A Coverless Information Hiding Method Based on Constructing a Complete Grouped Basis with Unsupervised Learning

JianFeng Lu

School of Computer Science and Technology Hangzhou Dianzi University Hangzhou 310018, China

JinBin Ni

School of Computer Science and Technology Hangzhou Dianzi University Hangzhou 310018, China

Li Li*

School of Computer Science and Technology Hangzhou Dianzi University Hangzhou 310018, China *Corresponding author: lili2008@hdu.edu.cn

Ting Luo

College of Science and Technology Ningbo University Ningbo 315212, China

Chin-Chen Chang

Department of Information Engineering and Computer Science Feng Chia University Taichung 40724, Taiwan

Received November 2020; revised December 2020

ABSTRACT. Traditional information hiding algorithms can be used to modify the carrier for embedding secret message, while the coverless information hiding methods implement secret message transmission by mapping secret information and the carrier image without modifying the image. In this paper, we propose a coverless information hiding method based on constructing a complete grouped basis with unsupervised learning, and the base image of the complete grouped basis is used to map the secret message for obtaining coverless information hiding. At first, texture estimation is used to extract image features. Secondly, learning of the complete grouped basis is designed, which ensures the establishment of a relationship between the secret message and the image feature. Finally, the complete grouped basis and the secret message are jointly operated to obtain a series of stenographicimages for embedding data. Our experimental results prove that the proposed method has the capability of robustness, and is more feasible than the other coverless information hiding methods.

Keywords: Coverless information hiding, Texture estimation, Complete grouped basis.

1. Introduction. Recently, the development of computer technology has promoted the progress of image processing technology [1, 2], in which information hiding methods [3, 4] are widely used in daily lives, and embed secret message into the carrier without vision. Currently, steganography is one of popular information hiding technologies [5, 6, 7]. Steganography is mainly classified into traditional information hiding methods [8, 9] and coverless information hiding methods [10, 11]. The commonly used traditional hiding is classified into two types. One is spatial domain-based methods, such as histogram shifting [12], adaptive LSB (Least Significant Bit) [13], Hamming code-based [14], WOW (Wavelet Obtained Weights) [15], and so on. The other is transform domain-based methods which embed information by modifying the coefficients of the image frequency domain transform, such as DCT (Discrete Cosine Transform) [16, 17], DWT (Discrete Wavelet Transformation) [18] and DFT (Discrete Fourier Transform) [19]. But traditional hiding methods must modify the carrier so that it cannot be robust to some steganographic analysis algorithms, and the secret message is often stolen by third parties. Since the coverless information hiding method embeds secret message into the carrier without any modifications [20, 21], it can effectively resist steganographic analysis algorithms.

The coverless information hiding method does not exclude requirement for carrier data, while features of the carrier are extracted to represent secret messages. Generally, coverless information hiding methods are mainly classified into the text-based method [22] and the image-based method [23, 24]. For text-based method, Chen et al. used Chinese mathematical expression to determine the location of the secret message according to a certain rule [25]. However, since the image is more popular than the text, the image-based coverless information hiding has attracted much more attention.

For image-based coverless information hiding, in general, image features are firstly extracted, and mapped to the secret message to generate steganographic images for embedding data. Zhou et al. invented a coverless information hiding method, in which the intensity differences between image blocks are computed as the secret message to be mapped to the hash sequence [26]. Zou et al. generated hash sequences based on the average pixel values of sub-image to realize the secret message hiding through mapping relationship [27]. In order to resist some image attacks, Zheng et al. extracted the feature of scale-invariant feature transformed (SIFT) image to construct a binary hash sequence for data embedding [28]. Yuan et al. built the information mapping between the secret message and the SIFT features of images [24]. Zhou et al. generated feature sequences by BOW (Bag of Words) model for mapping to the secret message [23]. Zhang et al. employed DCT and LDA (Latent Dirichlet Allocation) models to compute robust features, including DC coefficients, position coordinates, and so on [29]. Wu et al. built mapping relationship between the images and the secret message by the grayscale gradient co-occurrence matrix [30].

