IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 17, 2019, accepted April 28, 2019, date of publication May 1, 2019, date of current version May 15, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2914226

Secure Cover Selection for Steganography

ZICHI WANG AND XINPENG ZHANG

Shanghai Institute for Advanced Communication and Data Science, Key Laboratory of Specialty Fiber Optics and Optical Access Networks, Joint International Research Laboratory of Specialty Fiber Optics and Advanced Communication, Shanghai University, Shanghai 200444, China

Corresponding author: Xinpeng Zhang (xzhang@shu.edu.cn)

This work was supported in part by the Natural Science Foundation of China under Grant U1636206, Grant 61525203, and Grant 61472235, and in part by the Shanghai Excellent Academic Leader Plan under Grant 16XD1401200.

ABSTRACT Existing cover selection methods for steganography cannot resist pooled steganalysis. This paper proposes a secure cover selection method which is able to resist pooled steganalysis and single object steganalysis meanwhile. To resist pooled steganalysis, the maximum mean discrepancy (MMD) distance between the stego set and a clear arbitrary image set is kept not larger than a normal threshold during cover selection, where the threshold is the MMD distance between two clear arbitrary image sets. Under this constraint, a searching strategy is designed to select the minimal steganographic distortion images within the affordable computational complexity to resist single object steganalysis. With the selected covers, the security of steganography is guaranteed against both single object steganalysis and pooled steganalysis. The experimental results demonstrated the effectiveness of the proposed method.

INDEX TERMS Steganography, security, distortion, cover selection.

I. INTRODUCTION

Steganography aims to transmit secret data through public channels without drawing suspicion [1], [2]. To achieve this, the most popular approach is to embed the secret data into cover object by slightly modifying the content of cover [3], [4]. Digital images are widely used as covers in steganography since it is widely used around the world. In modern steganography, the steganographic distortion caused by modifications on a cover image is minimized to guarantee the security performance [5].

On the contrary, single object steganalysis aims to disclose the covert communication by analyzing the images on public channels [6], [7]. Modern steganalytic methods are based on supervised machine learning [8]. The features are extracted from a set of images to train a common steganalytic model, which is then used to distinguish the suspicious images [9]–[11]. Recently, deep learning based steganalysis can also achieve good performances [12]–[14]. The decisions made on suspicious images are correct with high probability.

When a steganographer possesses a number of images, he can choose the most suitable image for data embedding. Most of existing cover selection methods select cover images empirically [15]–[19]. In [15], the changeable DCT coefficients are counted. Then the images with a larger number of changeable DCT coefficients are selected as cover images. In [16], the images with high visual quality are regarded as suitable covers for embedding. Considering the content of image, researchers select suitable cover images according to image texture and complexity [17]–[19]. In [17], the blocks of secret image are compared with the blocks of available images, and then the images with the most similar blocks to those of secret image are selected as covers. In [18], image complexity is measured by visual quality and amount of modifications on a stego image. The authors of [19] proposed to calculate image complexity using image residuals which is modeled by fuzzy logic. These above-mentioned empirical cover selection methods do not perform satisfactory security.

A unified measure to evaluate the hiding ability of a cover image is proposed in [20]. Available images are represented by the Gaussian mixture model, and then the Fisher Information Matrix of image is calculated and mapped into a real value to evaluate the hiding ability. But the employed model is not able to describe natural image precisely. The authors of [21] proved that the first-order derivative of steganographic distortion of a single image is monotonically increasing, and the first-order derivative of steganographic distortion of selected cover images should be equal. Based on the two deductions, the images set with the minimal total steganographic distortion are selected as covers. This method performs high security against single object steganalysis.

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

However, all the existing cover-selection methods have a theoretical flaw that selected cover images (as a subset of all possible images) will always have some statistical properties different from the whole set of all possible images [22]. Because of this, existing cover-selection methods cannot resist pooled steganalysis which aims to find the steganographers among other innocent individuals [23]–[27] (each individual emitted a number of images). Different from single object steganalysis which makes an binary decision (''clear'' or ''stego'') on a suspicious image, pooled steganalysis makes an binary decision (''guilty'' or ''innocent'') on a suspicious individual. In pooled steganalysis, it is suppose that the steganalyst is monitoring a number of individuals, with multiple innocent individuals and some potentially steganographers. To determine who is guilty, it is assumed that the steganographers are significantly deviate from the majority innocent individuals. Based on this assumption, the steganographers can be recognized by unsupervised clustering algorithms because that the individuals' deviation is evidence of their guilt. Despite of the process of data embedding, the covers selected by existing cover-selection methods are different with the whole set of all possible images. For this situation, the assumption in pooled steganalysis is correct. Therefore, the steganographer using existing cover-selection methods can be easily identified by pooled steganalysis.

This paper proposes a secure cover selection method, which is able to resist single object steganalysis and pooled steganalysis meanwhile. To resist pooled steganalysis, the MMD distance between the stego set and a clear arbitrary image set is kept not larger than a normal threshold during cover selection, where the threshold is the MMD distance between two clear normal image sets. Under this constraint, a searching strategy is designed to select the minimal steganographic distortion images within affordable computational complexity to resist single object steganalysis. With the selected covers, the security of steganography can be guaranteed against both single object steganalysis and pooled steganalysis.

The contributions of this paper are listed as follows:

(1) We give clear descriptions of steganography security in image level and individual level, and expound the theoretical flaw of existing cover-selection methods in individual level;
(2) We propose a cover selection method which is secure in both image level and individual level;
(3) Experimental results show that the proposed cover-selection method is able to resist single object steganalysis and pooled steganalysis meanwhile.

The rest of this paper is organized as follows. In section II, the descriptions of steganography security in image level and individual level are given. The proposed cover selection method described in section III. Experimental results and analysis are provided in Section IV. Section V concludes the whole paper.

II. STEGANOGRAPHIC SECURITY IN IMAGE AND INDIVIDUAL LEVEL

There are two levels of steganographic security: image level and individual level. However, there is no definite descriptions of steganography security in image level and individual level. For this reason, we describe the two levels of steganographic security before introducing our method.

A. IMAGE LEVEL SECURITY

In image level, the opponent of steganography is single object steganalysis. That means the steganalyst aims to give correct decision (''clear'' or ''stego'') on a suspicious image. On the contrary, the steganographer aims to make the stego images transmitted by him indistinguishable from other clear images.

Current single object steganalysis uses supervised machine learning to investigate the models of the covers and the stegos. The features are extracted from a set of images with labels firstly, and then used to train a classifier which is used to distinguish the suspicious images. The classifier can also be trained by deep learning to achieve better steganalytic model.

Therefore, the steganographic security in image level can be measured by the error rate of the steganalytic classifier. Specifically, the error rate can be denoted as the minimal total error P_{E},

$$P_E = \min_{P_{FA}} \left(\frac{P_{\mathrm{FA}} + P_{MD}}{2} \right) \tag{1}$$

where P_{FA} is the false alarm rate and P_{MD} the missed detection rate. A large value of P_{E} means high security of steganography in image level.

B. INDIVIDUAL LEVEL SECURITY

In individual level, the steganographer aims to conceal himself among other normal individuals when examined by pooled steganalysis.

Pooled steganalysis is based on unsupervised clustering, and aims to find the individuals of steganography among a number of innocent individuals. It is supposed that the steganalyst is monitoring a number of individuals, with multiple innocent individuals and some potentially guilty individuals. To determine who are the guilty individuals, it is assumed that their behaviors are significantly deviate from the majority of innocent individuals. Based on this assumption, the steganographers can be recognized by unsupervised clustering algorithms because that the individuals' deviation is evidence of their guilt.

$$DA = \frac{\text{Times of correct detection}}{\text{Total number of detections}} \times 100\% \tag{2}$$

The steganographic security in individual level can be measured by the detection accuracy of steganographers identification of pooled steganalysis. Where the detection accuracy (DA) is the rate of correctly identifying the steganographers, which can be calculated using Equation (2). A low value of detection accuracy means high security of steganography in individual level.

