



Block-based image steganalysis: Algorithm and performance evaluation



Seongho Cho^a, Byung-Ho Cha^{b,*}, Martin Gawecki^a, C.-C. Jay Kuo^a

^a Ming Hsieh Department of Electrical Engineering and Signal and Image Processing Institute, University of Southern California, Los Angeles, CA 90089-2546, USA

^b Convergence S/W Lab, Samsung Electronics Co. LTD., Suwon-City, Gyeonggi-Do 443-742, Republic of Korea

ARTICLE INFO

Article history:

Received 22 June 2012

Accepted 16 May 2013

Available online 5 June 2013

Keywords:

Steganalysis

Steganography

Block-based image steganalysis

Decision fusion

Stego image

Block decomposition

Fisher linear discriminant classifier

Dempster-Shafer theory

ABSTRACT

Traditional image steganalysis is conducted with respect to the entire image frame. In this work, we differentiate a stego image from its cover image based on steganalysis of decomposed image blocks. After image decomposition into smaller blocks, we classify image blocks into multiple classes and find a classifier for each class. Then, steganalysis of the whole image can be obtained by integrating results of all image blocks via decision fusion. Extensive performance evaluation of block-based image steganalysis is conducted. For a given test image, there exists a trade-off between the block size and the block number. We propose to use overlapping blocks to improve the steganalysis performance. Additional performance improvement can be achieved using different decision fusion schemes and different classifiers. Besides the block-decomposition framework, we point out that the choice of a proper classifier plays an important role in improving detection accuracy, and show that both the logistic classifier and the Fisher linear discriminant classifier outperforms the linear Bayes classifier by a significant margin.

© 2013 Elsevier Inc. All rights reserved.

1. Introduction

The goal of image steganography is to embed secret messages in an image so that no one except the intended recipients can detect presence of secret messages. It has many applications such as embedding the copyright information into professional images, personal information into photographs in smart IDs (identity cards), and patient information into medical images [1]. Using image steganalysis, one attempts to detect the presence of secret messages hidden in such images.

With the advance of image steganography, many steganalysis methods have been developed to deal with new breakthroughs in image steganography. In the early stage, it is assumed that some prior information about steganographic algorithms that embeds a secret message into images is available. This is called targeted steganalysis. However, more attention has been paid to a more realistic situation in recent years. That is, no information about steganographic algorithms is available. This is known as blind steganalysis, which attempts to differentiate stego images from cover images without the knowledge of steganographic embedding algorithms [2]. Using features extracted from cover and stego images in a training set, we may design a classifier that separates cover and stego images in the feature space.

Most previous work on image steganalysis focused on extracting features from images and used a binary classifier to differentiate stego images from cover images. The research objective was to find a better feature set to improve the steganalysis performance. Fridrich [3] proposed the use of DCT features for steganalysis since inter-block dependency between neighboring blocks is often affected by steganographic algorithms. Shi et al. [4] proposed to use Markov features since the differences between absolute values of neighboring DCT coefficients can be modeled as a Markov process. This feature set is useful because intra-block correlations among DCT coefficients within the same block can be affected by steganographic embedding. Pevný and Fridrich [5] proposed a set of 274 merged features by combining DCT and Markov features together.

So far, little attention has been paid to the characteristics of cover images to design content-adaptive classifiers in steganalysis. An input image typically consists of heterogeneous regions. We may decompose an image frame into smaller blocks and use each block as a basic unit for steganalysis. The effect of steganographic embedding on similar image blocks is known to have a stronger correlation [6]. As a result, the characteristics of smaller blocks can be used to design content-adaptive classifiers.

The frame-based steganalysis, which extracts a set of features from the whole image, was reported in almost all previous work [3–5]. In contrast, the block-based steganalysis, which extracts features from each individual block, was proposed by the authors in [7]. Based on the block features, a tree-structured vector quantization (TSVQ) scheme can be adopted to classify blocks into multiple

* Corresponding author.