However, in the above coverless information hiding methods, the mapping relationship between the extracted feature sequence and the secret message is often not complete [20, 21, 22], which results in the failure of the secret message extraction. In order to solve those problems, this paper proposes a novel coverless information hiding method based on constructing a complete grouped basis with unsupervised learning. Unsupervised learning of the complete grouped basis is designed to ensure the establishment of a mapping relationship between the secret message and the image feature. The complete grouped basis and the secret message are jointly computed to obtain a series of steganographic images for embedding message. Experimental results show that the proposed method has high completeness and embedding capacity compared with the existing coverless information hiding methods. The main contributions of this paper are listed as follows. (1). A novel coverless information hiding method based on constructing a complete grouped basis with unsupervised learning is presented.

(2). A complete grouped basis is computed to establish a mapping relationship between the secret message and the original image.

(3). The proposed method has good robustness on noise attacks and filtering attacks.

The reminder of this paper is organized as follows. In Section 2, we introduce the proposed method, which consists of the learning of the complete grouped basis, the acquisition of stego images and the extraction of secret messages. The results of the experiments and analysis are shown in Section 3. Section 4 concludes our work and outlines our future research direction.

2. The proposed method. We propose a coverless information hiding method based on constructing a complete grouped basis by using unsupervised learning without modifying the original image. The method mainly consists of stego image generation for secret message embedding at the sender and secret message extraction at the receiver as illustrated in FIGURE 1. At the sender, an unsupervised learning method is designed to generate a complete grouped basis, which includes image selecting from an image database via a generated pseudo random sequence, image features extracting via texture estimation, and stego images generation with secret message. At the receiver, secret message is extracted by using the received stego images and the generated pseudo random sequence.



FIGURE 1. Flowchart of the proposed coverless information hiding method

2.1. Generation of the Complete Grouped Basis Based on Unsupervised Learning. Unsupervised learning is one of the most studied learning methods, which is very different from supervised learning. Supervised learning is to train an optimal model through the existing training samples and classify data by using known models. Unsupervised learning requires direct data modeling because there are no training samples in advance. The complete grouping basis is a set of m-order square matrices consisting of m-image feature sequences, which are computed based on unsupervised learning. The generation processes are illustrated in FIGURE 2. 2.1.1. Feature Sequence Extraction. A pseudo random sequence R is generated for selecting m images from the image database, these images are denoted as G_i , where $i = \{1, 2, \ldots, m\}$, and their image indexes from the database are denoted as $\{fid_1, fid_2, \ldots, fid_m\}$. The size of G_i is $N \times N$, and G_i is divided into m non-overlapping blocks with the size of $N/\sqrt{m} \times N/\sqrt{m}$, denoted as B_j , where $j = \{1, 2, \ldots, m\}$. In the following, image texture is estimated by comparing the mean of two adjacent blocks to generate the image feature sequence.

Step 1. For $b_{i,j}$, calculate the average pixel.

$$b_{i,j} = \frac{1}{(N/\sqrt{m})^2} \sum_{x=0}^{(N/\sqrt{m})^2} \sum_{y=0}^{(N/\sqrt{m})^2} B_{i,j}(x,y),$$
(1)

where $B_{i,j}(x, y)$ is the pixel value in the B_j , and (x, y) is the location.

Step 2. Texture estimation is used to compute the image feature bit. Differences of the two adjacent blocks are computed for texture estimation. If the difference is large, the block is located at the complex region, and vice versa. Specifically, the feature bit f_i is computed as

$$f_i = \begin{cases} 0, \text{ if } b_j - b_{j+1} \le g \\ 1, \text{ if } b_j - b_{j+1} > g \end{cases}, 1 < i \le m - 1, \qquad (2)$$

where b_j is the average value of B_j , and g is the threshold. For the last block, b_m and b_1 are compared for computing f_m .