III. PROPOSED METHOD

In this section, we expound the theoretical flaw of existing cover-selection methods specifically, and then give the proposed secure cover-selection method.

A. EXISTING FLAW

In pooled steganalysis [23]–[27], the maximum mean discrepancy (MMD) [28] is employed to measure the distance between two feature sets. Denote two feature sets (each contains n vectors) as $\mathbf{F}_x = \{f_x(i)\}$ and $\mathbf{F}_y = \{f_y(i)\}$, where $f_x(i)$ and $f_y(i)$ are the vectors with same number of dimensions, $i \in \{1, 2, \ldots, n\}$, the MMD distance can be calculated as:

$$\begin{aligned} MMD^2\left(F_x, F_y\right) = \frac{1}{n(n-1)} \sum_{i \neq j} [k\left(f_x(i), f_x(j)\right) \\ -k\left(f_x(j), f_y(i)\right) - k\left(f_x(i), f_y(j)\right) \\ +k\left(f_y(i), f_y(j)\right)] \end{aligned} \tag{3}$$

where $k(x,y)$ is a kernel function need to be pre-defined. The linear kernel $k(x,y) = x^{\mathrm{T}}y$ is the most effective kernel function, which is also used in our cover selection method.

There is a theoretical flaw in existing cover selection methods that the statistical properties of the selected cover images are different from the whole set of all possible images. The differences can be observed via the MMD distance. To verify this, we conduct a group of experiments over image data set BOSSbase ver. 1.01 [29] which contains 10000 grayscale images sized 512 × 512. We arbitrarily select 100, 250, 500, 750 and 1000 images respectively as the normal image sets. All the five image sets are arbitrarily selected twice to calculate the normal MMD distance. Then the same number images are respectively selected using the cover selection method in [21]. To calculate MMD distance, the popular feature extraction method SPAM [9] is employed to obtain the features of the selected images.

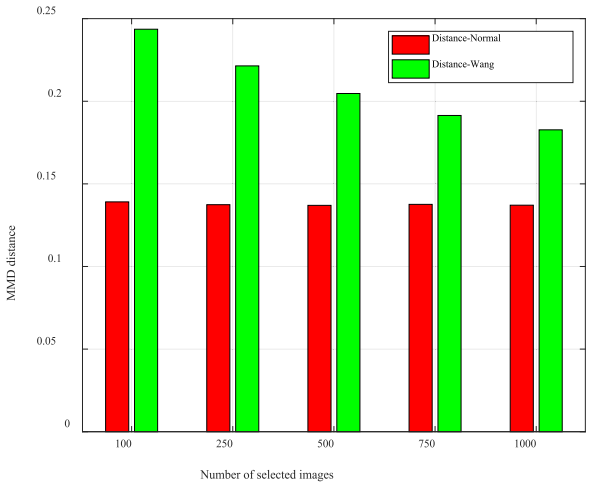

FIGURE 1. MMD distance comparisons.

The comparisons of MMD distance are shown in Fig. 1. Where ''Distance-Normal'' and ''Distance-Wang'' stand for the normal MMD distance and the MMD distance between arbitrary images with the images selected by the method in [21] respectively. The results indicate that the MMD distance is increased obviously when the cover selection method in [21] is employed. That means the cover images selected by [21] are different from the arbitrary images. Although the selected images with minimal steganographic distortion are suitable for concealing the modification trace made by steganography, the images themselves can still be identified from the whole set of all possible images according to their statistical abnormality.

For steganography, it is disadvantageous that the cover images are abnormal since the abnormality is evidence of the steganographer's guilt. Therefore, the steganographer employs existing cover selection methods can be easily identified by pooled steganalysis, which is verified in Section IV. In our method, the MMD distance between the cover and stego set is restrained during cover selection. Thus, the statistical properties differences are shortened as far as possible. As a result, the security in individual level of our method is guaranteed. The details will be discussed in the following subsection.

B. COVER SELECTION METHOD

In existing cover-selection methods, the images with more complex texture are preferentially selected. But it is difficult to build a precise model to describe natural image. To resist single object steganalysis, actually, it is easy to select covers for modern steganographyic methods, e.g., WOW [30], SUNIWARD [31], HILL [32] which are based on additive distortion minimization [5].

In modern steganography, a per-defined distortion function is used to assign an embedding cost value for each cover element to quantify the modification effect. Given an image contains t elements $\{x(1), x(2), \ldots, x(t)\}$, denote the embedding cost for $+1$ and -1 operation assigned by a distortion function of $x(i)$ as $\rho^+(i)$ and $\rho^-(i)$ respectively $(1 \leq i \leq t)$. The theoretical minimal steganographic distortion D of stego image with embedding capacity C(bits) [33] is,

$$D = \sum_{i=1}^{t} [p^+(i)\rho^+(i) + p^-(i)\rho^-(i)] \tag{4}$$

where

$$p^+(i) = \frac{e^{-\lambda\rho^+(i)}}{1 + e^{-\lambda\rho^+(i)} + e^{-\lambda\rho^+(i)}} \tag{5}$$

and

$$p^-(i) = \frac{e^{-\lambda\rho^-(i)}}{1 + e^{-\lambda\rho^-(i)} + e^{-\lambda\rho^-(i)}} \tag{6}$$

are the probabilities of modifying $x(i)$ by $+1$ or -1 respectively. The parameter λ ($\lambda > 0$) is used to make the ternary information entropy of modifying probability equal

to the capacity C,

$$-\sum_{i=1}^{t}\{p^{+}(i)\log_2 p^{+}(i)+p^{-}(i)\log_2 p^{-}(i) +[1-p^{+}(i)-p^{-}(i)]\log_2[1-p^{+}(i)-p^{-}(i)]\}=C \quad (7)$$

Therefore, in image level, it is reasonable to select the images with the minimal values of D. Given k images $\{\mathbf{I}_1, \mathbf{I}_2, \ldots, \mathbf{I}_k\}$ for selection, denote the corresponding steganographic distortions as $\{D_1, D_2, \ldots, D_k\}$ respectively. After sorting in ascending order, $\{D_1, D_2, \ldots, D_k\}$ are reordered into $\{D_{\xi(1)}, D_{\xi(2)}, \ldots, D_{\xi(k)}\}$, $\xi(i) \in\{1, 2, \ldots, k\}$, $i \in \{1, 2, \ldots, k\}$. Then a selection order $\{\xi(1), \xi(2), \ldots, \xi(k)\}$ is obtained. To resist single object steganalysis, the cover images should be selected following this order.

However, the images selected by this order are not secure in individual level. To resist pooled steganalysis, the MMD distance between the stego set and a clear arbitrary image set should be kept not larger than a normal threshold during cover selection. We set the MMD distance between two clear arbitrary selected image sets as this threshold. The security in individual level can be guaranteed as long as this restriction is satisfied. Under this restriction, meanwhile, the images with low steganographic distortion should be selected as many as possible for the security in image level. In this way, the selected cover images are secure in both image and individual level.