E-mail addresses: seonghoc@usc.edu (S. Cho), bhpaul.cha@samsung.com (B.-H. Cha), gawecki@usc.edu (M. Gawecki), cckuo@sipi.usc.edu (C.-C. Jay Kuo).

classes. For each class, a specific classifier can be trained using block features, which represent the characteristics of the block class. For a given test image, instead of making a single decision for the entire image, we repeat the block decomposition process and choose a classifier to make a cover/stego decision for each block depending on block features. Finally, a decision fusion technique can be used to fuse steganalysis results of all blocks so that one can decide whether an unknown image is a cover or stego image.

The rest of this paper is organized as follows. Related previous work is reviewed in Section 2. The proposed block-based image steganalysis system is presented in Section 3. Analysis of the performance of block-based image steganalysis by considering the effects of block sizes, block numbers and the block overlapping design is conducted in Section 4. Fusion of multiple block decisions into one final decision for a test image is examined in Sec. 5. Extensive experimental results are shown for thorough performance evaluation in Section 6. Finally, concluding remarks and future research directions are provided in Sec. 7.

2. Review of previous work

Previous research in blind steganalysis has focused on extracting features from the whole image [3–5]. The number of features was increased to achieve better steganalysis performance in recent years. Chen et al. [8] proposed a set of updated Markov features (486 features in total) by considering both intra-block and inter-block correlations among DCT coefficients of JPEG images. Kodovský et al. [9] examined a set of updated merged features (548 features in total) using the concept of Cartesian calibration. Pevný et al. [10] used higher order Markov models to capture the differences between neighboring pixels in the spatial domain and developed a subtractive pixel adjacency model feature set (686 features in total). This feature set is also known to be effective with the LSB matching algorithm. Note that LSB matching is similar to LSB replacement, but it differs in that LSB matching changes LSBs only when the LSB of the next pixel from the cover image is different from the next bit of the secret message. In general, the steganalysis of LSB matching is known to be much more challenging compared to that of LSB replacement. More recently, Kodovský et al. [11] introduced the cross-domain feature set (1234 features in total), which considers features from the spatial domain and the DCT domain at the same time. This feature set is known to be effective for steganalysis of the YASS algorithm [12], which embeds secret messages into randomized locations to make the calibration process ineffective.

Many steganographic embedding algorithms are block-based; namely, embedding the secret message into each 8×8 DCT block separately. Yang et al. [13] performed an information-theoretic steganalysis on the block-structured stego image. They provided an approximation of the relative entropy between probability distributions of the cover and the stego images. The relative entropy increases linearly with $N/K - 1$, where N, K represent the total number of samples (pixels) and the block size, respectively. A larger relative entropy means a higher detection probability of the stego image. Although Yang et al. [13] studied block-structured stego images, their work is still a frame-based approach from our viewpoint since only one set of features is extracted from an image.

The block-based image steganalysis was first introduced in [7], which extracted features from smaller blocks for image steganalysis. While the frame-based approach extracts a set of features from the whole image, the block-based approach takes advantage of the rich information of images by extracting a set of features from each individual image block. The characteristics of smaller image blocks were also exploited in [7] to design a content-adaptive classifier for

steganalysis. It was shown by experimental results that the performance of blind steganalysis with merged features is significantly improved using the block-based approach. In this work, we will review results in [7] and add more discussion.

3. Block-based image steganalysis

3.1. System overview

The block-diagram of a block-based image steganalysis system is shown in Fig. 1. It consists of the training process and the testing process, which will be detailed in the following two subsections, respectively.

- The training process. The system decomposes an image into smaller blocks and treats each block as a basic unit for steganalysis. A set of features is extracted from each individual image block and a tree-structured hierarchical clustering technique is used to classify blocks into multiple classes based on extracted features. For each class of blocks, a specific classifier can be trained using extracted features which represent the characteristics of that block class. Note that if the number of training blocks is too large, a statistical sampling method can be used to reduce the number of training blocks.
- The testing process. The system performs the same block decomposition and feature extraction tasks on the test image. Then, it classifies each image block into one specific block class, and uses its associated classifier to make a decision whether the underlying block is a cover/stego block. Finally, there is a decision fusion step that integrates the decisions of multiple blocks into a single decision for the test image is conducted.