Step 3. Repeat the above steps until all feature bits are computed from all images.

Since the feature sequence is computed from different parts of images, and the feature sequence is not located at a certain region, it is robust to some image attacks, such as compression, noise addition, and so on.



FIGURE 2. Flowchart of constructing a complete grouped basis

2.1.2. Construction of a Complete Grouped Basis. The processes of constructing a complete grouped basis are organized as follows.

Step1. \boldsymbol{H} with the size of $m \times m$ is computed as

$$\boldsymbol{H} = \begin{bmatrix} f_{1,1} & f_{1,2} & f_{1,3} & & f_{1,m} \\ f_{2,1} & f_{2,2} & f_{2,3} & \cdots & f_{2,m} \\ f_{3,1} & f_{3,2} & f_{3,3} & & f_{3,m} \\ \vdots & & \ddots & \vdots \\ f_{m,1} & f_{m,2} & f_{m,3} & \cdots & f_{m,m} \end{bmatrix} \xrightarrow{\rightarrow} fid_{1}$$

$$\rightarrow fid_{2}$$

$$\rightarrow fid_{3} . \qquad (3)$$

Each row represents the features from the same image. For instance, the first row represents the features of G_1 .

Step 2. H is converted to obtain a line minimalist matrix by using elementary transformation. Elements of columns in H are searched from the first to the last, and when the element value is 1, its corresponding row is switched with the first row as illustrated in FIGURE 3. Then, elementary transformation is performed on the matrix again as illustrated in FIGURE 3(b) and 3(c). At this point, if a row of elements in the matrix are all 0, then the eigenvalue of a new image is selected to replace the row, that process is repeated until each row in the matrix is the simplest. Finally, the new line minimalist matrix H'is obtained by using Eq. (4), and the index is also recorded as $\{fid'_1, fid'_2, \ldots, fid'_m\}$.



FIGURE 3. Matrix elementary transformation

$$\boldsymbol{H}' = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 \\ \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix} \xrightarrow{\rightarrow fid'_1}_{\rightarrow fid'_2}$$
(4)

Step 3. Each row is replaced by the original features of each image and the novel image position number pid_i is recorded.

$$\boldsymbol{H}_{\boldsymbol{c}} = \begin{bmatrix} f_{3,1} & f_{3,2} & f_{3,3} & & f_{3,m} \\ f_{4,1} & f_{4,2} & f_{4,3} & \cdots & f_{4,m} \\ f_{6,1} & f_{6,2} & f_{6,3} & & f_{6,m} \\ \vdots & & \ddots & \vdots \\ f_{1,1} & f_{1,2} & f_{1,3} & \cdots & f_{1,m} \end{bmatrix} \xrightarrow{\rightarrow} fid'_{1} \quad pid_{1} \\ \rightarrow fid'_{2} \quad pid_{2} \\ \rightarrow fid'_{3} \quad pid_{3} \\ \vdots & \vdots \\ \rightarrow fid'_{m} \quad pid_{m} \end{bmatrix}$$
(5)

Step 4. If the transformed row simplest matrix \mathbf{H}' is not a unit matrix, new images are selected from the database and its feature sequence is computed to replace corresponding rows. If these rows are not in line with the complete grouped basis, Step 2 to Step 3 are repeated. This process is repeated until \mathbf{H}' is the unit matrix as shown in Eq. (6)

$$\boldsymbol{H}_{c}^{\prime} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 \\ \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix} \xrightarrow{\rightarrow} fid_{1}^{\prime} \quad pid_{1} \\ \rightarrow fid_{2}^{\prime} \quad pid_{2} \\ \rightarrow fid_{3}^{\prime} \quad pid_{3} \quad . \tag{6}$$

2.2. Stego Images Generation Using Grouped Basis. The steps of stego images generation using the complete grouped basis and the secret message are listed as follows.

Step 1. Divide the secret binary message S into n = [l/m] copies and $S = \{s_1, s_2, \ldots, s_n\}$, where l is the length of S. If the length of s_n is less than m, it is filled with zeros.