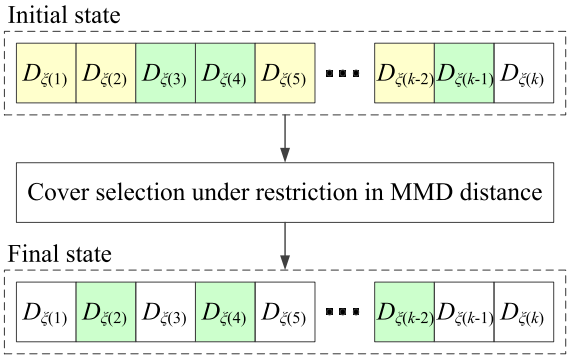

FIGURE 2. Demonstration of cover selection.

As shown in Fig. 2, cover images are selected under the restriction in MMD distance. In the initial state, specified quantity of images (the squares marked with green) are selected arbitrarily. At this time, the selected images are secure in individual level. Then the images (the squares marked with yellow) which corresponding to smaller steganographic distortions than the selected images are checked one by one for possible replacement of the selected images. While the images (the unpainted squares) corresponding to larger steganographic distortions would not be considered since these images make no contributions to image level security.

A selected image $\mathbf{I}_i$ (marked with green) would be replaced by a under consideration image $\mathbf{I}_j$ (marked with yellow) when the following conditions are satisfied:

a) The steganographic distortion of $\mathbf{I}_j$ is smaller than $\mathbf{I}_i$ ($\mathbf{I}_j$ is on the left of $\mathbf{I}_i$ in Fig. 2), and $\mathbf{I}_i$ has not been replaced;
b) The MMD distance between the stego image set (obtained by embedding secret data into the selected image set) with a clear arbitrary image set would not larger than the MMD distance between two clear arbitrary image sets if $\mathbf{I}_i$ is replaced by $\mathbf{I}_j$;

The first condition helps to increase the steganographic security in image level, while the second condition ensures the individual level security not decreased. After all the images under consideration are checked by the two conditions, the final selected images are obtained, as shown in the final state of Fig. 2. Note that Fig. 2 is just an illustration to demonstrate the idea (the images with low steganographic distortion should be selected as many as possible for image level security under the MMD restriction) of the proposed cover-selection method. More details about the proposed cover selection strategy are given below.

Assume the steganographer intend to select r images as cover, denote the average MMD distance between two clear arbitrarily image sets (each contains r images) as d_{T}. The steps to determine d_{T} are listed below.

(1) Arbitrarily select r images from $\{\mathbf{I}_1, \mathbf{I}_2, \ldots, \mathbf{I}_k\}$ to obtain an image set $\dot{\mathbf{I}}$;
(2) Repeat step (1) to obtain another arbitrary image set $\ddot{\mathbf{I}}$;
(3) Calculate the MMD distance (feature sets of images are obtained using SPAM) between $\dot{\mathbf{I}}$ and $\ddot{\mathbf{I}}$;
(4) To obtain a stable threshold, repeat steps (1)∼(3) for Δ times, and calculate the average MMD distance d_{T}. The value of Δ will be discussed later.

To resist pooled steganalysis, the MMD distance between the stego set and a clear arbitrary image set should be kept not larger than d_{T}. Under this constraint, a searching strategy is designed to select the most suitable r images according to selection order $\{\xi(1), \xi(2), \ldots, \xi(k)\}$ within affordable computational complexity. In this way, single object steganalysis and pooled steganalysis can be resisted meanwhile. The searching strategy is described in ALG. 1.

The logic behind the above cover selection strategy is that the images in $\ddot{\mathbf{I}}$ can be replaced by the images with less steganographic distortion to resist single object steganalysis. Meanwhile, the MMD distance between the stego set and a clear arbitrary image set is kept not larger than d_{T} to resist pooled steganalysis. In other words, with the restriction of MMD distance, the images with low steganographic distortion are selected as many as possible. In this way, the undetectability of steganography is guaranteed against both single object steganalysis and pooled steganalysis.

To determine the value of Δ which used to calculate d_{T}, a group of experiments are carried out. In detail, the image dataset BOSSbase ver. 1.01 [29] is employed to simulate the available images $\{\mathbf{I}_1, \mathbf{I}_2, \ldots, \mathbf{I}_k\}$. We arbitrarily select 100 images from BOSSbase as the image set $\dot{\mathbf{I}}$, and arbitrarily select 100 images again as $\ddot{\mathbf{I}}$. Then calculate the variance of the MMD distance between $\dot{\mathbf{I}}$ and $\ddot{\mathbf{I}}$. The selection and

Algorithm 1 Cover Selection Strategy

Input: The available images $\{\mathbf{I}_1, \mathbf{I}_2, \ldots, \mathbf{I}_k\}$, threshold value d_T, and the selection order $\{\xi(1), \xi(2), \ldots, \xi(k)\}$.

Output: Selected r images.

1) Use $\dot{\mathrm{I}}$ as the initial selected r images;
2) Reorder the r images in $\dot{\mathrm{I}}$ according to the order $\{\xi(1), \xi(2), \ldots, \xi(k)\}$, denote the obtained image set as $\mathrm{I} = \{\mathbf{I}_{\varphi(1)}, \mathbf{I}_{\varphi(2)}, \ldots, \mathbf{I}_{\varphi(r)}\}$, where $\varphi(j) \in \{1, 2, \ldots, k\}$, $j \in \{1, 2, \ldots, r\}$, and $D_{\varphi(1)} \leq D_{\varphi(2)} \leq \ldots \leq D_{\varphi(r)}$;
3) Embed C secret bits into each image in I;
4) for $v = 1$ to k,
    if the number of replaced images reaches r,
        break
    end
    for $u = r$ to 1,
        if $D_{\xi(v)} > D_{\varphi(u)}$,
            break;
        End
        if $\varphi(u)$ is not equal to $\xi(v)$, and $\mathbf{I}_{\varphi(u)}$ has not been replaced,
            Embed C secret bits into $\mathbf{I}_{\xi(v)}$;
            Replace image $\mathbf{I}_{\varphi(u)}$ in I by the stego image $\mathbf{I}_{\xi(v)}$ to obtain an intermediate image set $\tilde{\mathrm{I}}$;
            Calculate the MMD distance d between $\ddot{\mathrm{I}}$ and the $\tilde{\mathrm{I}}$;
            if $d \leq d_T$,
                Replace I by $\tilde{\mathrm{I}}$;
                break;
            end
        end
    end
end
5) Find the r cover images from $\{\mathbf{I}_1, \mathbf{I}_2, \ldots, \mathbf{I}_k\}$ which corresponding to the stego images in set I, then the obtained images are the finally selected r images.

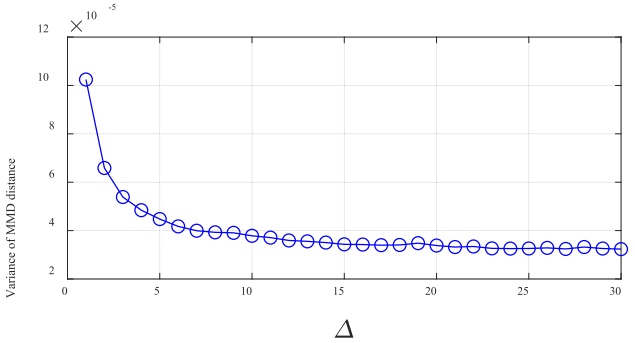

FIGURE 3. Parameter determination.

calculation steps are executed for Δ times. The relationship between Δ with the variance of MMD distance is shown in Fig. 3. It can be seen that the variance is hardly decreased any more after the value of Δ is larger than 15, which results in a stable threshold d_T. To save computational complexity, the value of Δ is determined as 15. On the whole, the threshold of MMD is determined using the available images $\{\mathbf{I}_1, \mathbf{I}_2, \ldots, \mathbf{I}_k\}$ which can be obtained from any image dataset. That means the determination of the threshold of MMD is not depended on specific image dataset. In the above determination method, we use dataset BOSSbase ver. 1.01 as an example. For different image datasets, the values of MMD threshold are different, while the methods to determine the MMD threshold are the same.