For block-based image steganalysis in [7,14], the merged feature set as proposed in [5] was extracted from image blocks, random sampling was adopted as the statistical sampling method in the training process, and the majority voting rule was used to fuse decision results from all the image blocks. For the classification task, a binary classifier was proposed in [7] and a multi-classifier was considered in [14]. It was shown by experimental results in [7,14] that the block-based approach offers better blind steganalysis performance than the frame-based approach.

There are two main advantages with the block-based steganalysis. First, it can offer better steganalysis performance without increasing the number of features. It provides a methodology to complement traditional frame-based steganalysis research that has focused on the search for more effective features. Second, the

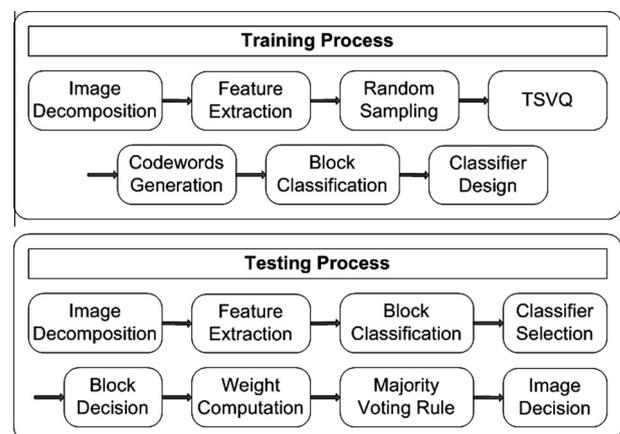


Fig. 1. The block-based image steganalysis system.

block-based scheme can provide more robust detection results for a single test image since the block decomposition step will generate more samples, and each of them can be tested independently. In contrast, the performance of a frame-based scheme is highly dependent on the correlation between the test image and the set of training images. If the test image happens to have characteristics that are very different from those of the training images, the classifier obtained from the training process may not work well for test images.

It is worthwhile to emphasize one main difference between traditional frame-based steganalysis and block-based steganalysis. While only one classifier is obtained after the training process in frame-based scheme, multiple classifiers can be adopted for blocks of different types for a test image in the block-based approach. Intuitively speaking, a content-adaptive classifier should provide more accurate steganalysis performance since each classifier can focus more on the feature changes due to steganographic embedding rather than the feature variations between different block classes.

3.2. Training process

For a given steganographic algorithm, we embed the secret message into the cover image to get its corresponding stego image. This process is applied to all cover images to result in cover/stego image pairs. Then, we decompose all cover/stego image pairs in the training set into smaller blocks of size $B \times B$ ($B = 8b$, $b = 2, 3, \dots, \min(M, N)/8$). The merged DCT and Markov features [5] are extracted from each block of the cover/stego image pairs. Each $B \times B$ block is divided into $B^2/64$ DCT blocks of size 8×8 to compute the inter-block dependency between 8×8 DCT blocks and the intra-block correlation within 8×8 DCT blocks for the merged feature set.

On one hand, the inclusion of more blocks in the training set demands a higher computational cost. On the other hand, a larger number of blocks provides more accurate block classification results. Thus, there is a trade-off between the accuracy and computational complexity, and we need to find a balance between them. If the number of decomposed image blocks is too large, we may use a random sampling method to select a subset of the image blocks to reduce the classification complexity. For example, for an image of size $M \times N$, we have about $A \approx MN/B^2$ blocks of size $B \times B$. If A is too large, we can select a subset of size K randomly. This process is denoted as “random sampling” in Fig. 1.

The training set consists of cover images and the corresponding stego images created with a specific steganographic algorithm. For K sampled blocks selected by random sampling, $K/2$ sample blocks are randomly selected from cover images while the remaining $K/2$ sample blocks are corresponding blocks from stego images at the same location. Generally speaking, random sampling is better than sampling in a spatial order, since it allows us to collect blocks with more diversity so that more representative sample blocks can be used in the block classification process.