Step 2. H_c and s_1 are concatenated to form the augmented matrix H_w .

$$\boldsymbol{H}_{\boldsymbol{w}} = \begin{bmatrix} f_{3,1} & f_{3,2} & f_{3,3} & & f_{3,m} & s_{1,1} \\ f_{4,1} & f_{4,2} & f_{4,3} & \cdots & f_{4,m} & s_{12} \\ f_{6,1} & f_{6,2} & f_{6,3} & & f_{6,m} & s_{1,3} \\ \vdots & & \ddots & \vdots & \vdots \\ f_{1,1} & f_{1,2} & f_{1,3} & \cdots & f_{1,m} & s_{1,m} \end{bmatrix}.$$
(7)

Step 3. Perform elementary transformation on H_w , and the line minimalist matrix is obtained as shown in Eq. (8). c_i is defined according to Eq. (9).

$$\boldsymbol{H}_{\boldsymbol{c}}' = \begin{bmatrix} 1 & 0 & 0 & 0 & s_{1,1}' \\ 0 & 1 & 0 & \cdots & 0 & s_{1,2}' \\ 0 & 0 & 1 & 0 & s_{1,3}' \\ \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & s_{1,m}' \end{bmatrix}.$$
(8)

$$c_i = \left\{ s'_{i,1}, s'_{i,2}, \dots, s'_{i,m} \right\}, 1 \le i \le n.$$
(9)

Step 4. c_i is divided into substrings with l_c bits, where $l_c = \log_2 m$. Each substrings is converted to decimal number $d_{i,k}$, where $k = \{1, 2, \ldots, l_c\}$. The selected base grouped c'_i is computed as

$$c_i = \left\{ s'_{i,1}, s'_{i,2}, \dots, s'_{i,m} \right\}, 1 \le i \le n.$$
(10)

For m selected images, the number of stego images is computed as

$$N = \begin{cases} n \times l_c & \text{if } l\%m = 0\\ n \times l_c + 1 & \text{if } l\%m = 1 \end{cases}$$
(11)

2.3. Secret Message Extraction. The receiver gets the steganographic image in sequence and then extracts the secret message. Restore secret message is to calculate the complete grouped basis and obtain the selected base sequence from the stego image. In the extracting processes, SIFT is used to match stego images with images from the complete grouped basis, which is constructed in the same way as the construction at the sender.

The steps of secret message extraction are listed as follows.

Step 1. Construct a complete grouped basis H_c according to the pseudo-random sequence R

$$\boldsymbol{H}_{\boldsymbol{c}} = \begin{bmatrix} f_{3,1} & f_{3,2} & f_{3,3} & & f_{3,m} \\ f_{4,1} & f_{4,2} & f_{4,3} & \cdots & f_{4,m} \\ f_{6,1} & f_{6,2} & f_{6,3} & & f_{6,m} \\ \vdots & & \ddots & \vdots \\ f_{1,1} & f_{1,2} & f_{1,3} & \cdots & f_{1,m} \end{bmatrix} \xrightarrow{\rightarrow} fid'_{1} \quad pid_{1} \\ \rightarrow fid'_{2} \quad pid_{2} \\ \rightarrow fid'_{3} \quad pid_{3} \\ \vdots & \vdots \\ \rightarrow fid'_{m} \quad pid_{m} \end{bmatrix}$$
(12)

Step 2. SIFT feature points of stego images and each image in complete grouped basis are computed, respectively. The number of their same SIFT feature points is computed, the base image with the largest number is selected and the corresponding pid_i is converted to binary. This step is repeated until a sequence with the length of m is obtained.

$$c_i = \left\{ s'_{i,1}, s'_{i,2}, \dots, s'_{i,m} \right\}, 1 \le i \le n.$$
(13)