In our method, it is assumed that the normal individuals not employ any image selection strategy (select images arbitrarily). According to this, the r images in initial state are selected arbitrarily to simulate the normal individuals. For the case that the normal individuals employ a certain image selection strategy, our method can also work by selecting the initial r images using the certain image selection strategy. Beyond that, other steps are kept unchanged. Since the behavioral differences between the normal individuals with steganographer, the image selection strategy (if any) of normal individuals is different from the one employed by steganographer. Therefore, our method can always work on secure cover selection in both image and individual levels. In addition, our method is universal for both spatial and JPEG steganography although the feature extraction method SPAM used to obtain image features is designed for spatial image. For JPEG steganography, SPAM can be executed after the JPEG image is decompressed into spatial domain, or replaced by JPEG steganalysis feature extraction method.

IV. EXPERIMENTAL RESULTS

In this section, we firstly setup the experimental environments using the popular database. Then we show the selected images, and compare the proposed method with the state-of-the-art cover selection method in image level and individual level respectively.

A. EXPERIMENT SETUP

The image dataset used in our experiments is BOSSbase ver. 1.01 [29] which contains 10000 grayscale images sized 512×512. Thereinto, 5000 images are arbitrarily selected from all the 10000 images to form the available image set of the steganographer ($k = 5000$). Other 5000 images are used for training the steganalytic classifier in image level (A pre-trained classifier is unnecessary in individual level).

To verify the security of the proposed method, 100 images are selected from the available 5000 images using the proposed method as cover images ($r = 100$). For comparison, 100 images are selected from the same 5000 images using the cover selection method in [21], and 100 arbitrary images are also selected from the same available image set. Then three cover image sets (each contains 100 images) are obtained.

For steganography, the popular steganographic methods HILL, WOW and SUNIWARD are used for embedding. The payloads of each image are set as 0.05, 0.1, 0.2, 0.3, 0.4, and 0.5 bpp respectively. Thus 54 stego image sets (each contains

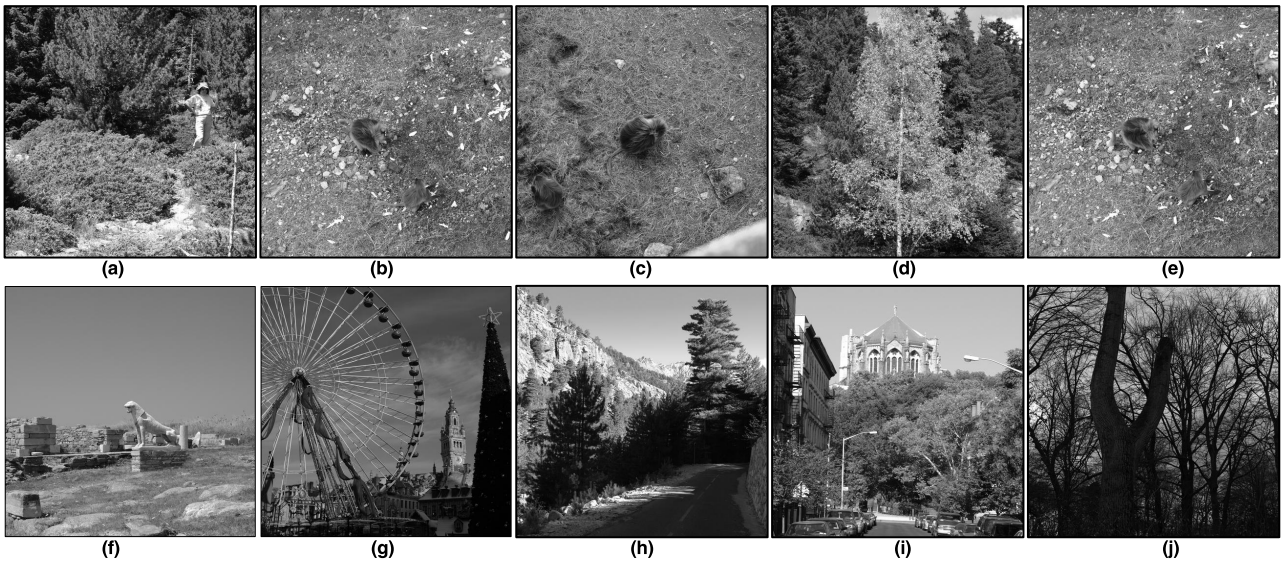

FIGURE 4. Demonstration of images (a) ∼ (e) selected by the method in [21] and images (f) ∼ (j) selected by the proposed method.

100 images) are formed. For data embedding, we use the ternary embedding simulator [34] since it is widely used to simulate the optimal embedding pattern.

For steganlaysis, the popular feature extraction methods SPAM [9] and SRMQ1 [10] are used to check the undetectability of steganography. We employ the ensemble classifier [8] to measure the property of feature sets. To train the steganalytic classifier in image level, the 5000 images used for training are also embedded with the above-mentioned three steganographic methods and the six values of payload respectively. The trained 36 classifiers (3 steganographic methods, 6 payloads, 2 feature extraction methods) are then used to test the three cover sets and the 54 stego sets respectively. The performance is evaluated using the average of P_{E} over 100 random tests.

In individual level, more than one individual should be simulated. Denote the number of individuals as w, other w-1 image sets (each contains 100 images) are selected arbitrarily to simulate the innocent individuals. The employed pooled steganalytic method is the hierarchical clustering method [23]. The detection accuracy also tested over 100 random tests.

B. COMPARISONS OF SELECTED IMAGE

To demonstrate the results of cover selection visually, five images are selected from the available image set by our method and the method in [21] respectively. The selected images are shown in Fig. 4, where (a) ∼ (e) are the five images selected by the method in [21], and (f) ∼ (j) are selected by our method.

It is clear that the images selected by the method in [21] contain extremely complex texture and edge. The texture complexity can be roughly evaluated by the summation of horizontal and vertical residual values of an image, which is shown in Equation (8), where $x(i,j)$ is the (i,j)th pixel value of an image sized $M \times N$. Larger h means more complex texture. Table 1 shows the h values of the corresponding images in Fig. 4, which indicates that the texture complexity of the images selected by [21] is higher than the images selected by our method.

TABLE 1. Texture complexity comparison.

Image	Fig. 4 (a)	Fig. 4 (b)	Fig. 4 (c)	Fig. 4 (d)	Fig. 4 (e)
w ($\times 10^6$)	11.987	11.768	10.982	11.594	11.807
Image	Fig. 4 (f)	Fig. 4 (g)	Fig. 4 (h)	Fig. 4 (i)	Fig. 4 (j)
w ($\times 10^6$)	3.366	5.571	5.647	7.794	11.040

$$h = \sum_{i=1}^{M}\sum_{j=1}^{N-1}|x(i,j) - x(i,j+1)| + \sum_{i=1}^{M-1}\sum_{j=1}^{N}|x(i,j) - x(i+1,j)| \quad (8)$$

The complex areas are hard to be modeled, and thus the modification trace made by steganography can be concealed effectively. For this reason, the method in [21] performs high security against single object steganalysis. But just because of this, statistical properties of the selected images are different from the whole set of all possible images, which can be observed in Fig. 1. Therefore, the method in [21] is insecure against pooled steganalysis, which will be shown in the following subsection.

