadhim, P. Premaratne, and P. J. Vial, "Improved image steganography based on super-pixel and coefficient-plane-selection," *Signal Process.*, vol. 171, Jun. 2020, Art. no. 107481.

[33] I. J. Kadhim, P. Premaratne, and P. J. Vial, "Adaptive image steganography based on edge detection over dual-tree complex wavelet transform," in *Proc. Int. Conf. Intell. Comput.*, 2018, pp. 544–550.

[34] M. Y. Valandar, M. J. Barani, P. Ayubi, and M. Aghazadeh, "An integer wavelet transform image steganography method based on 3D sine chaotic map," *Multimedia Tools Appl.*, vol. 78, no. 8, pp. 9971–9989, Apr. 2019.

[35] R. Kaur and B. Singh, "A novel approach for data hiding based on combined application of discrete cosine transform and coupled chaotic map," *Multimedia Tools Appl.*, vol. 80, no. 10, pp. 14665–14691, Apr. 2021.

[36] E. Ghasemi, J. Shanbehzadeh, and N. Fassihi, "High capacity image steganography usingWavelet transform and genetic algorithm," in *Proc. World Congr. Eng.*, London, U.K., 2012, pp. 495–498.

[37] R. Wazirali, W. Alasmary, M. M. E. A. Mahmoud, and A. Alhindi, "An optimized steganography hiding capacity and imperceptibly using genetic algorithms," *IEEE Access*, vol. 7, pp. 133496–133508, 2019.

[38] H. R. Kanan and B. Nazeri, "A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm," *Exp. Syst. Appl.*, vol. 41, no. 14, pp. 6123–6130, 2014.

[39] S. Khan and T. Bianchi, "Ant colony optimization (ACO) based data hiding in image complex region," *Int. J. Electr. Comput. Eng.*, vol. 8, no. 1, pp. 379–389, Feb. 2018.

[40] K. G. Beauchamp, *Applications of Walsh and Related Functions*. London, U.K.: Academic, 1984.

[41] A. Abuadbba and I. Khalil, "Walsh–Hadamard-based 3-D steganography for protecting sensitive information in point-of-care," *IEEE Trans. Biomed. Eng.*, vol. 64, no. 9, pp. 2186–2195, Sep. 2017.

[42] S. K. Pal, P. K. Saxena, and S. K. Muttoo, "Image steganography for wireless networks using the Hadamard transform," in *Proc. Int. Conf. Signal Process. Commun., (SPCOM)*, 2004, pp. 131–135.

[43] S. P. Maity and M. K. Kundu, "DHT domain digital watermarking with low loss in image informations," *AEU Int. J. Electron. Commun.*, vol. 64, no. 3, pp. 243–257, Mar. 2010.

[44] E. Etemad, S. Samavi, S. M. R. Soroushmehr, N. Karimi, M. Etemad, S. Shirani, and K. Najarian, "Robust image watermarking scheme using bit-plane of Hadamard coefficients," *Multimedia Tools Appl.*, vol. 77, no. 2, pp. 2033–2055, Jan. 2018.

[45] M. Favorskaya, E. Savchina, and A. Popov, "Adaptive visible image watermarking based on Hadamard transform," in *Proc. IOP Conf. Ser. Mater. Sci. Eng.*, vol. 450, 2018, pp. 052003.1–052003.6.

[46] V. Santhi and P. Arulmozhivarman, "Hadamard transform based adaptive visible/invisible watermarking scheme for digital images," *J. Inf. Secur. Appl.*, vol. 18, no. 4, pp. 167–179, Dec. 2013.

[47] H. F. Harmuth, "Applications of Walsh functions in communications," *IEEE Spectr.*, vol. S-6, no. 11, pp. 82–91, Nov. 1969.

[48] A. D. Andrushia and R. Thangarjan, "Saliency-based image compression using Walsh–Hadamard transform (WHT)," in *Biologically Rationalized Computing Techniques for Image Processing Applications*. 2018, pp. 21–42.

[49] P. Bas, T. Filler, and T. Pevný, "Break our steganographic system: The ins and outs of organizing BOSS," in *Proc. Int. Workshop Inf. Hiding*, 2011, pp. 59–70.

[50] 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.

[51] A. Alharbi and M.-T. Kechadi, "A steganography technique for images based on wavelet transform," in *Proc. Int. Conf. Future Data Secur. Eng.*, 2017, pp. 273–281.

[52] W. Tang, H. Li, W. Luo, and J. Huang, "Adaptive steganalysis based on embedding probabilities of pixels," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 4, pp. 734–745, Apr. 2015.

[53] A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems," in *Proc. Int. Workshop Inf. Hiding*, 1999, pp. 61–76.

[54] C. Stanley, "Pairs of values and the Chi-squared attack," Tech. Rep., 2005.

YING-QIAN ZHANG received the Ph.D. degree from the Dalian University of Technology, in 2015. He is a Professor with Xiamen University Tan Kah Kee College. His research interests include nonlinear systems, chaos theory, and information security.

KUAN ZHONG received the B.S. degree in electronic science and technology from Yanshan University, in 2019. He is currently pursuing the graduate degree in computer technology with Xiamen University. His research interests include image steganography, chaotic encryption, artificial intelligence, and information security.

XING-YUAN WANG was born in Liaoning, China, in 1964. He received the B.S. degree in application physics and the M.S. degree in optics from Tianjin University, Tianjin, China, in 1987 and 1992, respectively, and the Ph.D. degree in computer software and theory from Northeastern University, Shenyang, China, in 1999. From 1999 to 2001, he was a Postdoctoral Fellow at the Department of Automation, Northeastern University. He is currently a Professor with the Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology, Dalian, China. His research interests include biomedical information, computer graphics, image processing, complex networks, and chaos control and synchronization.