A Coverless Information Hiding Method Based on Constructing a Complete Grouped Basis

pid	1	2	3	4	5	6	7	8
Complete grouped	1. 11 - 11 -			Sugara Car	Law,			
basis images			Salay of the				10	
fid	0	15	4	3	8	7	6	5
pid	9	10	11	12	13	14	15	16
Complete grouped	1000	11		FCA. DA DA TRON				
basis images		1-0						
fid	2	1	10	11	12	34	13	23

TABLE 1. Complete grouped basis image group 1

TABLE 2. Steganographic image group 1

pid	1	2	3	4	5
Stego images	6 Th				
fid	0	15	4	3	8

Step 3. Multiply H_c by c_i to obtain the original secret message.

$$\begin{bmatrix} S_{i,1} \\ S_{i,2} \\ S_{i,3} \\ \vdots \\ s_{i,m} \end{bmatrix} = \begin{bmatrix} f_{3,1} & f_{3,2} & f_{3,3} & & f_{3,m} \\ f_{4,1} & f_{4,2} & f_{4,3} & \cdots & f_{4,m} \\ f_{6,1} & f_{6,2} & f_{6,3} & & f_{6,m} \\ \vdots & \ddots & \vdots \\ f_{1,1} & f_{1,2} & f_{1,3} & \cdots & f_{1,m} \end{bmatrix} \begin{bmatrix} s'_{i,1} \\ s'_{i,2} \\ s'_{i,3} \\ \vdots \\ s'_{i,m} \end{bmatrix}.$$
(14)

Step 4. Repeat the above steps to obtain all $s_{i,q}$, where $q = \{1, 2, ..., m\}$ and all $s_{i,q}$ are connected to form the original secret message.

3. Experiments. The experiments are done using a personal computer with Intel(R) Core (TM) i5-6600K CPU@3.50GHz, 16GB RAM, Windows 8.1, and MATLAB 2015a. Tiny ImageNet (Stanford CS231N) is used as the database, which contains one million images. Ten thousand images are selected for testing. In the experiments, we set m=16 and n=5.

3.1. Experimental Results and Analysis. Sixteen images are finally selected as shown in TABLE 1, and five stego images are generated as shown in TABLE 2. From the experiments, complete grouped basis can be achieved, and the secret message can be extracted successfully at the receiver side.

In order to show the feasibility of the proposed method, another similar experiment is done as shown in TABLE 3 and TABLE 4. The experimental results also show that secret message can be extracted successfully at the receiver side. According to the secret message, the complete grouped basis is different if the selected images are not the same, which assures diversity of the transmission for security. It still denotes that the proposed method can transmit the secret message without modifying the original images and has good efficiency.

3.2. Characteristic Sequence Completeness Analysis. Completeness is the success rate of mapping between the feature sequence and the original image. FIGURE 4 shows the grouping of partial decimal feature sequences under different g without a complete grouped basis. It can be clearly seen that it cannot fully meet the actual grouping

35

pid	1	2	3	4	5	6	7	8
Complete grouped		and an				and and a second second	and the second	N dening
basis images		1. C						and the second second
fid	0	15	4	3	8	7	6	5
pid	9	10	11	12	13	14	15	16
Complete grouped				and a state		A. 1001		M
basis images			and the second s					
fid	2	1	10	11	12	34	13	23

TABLE 3. Complete grouped basis image group 2

TABLE 4. Steganographic image group 2

pid	1	2	3	4	5
Stego	and the second s				
images					
fid	0	15	4	3	8

TABLE 5. Completeness of group images feature sequence

Threshold	0	1	2	3	4	5	6	7	8	9	10
Completeness($\%$)	32.71	32.48	32.19	31.62	31	30.26	29.40	28.44	27.49	26.42	25.31

requirements, and most of the groups do not have matching images as shown in TABLE 5. Thus, a complete grouped basis is added for the proposed method to solve and avoid the above fault.

In SIFT features [28], SIFT+BOF [24] and DCT+LDA [29], the number of images should be increased to a lot for increasing grouping requirements. However, the proposed method only needs a small number of images for good grouping because the complete grouped basis plays an important role.