While the images selected by our method contain various content instead of complex texture only, as shown in Fig. 4 (f) ∼ (j). This variety shortens the differences of statistical properties, which results in satisfactory security against pooled steganalysis. Meanwhile, the complex component

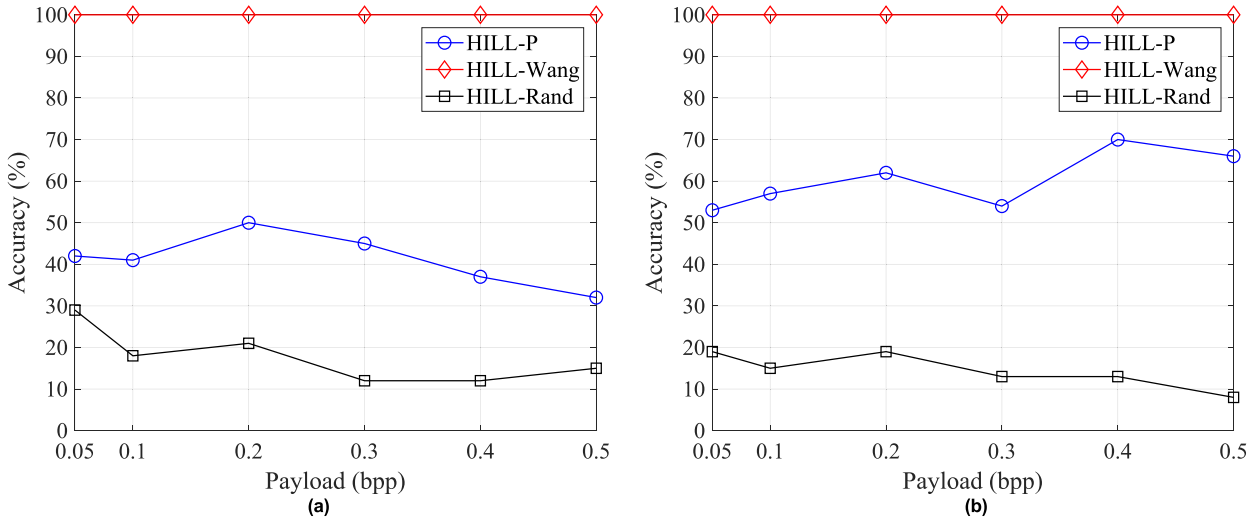

FIGURE 5. Comparisons of detection accuracy for HILL with k = 5000, r = 100, w = 5, and (a) SPAM, (b) SRMQ1.

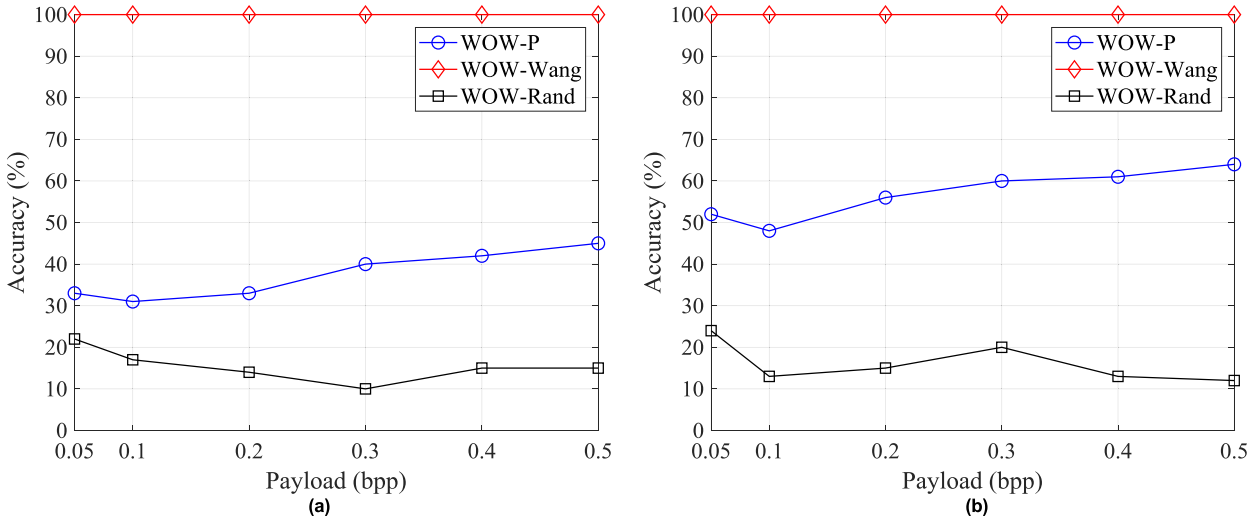

FIGURE 6. Comparisons of detection accuracy for WOW with k = 5000, r = 100, w = 5, and (a) SPAM, (b) SRMQ1.

contained in a part of the selected images guarantees the security against single object steganalysis.

C. SECURITY IN INDIVIDUAL LEVEL

The comparisons of detection accuracy DA on 5 individuals ($w = 5$) with feature sets SPAM and SRMQ1 are shown in Fig. 5 ∼ Fig. 7. Where "HILL-P", "WOW-P" and "SUNIWARD-P" mean the cover images are selected by the proposed method and then embedded by HILL, WOW and SUNIWARD respectively. "HILL-Wang", "WOW-Wang" and "SUNIWARD-Wang" mean the cover images are selected by the method in [21] and then embedded by HILL, WOW and SUNIWARD respectively. While "HILL-Rand", "WOW-Rand" and "SUNIWARD-Rand" mean no cover selection strategy is employed, the cover images are selected arbitrarily.

It can be seen from Fig. 5 ∼ Fig. 7 that the detection accuracy of pooled steganalysis is always 100% when the cover images are selected by the method in [21]. That means the cover selection method in [21] is extremely insecure in individual level. This is because of the theoretical flaw of the existing cover selection methods. The statistical properties of the selected cover images are different from the whole set of all possible images. After steganography is executed on the selected images, the statistical properties differences will be further enlarged. As a result, the steganographer can be easily identified by pooled steganalysis. In our method, the MMD distance between the stego set and a clear arbitrary image set is restrained during cover selection. As a result, the statistical properties differences are tiny. Therefore, the security in individual level of our method is guaranteed.

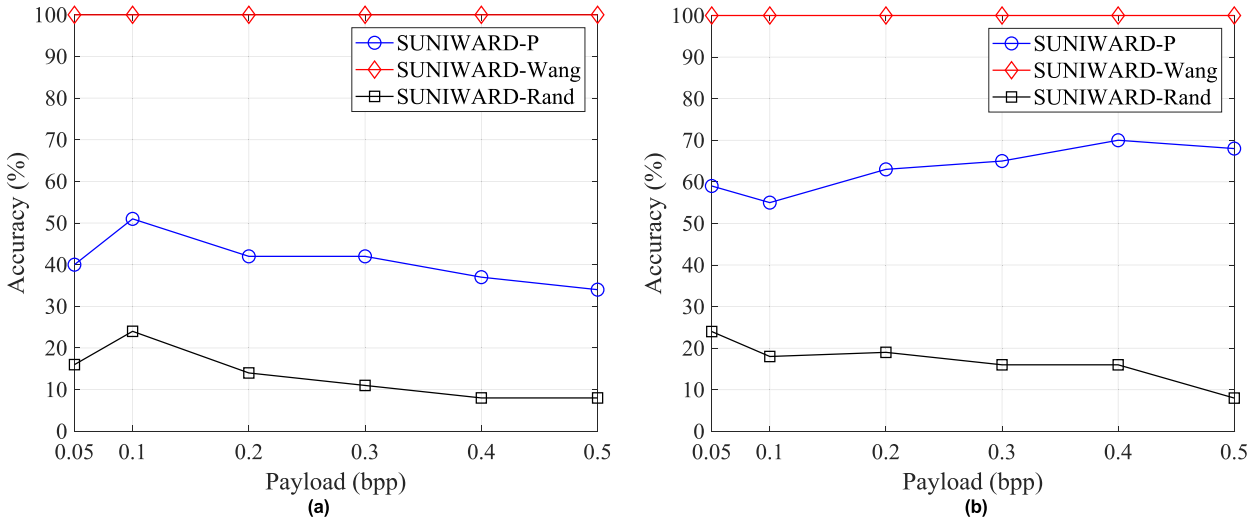

FIGURE 7. Comparisons of detection accuracy for SUNIWARD with k = 5000, r = 100, w = 5, and (a) SPAM, (b) SRMQ1.

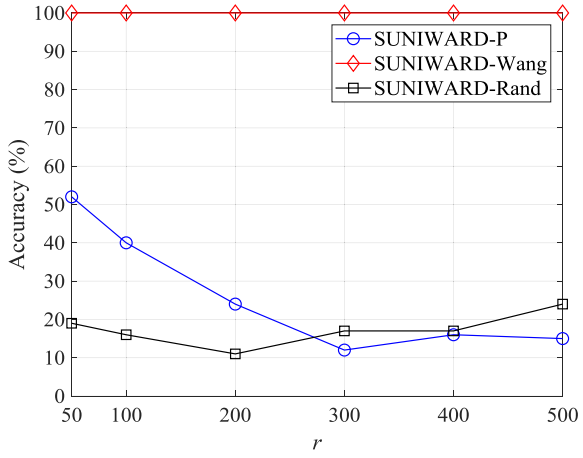

FIGURE 8. Comparisons of detection accuracy for SUNIWARD with k = 5000, w = 5, payload = 0.05 bpp, and SPAM.

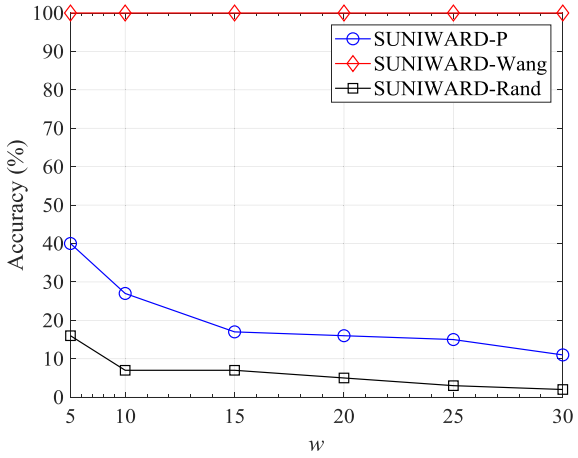

FIGURE 9. Comparisons of detection accuracy for SUNIWARD with k = 5000, r = 100, payload = 0.05 bpp, and SPAM.

Fig. 8 and Fig. 9 show the individual level security with different values of r and w respectively. Although the feature set SPAM is not advanced, the payload is low, and the pooled steganalytic method is primitive, the detection accuracy of pooled steganalysis is still 100% on the cover selection method in [21] for all cases. This verified the flaw in existing cover selection methods again. While our method performs a comparable security with the case of no cover selection strategy employed with a large r.

In fact, the statistical properties between the cover images selected by our method with the whole set of all possible images are consistent. The consistency will be remarkable when the number of selected images is large enough. This is the reason that the images selected by our method performs a comparable security with the arbitrarily selected images when r is large enough. Therefore, our method is secure in individual level. To verify this, we also conduct some additional experiments for the cases of $r = 500$, which are shown in Fig. 10. It is clear that our method performs similar security with arbitrary selection for all cases, while the detection accuracy on the method in [21] is still 100%. In a word, the individual level security of our method is the same with arbitrary selection. The image level security will be discussed in the following subsection.

D. SECURITY IN IMAGE LEVEL

In image level, the security of steganography is measured by the testing error P_E as discussed in subsection II.A. The comparisons of P_E based on HILL, WOW, and SUNIWARD with feature sets SPAM and SRMQ1 are shown in Fig. 11 ∼ Fig. 13 respectively. The meanings of the legends are the same with above subsection.

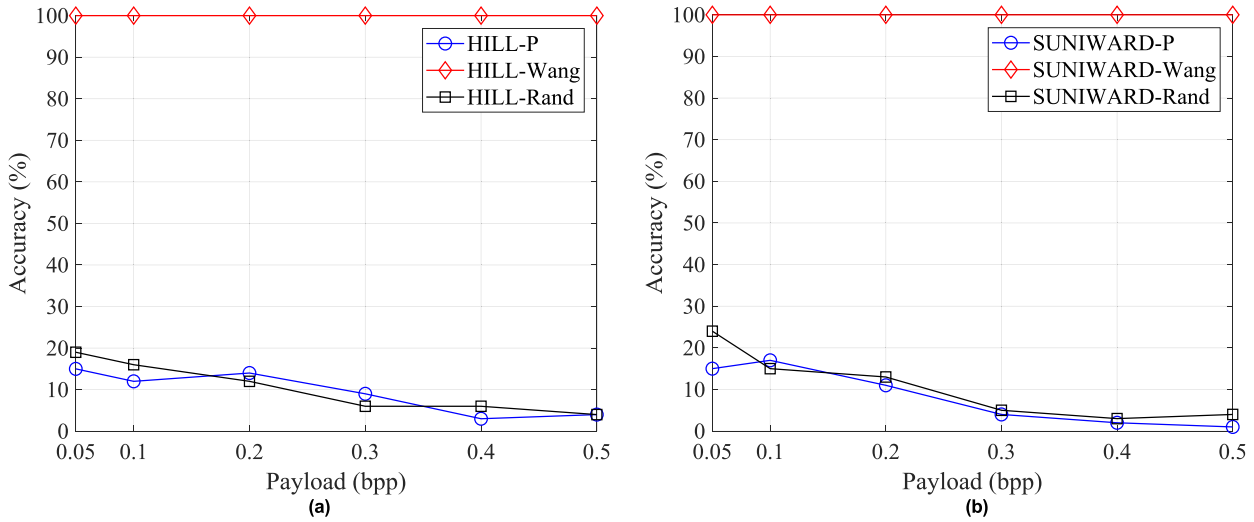

FIGURE 10. Comparisons of P_E for (a) HILL, (b) SUNIWARD with k = 5000, r = 500, w = 5, and SPAM.