FIGURE 4. Partial decimal feature sequence grouping under different thresholds

A Coverless Information Hiding Method Based on Constructing a Complete Grouped Basis TABLE 6. The BER between attacked images and primitive images

Attack image	Mode	Parameters	$Size(32^*32)$	Size(48*48)	Size(64*64)
		90%	99.38%	99.75%	100%
1000	IDEC	70%	97.50%	98.75%	99.38%
	ormprossion	50%	96.25%	98.13%	99.38%
	compression	30%	96.25%	98.13%	99.38%
		10%	95%	97.50%	98.13%
	Salt and pepper	0.1	90%	97.50%	98.75%
(i)	noise	0.05	98.75%	98.75%	100%
		0.01	99.38%	99.75%	100%
2015	Cause	0.1	92.50%	97.50%	98.75%
	noiso	0.05	93.13%	97.50%	98.75%
	lioise	0.01	95%	95%	100%
	Median	3*3	97.50%	98.13%	100%
	filtering	5*5	88.13%	96.88%	99.38%
	mitering	7*7	46.25%	83.75%	95.63%
	Moon	3*3	95%	98.75%	100%
	filtoring	5*5	61.25%	85.63%	95.63%
	intering	7*7	27.50%	55%	80%
100	Cause	3*3	98.13%	98.75%	100%
	filtoring	5*5	98.13%	98.75%	100%
	mitering	7*7	98.13%	98.75%	ize(48*48) Size(64*64) 99.75% 100% 98.75% 99.38% 98.13% 99.38% 98.13% 99.38% 97.50% 98.13% 97.50% 98.75% 97.50% 98.75% 97.50% 98.75% 97.50% 98.75% 97.50% 98.75% 97.50% 98.75% 97.50% 98.75% 97.50% 98.75% 95% 100% 95.83% 99.38% 95.63% 99.38% 98.75% 100% 98.75% 100% 98.75% 100% 98.75% 100% 98.75% 100% 98.75% 100% 98.75% 100% 98.75% 100% 98.75% 100% 98.75% 100% 98.75% 99.38% 98.13% 99.38% 98.13% 99.38% 95.63% 95.63%<
	Centered	Crop 20%	92.50%	97.50%	98.13%
	cropping	Crop 50%	28.75%	82.50%	88.75%
1-9	Scaling	zoom in 10%	97.50%	98.13%	99.38%
	beamig	Reduce by 10%	96.80%	98.13%	99.38%
		10°	83.75%	95.63%	96.25%
	Rotation	30°	75%	91.88%	95%
		50°	71.88%	91.25%	91.88%
	Mirroring	Flip up and down	38.75%	56.25%	67.50%
		Filp left and right	40%	60.63%	64.38%

3.3. Analysis of Robustness.	In this	section	BER is	s used	to	evaluate	the	robustne	3 S
in our proposed method.									

$$BER = \frac{q}{l},\tag{15}$$

where q is the number of correct extracted bits and l is the number of bits of secret message.

In order to show the robustness of this paper proposed method, the stego images are attacked by JPEG compression, Salt and Pepper noise, Gauss noise, Median filtering, Gauss filtering, Translation, Centered cropping, Scaling, Rotation, and Mirroring. All secret bits can be nearly extracted as shown in TABLE 6, since *BERs* are higher than 0.8. Especially for attacking of Gauss filtering, the *BERs* are close to 100%. It greatly supports that the proposed method has the capability of resisting image attacks.

4. **Conclusions.** This paper proposes a coverless information hiding method based on constructing a complete grouped basis with unsupervised learning, and realizes the secret message hiding by establishing a mapping relationship between original image feature sequences and the secret message. Since the carrier image is not modified during the implementation, it has high security. Moreover, the concept of a complete grouped basis is put forward, which completes feature sequences of the original image based on matrix theory. It is effective to solve the problem of incomplete mapping between secret message and feature sequences. Our experimental results show that the proposed method is very good in information hiding than the existing methods, and it has good robustness to some image attacks. However, in order to compensate for the lack of feature sequence types, the method sacrifices the embedding capacity of some private images, which results in transmitting many stego images. In the next work, we will strive to increase the embedding capacity of stego images, meanwhile, reduce the number of stego images during the image transmitting.