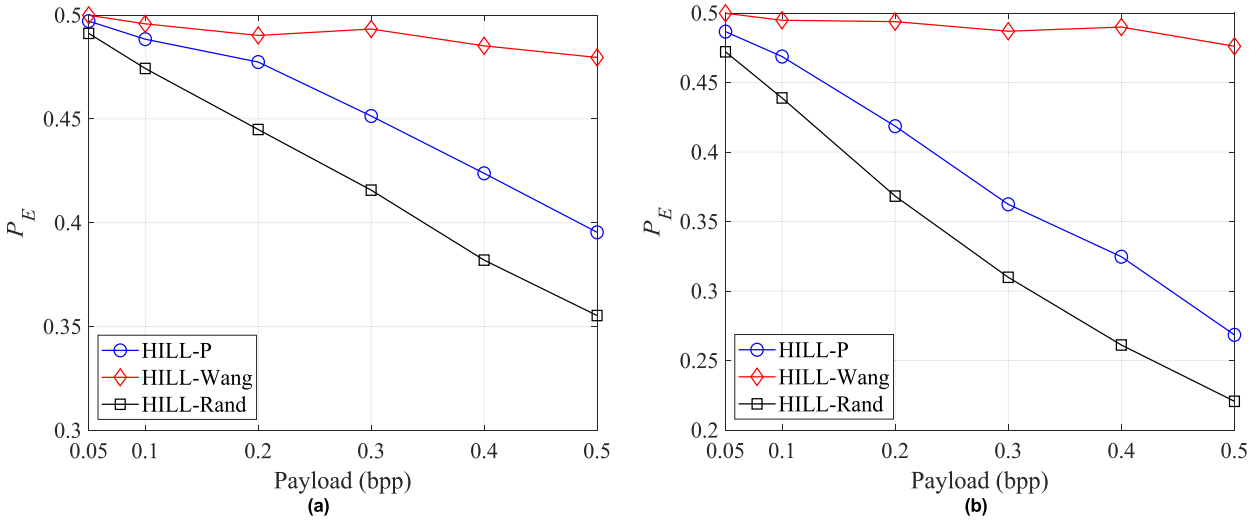

FIGURE 11. Comparisons of P_E for HILL with k = 5000, r = 100, and (a) SPAM, (b) SRMQ1.

The results indicate that the security of all approaches are improved by using the proposed cover selection method for all cases. It is also clear that the method in [21] performs the best security in image level. However, the method in [21] is extremely insecure in individual level as shown in Fig. 5 ∼ Fig. 10. A steganographer selects cover images using the method in [21] can be easily identified. As shown in the above subsection, the security in individual level of our method is guaranteed. Therefore, the security of our method is satisfactory in both image and individual level. In other words, our method can resist both single object steganalysis and pooled steganalysis meanwhile.

On the whole, no cover selection strategy outperforms our method in individual level for small cover image set (e.g. 100 images), and performs comparably with our method for large cover image set (e.g. 500 images). The possible reason which has been analyzed in subsection IV-C is that the consistency of statistical properties between the cover images selected by our method with the whole set of all possible images is remarkable when the number of selected images is large enough. In image level, our method is always outperforms no cover selection strategy.

Actually, there is a trade-off between image level security with individual level security. We find an approach to balance steganographic security in the two levels. Existing cover selection methods spare no pains to increase the image level security without considering individual level security. This is the reason that the method in [21] performs outstanding security in image level but loses it all in individual level.

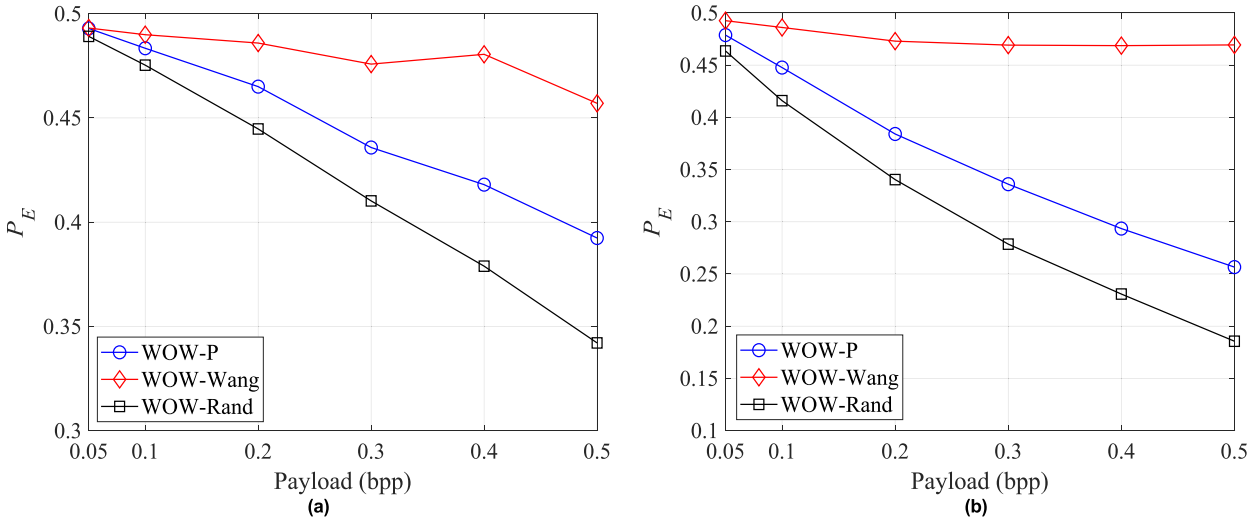

FIGURE 12. Comparisons of P_E for WOW with k = 5000, r = 100, and (a) SPAM, (b) SRMQ1.

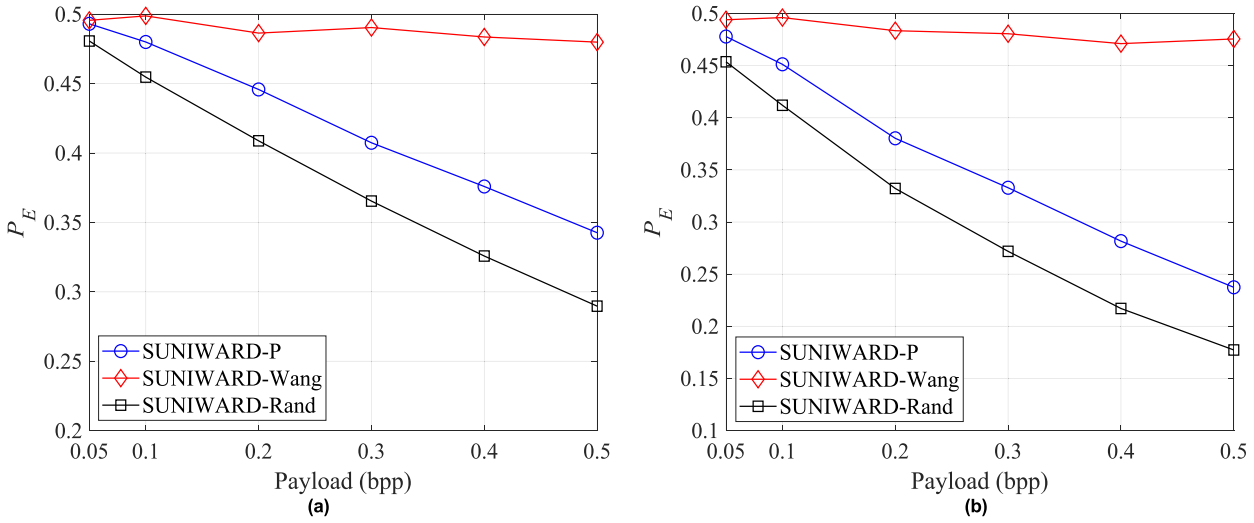

FIGURE 13. Comparisons of P_E for SUNIWARD with k = 5000, r = 100, and (a) SPAM, (b) SRMQ1.

V. CONCLUSION

In this paper, we propose a cover selection method which is secure in both image and individual level by restraining MMD distance and searching the minimal steganographic distortion images. Experimental results show that the undetectability of steganography is guaranteed against both single object steganalysis and pooled steganalysis when using the proposed method.

For further study, the security in image level and individual level of steganography can be further increased by other approaches except cover-selection, e.g., develop joint distortion function for multiple images, which focuses on the joint statistical properties of a number of cover images.

REFERENCES

[1] Z. Wang, Z. Qian, X. Zhang, M. Yang, and D. Ye, "On improving distortion functions for JPEG steganography," *IEEE Access*, vol. 6, pp. 74917–74930, 2018.

[2] S. Li and X. Zhang, "Towards construction based data hiding: From secrets to fingerprint images," *IEEE Trans. Image Process.*, vol. 28, no. 3, pp. 1482–1497, Mar. 2019.