Acknowledgment. This work was partially supported by National Natural Science Foundation of China (No. 61971247, No. 61370218), and Public Welfare Technology and Industry Project of Zhejiang Provincial Science Technology Department (No. LGG19F020016).

REFERENCES

- J. W. Wang, H. Hang, J. Li, and X. Y.Luo, Detecting Double JPEG Compressed Color Images with The Same Quantization Matrix in Spherical Coordinates *IEEE Transactions on Circuits and* Systems for Video Technology, vol.30, no.8, pp.2736–2749, 2020
- [2] J. W. Wang, J. Li, X. Y. Luo, Y. Q. Shi, and S. KrJha, Identifying Computer Generated Images Based on Quaternion Central Moments in Color Quaternion Wavelet Domain, *IEEE Transactions* on Circuits and Systems for Video Technology, vol.29, no.9, pp.2775–2785, 2019.
- [3] T. Y. Wu, X. N. Fan, K. H. Wang, C. F. Lai, N. X. Xiong, and J. M. T. Wu, A DNA computation based image encryption scheme for cloud CCTV systems, *IEEE Access*, vol.7, pp.181434–181443, 2019.
- [4] T. Y. Wu, X. N. Fan, K. H. Wang, J. S. Pan and C. M. Chen, Security Analysis and Improvement on An Image Encryption Algorithm using Chebyshev Generator, *Journal of Internet Technology*, vol.20, no. 1, pp.13–23, 2019.
- [5] T. Y. Wu, X. N. Fan, K. H. Wang, J. S. Pan, C. M. Chen and J. M. T. Wu, Security Analysis and Improvement of An Image Encryption Scheme Based on Chaotic Tent Map, *Journal of Information Hiding and Multimedia Signal Processing*, vol.9, no. 4, pp.1050–1057, 2018.
- [6] V. SedighiY, R. Cogranne and J. Fridrich, Content-Adaptive Steganography by Minimizing Statistical Detectability *IEEE Transactions on Information Forensics and Security*, vol.11, pp.221–234, 2015.
- [7] K. Yamato, K. Shinoda, M. Hasegawa and S. Kato, Reversible Data Hiding Based on Two-Dimensional Histogram and Generalized Histogram Shifting, *IEEE International Conference on Image Processing*, 2014.
- [8] A. Vinothini and A. Lathika, Secure and Lossless Data Hiding by Histogram Shifting and Scan Paths Using Integer Wavelet Transform, International Conference on Information Communication and Embedded Systems, 2015.
- [9] H. W. Wang, H. J. Lin, X. Y. Gao, W. H. Cheng, and Y. Y. Chen, Reversible AMBTC-Based Data Hiding with Security Improvement by Chaotic Encryption, *IEEE Access*, vol.7, pp.38337–38347, 2019.
- [10] Z. L. Zhou, Y. Mu, N. S. Zhao, Q. M. J. Wu, and C. N. Yang, Coverless Information Hiding Method Based on Multi-keywords, *International Conference on Cloud Computing and Security*, pp.39–47, 2016.
- [11] J. K. Wu, and Z. B. Guo, A Coverless Text Information Hiding Algorithm Based on Hamming Code, Journal of Qingdao University, Natural Science Edition, vol.39, no.2, pp.1006–1037, 2019.