[3] F. Li, K. Wu, X. Zhang, J. Yu, J. Lei, and M. Wen, "Robust batch steganography in social networks with non-uniform payload and data decomposition," *IEEE Access*, vol. 6, pp. 29912–29925, May 2018.

[4] J. Tao, S. Li, X. Zhang, and Z. Wang, "Towards robust image steganography," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 29, no. 2, pp. 594–600, Feb. 2019.

[5] T. Filler, J. Judas, and J. Fridrich, "Minimizing additive distortion in steganography using syndrome-trellis codes," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 920–935, Sep. 2011.

[6] Y. Ma, X. Luo, X. Li, Z. Bao, and Y. Zhang, "Selection of rich model steganalysis features based on decision rough set α-positive region reduction," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 29, no. 2, pp. 336–350, Feb. 2019.

[7] G. Feng, X. Zhang, Y. Ren, Z. Qian, and S. Li, "Diversity-based cascade filters for JPEG steganalysis," *IEEE Trans. Circuits Syst. Video Technol.*, to be published. doi: 10.1109/TCSVT.2019.2891778.

[8] J. Kodovský, J. Fridrich, and V. Holub, "Ensemble classifiers for steganalysis of digital media," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 432–444, Apr. 2012.

[9] 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.
[10] J. Fridrich and J. Kodovský, "Rich models for steganalysis of digital images," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 3, pp. 868–882, Jun. 2012.
[11] B. Li, Z. Li, S. Zhou, S. Tan, and X. Zhang, "New steganalytic features for spatial image steganography based on derivative filters and threshold LBP operator," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 5, pp. 1242–1257, May 2018.
[12] J. Ni, J. Ye, and Y. I. Yang, "Deep learning hierarchical representations for image steganalysis," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 11, pp. 2545–2557, Nov. 2017.
[13] J. Zeng, S. Tan, B. Li, and J. Huang, "Large-scale JPEG image steganalysis using hybrid deep-learning framework," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 5, pp. 1200–1214, May 2018.
[14] M. Boroumand, M. Chen, and J. Fridrich, "Deep residual network for steganalysis of digital images," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 5, pp. 1181–1193, May 2019.
[15] M. Kharrazi, H. T. Sencar, and N. Memon, "Cover selection for steganographic embedding," in *Proc. IEEE Int. Conf. Image Process.*, Atlanta, GA, USA, Oct. 2006, pp. 117–120.
[16] O. Evsutin, A. Kokurina, and R. Meshcheryakov, "Approach to the selection of the best cover image for information embedding in JPEG images based on the principles of the optimality," *J. Decis. Syst.*, vol. 27, no. S1, pp. 256–264, Apr. 2018.
[17] H. Sajedi and M. Jamzad, "Cover selection steganography method based on similarity of image blocks," in *Proc. IEEE Int. Conf. Comput. Inf. Technol. Workshops*, Jul. 2008, pp. 379–384.
[18] H. Sajedi and M. Jamzad, "Using contourlet transform and cover selection for secure steganography," *Int. J. Inf. Secur.*, vol. 9, no. 5, pp. 337–352, Oct. 2010.
[19] M. S. Subhedar and V. H. Mankar, "Curvelet transform and cover selection for secure steganography," *Multimedia Tools Appl.*, vol. 77, no. 7, pp. 8115–8138, Apr. 2018.
[20] S. Wu, Y. Liu, S. Zhong, and Y. Liu, "What makes the stego image undetectable?" in *Proc. 7th Int. Conf. Internet Multimedia Comput. Service (ICIMCS)*, Hunan, China, Aug. 2015, p. 47.
[21] Z. Wang, X. Zhang, and Z. Yin, "Joint cover-selection and payload-allocation by steganographic distortion optimization," *IEEE Signal Process. Lett.*, vol. 25, no. 10, pp. 1530–1534, Oct. 2018.
[22] S. Li, A. Ho, Z. Wang, and X. Zhang, "Lost in the digital wild: Hiding information in digital activities," in *Proc. 2nd Int. Workshop Multimedia Privacy Secur. (MPS)*, Toronto, ON, Canada, Oct. 2018, pp. 27–37.
[23] A. D. Ker and T. Pevný, "A new paradigm for steganalysis via clustering," *Proc. SPIE*, vol. 7880, Feb. 2011, Art. no. 78800U01.
[24] A. D. Ker and T. Pevný, "Identifying a steganographer in realistic and heterogeneous data sets," *Proc. SPIE*, vol. 8303, pp. 83030N-1–83030N-13, Feb. 2012.
[25] A. D. Ker and T. Pevný, "The steganographer is the outlier: Realistic large-scale steganalysis," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 9, pp. 1424–1435, Sep. 2014.
[26] T. Pevný and I. Nikolaev, "Optimizing pooling function for pooled steganalysis," in *Proc. IEEE Int. Workshop Inf. Forensics Secur.*, Rome, Italy, Nov. 2015, pp. 1–6.
[27] F. Li, K. Wu, J. Lei, M. Wen, Z. Bi, and C. Gu, "Steganalysis over large-scale social networks with high-order joint features and clustering ensembles," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 2, pp. 344–357, Feb. 2016.
[28] A. Gretton, K. M. Borgwardt, M. Rasch, B. Schölkopf, and A. J. Smola, "A kernel method for the two-sample-problem," in *Advances in Neural Information Processing Systems*, vol. 19. Cambridge, MA, USA: MIT Press, 2007, pp. 513–520.
[29] P. Bas, T. Filler, and T. Pevný, "'Break our steganographic system': The ins and outs of organizing BOSS," in *Proc. 13th Int. Conf. Inf. Hiding*, Prague, Czech Republic, May 2011, pp. 59–70.
[30] V. Holub and J. Fridrich, "Designing steganographic distortion using directional filters," in *Proc. IEEE Int. Workshop Inf. Forensics Secur.*, Binghamton, NY, USA, Dec. 2012, pp. 234–239.
[31] V. Holub, J. Fridrich, and T. Denemark, "Universal distortion function for steganography in an arbitrary domain," *EURASIP J. Inf. Secur.*, vol. 2014, no. 1, pp. 1–13, 2014.
[32] B. Li, M. Wang, J. Huang, and X. Li, "A new cost function for spatial image steganography," in *Proc. IEEE Int. Conf. Image Process.*, Paris, France, Oct. 2014, pp. 4206–4210.
[33] J. Fridrich and T. Filler, "Practical methods for minimizing embedding impact in steganography," *Proc. SPIE*, vol. 6505, Feb. 2007, Art. no. 650502.
[34] T. Pevný, T. Filler, and P. Bas, "Using high-dimensional image models to perform highly undetectable steganography," in *Proc. 12th Int. Conf. Inf. Hiding*, Calgary, AB, Canada, Jun. 2010, pp. 161–177.

ZICHI WANG received the B.S. degree in electronics and information engineering and the M.S. degree in signal and information processing from Shanghai University, China, in 2014 and 2017, where he is currently pursuing the Ph.D. degree. His research interests include steganography, steganalysis, and reversible data hiding. He has published about 20 papers in these areas.

XINPENG ZHANG received the B.S. degree in computational mathematics from Jilin University, China, in 1995, and the M.E. and Ph.D. degrees in communication and information system from Shanghai University, China, in 2001 and 2004, respectively. Since 2004, he has been with the faculty of the School of Communication and Information Engineering, Shanghai University, where he is currently a Professor. His research interests include information hiding, image processing, and digital forensics. He has published over 200 papers in these areas.