- [12] W. C. Kuo, and Y. H. Lin, On the Security of Reversible Data Hiding Based-on Histogram Shift, The 3rd International Conference on Innovative Computing Information and Control, vol.1, pp.174, 2008.
- [13] J. Fridrich, M. Goljan, and R. Du, Detecting LSB Steganography in Color and Gray-Scale Images, *IEEE Multimedia*, vol.8, no.4, pp.22–28, 2001.
- [14] C. Kim, and C. N. Yang, Data Hiding Based on Overlapped Pixels Using Hamming Code, Multimedia Tools and Applications, vol.75, no.23, pp.15651–15663, 2016.
- [15] V. Holub, and J. Fridrich, Designing Steganographic Distortion Using Directional Filters, IEEE Workshop on Information Forensic and Security, 2012.
- [16] C. C. Lin, and P. F. Shiu, DCT-based Reversible Data Hiding Scheme, Journal of Software, vol.5, no.2, pp.327–335, 2010.
- [17] C. C. Chang, C. C. Lin, C. S. Tseng, and W. L. Tai, Reversible Hiding in DCT-based Compressed Images, *Information Sciences*, vol.177, no.13, pp.2768–2786, 2007.
- [18] H. A. AI-Korbi, A. AI-Atady, M. A. Al-Taee, and W. AI-Nuaimy, High-capacity Image Steganography Based on Haar DWT for Hiding Miscellaneous Data, *Applied Electrical Engineering and Computing Technologies, IEEE*, 2015.
- [19] Y. X. Song, M. H. Cui, and H. X. Yao, A High Capacity Data Hiding Scheme Based on DFT, Pacific-Rim Conference on Multimedia, pp.82–88, 2002.
- [20] Z. L. Zhou, Y. Mu, and Q. M. J. Wu, Coverless Image Steganography Using Partial-Duplicate Image Retrieval, Soft Computing, pp.1–12, 2018.
- [21] X. T. Duan, and H. X. Song, Coverless Information Hiding Based on Generative Model, arXiv:1802.03528, 2018.
- [22] J. Zhang, H. Huang, L. Wang, and D. Gao, Coverless Text Information Hiding Method Using the Frequent Words Distance, International Conference on Cloud Computing and Security, pp.121–132, 2017.
- [23] Z. L. Zhou, Y. Cao and X. M. Sun, Coverless Information Hiding Based on Bag-of-Words Model of Image, *Journal of Applied Sciences*, vol.34, no.5, pp.527–536, 2018.
- [24] C. S. Yang, Z. H. Xia and X. M. Sun, Coverless Image Steganography Based on SIFT and BOF, Journal of Internet Technology, vol.18, no.2, pp.435–442, 2017.
- [25] X. Y. Chen, H. Y. Sun, Y. Tobe, Z. L. Zhou and X. M. Sun, Coverless Information Hiding Method Based on the Chinese Mathematical Expression, *International Conference on Cloud Computing and Security*, pp.133–143, 2016.
- [26] Z. L. Zhou, H. Y. Sun, R. Harit, X. Y. Chen and X. M. Sun, Coverless Image Steganography Without Embedding, International Conference on Cloud Computing and Security, pp.123–132, 2015.
- [27] L. M. Zou, J. D. Sun, M. Gao, W. B. Wan and B. B. Gupta, A Novel Coverless Information Hiding Method Based on The Average Pixel Value of The Sub-Images, *Multimedia Tools and Applications*, vol.78, no.7, pp.7965–7980, 2018.
- [28] S. L. Zheng, L. Wang, B. H. Ling and G. H. Hu, Coverless Information Hiding Based on Robust Image Hashing, International Conference on Intelligent Computing, pp.536–547, 2017.
- [29] X. Zhang, F. Peng and M. Long, Robust Coverless Image Steganography Based on DCT and LDA Topic Classification, *IEEE Transactions on Multimedia*, vol.20, pp.3223–3238, 2018.
- [30] J. B. Wu, Y. W. Liu, Z. W. Dai, Z. K. Kang, S. Rahbar and Y. K. Jia, A Coverless Information Hiding Algorithm Based on Grayscale Gradient Co-occurrence Matrix, *IETE Technical Review*, pp.1–11, 2018.