Then, we need to think about ways to classify blocks into different classes for block-based image steganalysis. After block classification, a specific classifier will be designed for each block class. We may consider two different methods for block classification as detailed below.

1. Scheme A: classification based on gray levels.

One intuitive way to classify block classes is to use gray levels of the block. If we deal with blocks of size 8×8 , each block has 64 gray level values. Then, vector quantization based on gray scale values can be used to classify blocks into different block classes. However, gray scale values from blocks do not reflect the difference between cover images and stego images. In fact, cover

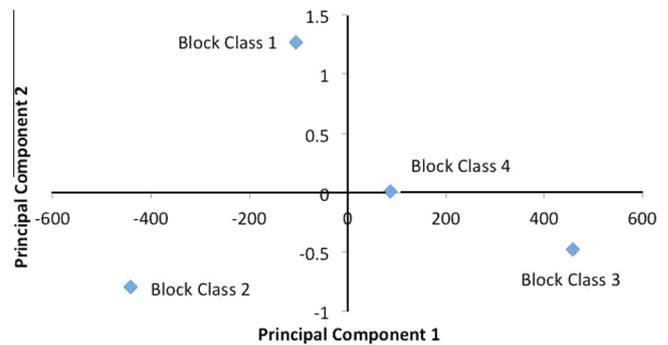


Fig. 2. The 4 codewords representing 4 block types in the 2-D feature space derived from the principal component analysis.

images and stego images are visually identical in most cases. This is because gray scale values are not sensitive to subtle changes made after steganographic embedding.

2. Scheme B: classification based on derived steganalysis features. Another way to do block classification is to use derived steganalysis features. Since our goal is to maximize the performance of classifiers trained by features of different block classes, it is desirable to classify blocks into multiple classes based on the same features used in steganalysis. These classifiers are sensitive to the change of these features as a result of steganographic embedding. After classifying blocks into different classes, the averaged feature vector in each block class is computed, which is called the codeword of that block type. When the merged features are used for block classification, each codeword has 274 feature components. We apply the k-means clustering technique to partition blocks into 4 groups, where each group corresponds to one block class. Then, we apply the principal component analysis to reduce the feature dimension to two. The centroids of all 4 clusters, called the codewords, in the 2-D feature space are shown in Fig. 2.

We compared the performance of block classification schemes A and B, and observed that the detection accuracy of Scheme B is higher than that of Scheme A by 10% or more. Thus, we decided to adopt Scheme B for block classification in block-based image steganalysis.

Based on the merged features from $B \times B$ blocks, we would like to classify K sampled blocks into C different classes, where each class consists of smaller blocks with similar characteristics. If the class number, C , is larger, we may have better steganalysis performance at the cost of higher complexity. Thus, we seek for a suitable C that balances computational complexity and performance. Block classification has been considered in various image processing contexts. The tree structured vector quantization (TSVQ) technique has been used to classify image blocks using a binary tree structure based on block similarity. We borrow this idea and apply it to our current application. The main difference is that block similarity is measured using Euclidean distance between the pixel-wise difference of two image blocks in the vector quantization context. Here, we consider a different criterion as described below.

Following the spirit of TSVQ, we divide the whole set of sampled blocks into 2 sub-sets, and repeat the same process within each sub-set until all blocks have similar characteristics to a certain degree within a sub-set. At each classification step, the K -means clustering algorithm is used to partition blocks in the same class, denoted by S , into 2 sub-classes, denoted by S_1 and S_2 , by minimizing the within-cluster sum of energies $E(S_1, S_2)$. Mathematically, this can be written as

$$E(S_1, S_2) = \sum_{X_i \in S_1} \|X_i - \mu_1\|^2 + \sum_{X_i \in S_2} \|X_i - \mu_2\|^2, \quad (1)$$

where X_1, X_2, \dots, X_n are 274-dimensional feature vectors of n blocks and μ_i is the mean of feature vectors in S_i ; namely,

$$\mu_1 = \sum_{X_i \in S_1} X_i, \quad \mu_2 = \sum_{X_i \in S_2} X_i \quad (2)$$

After classifying K blocks into C classes, the averaged feature vector for each class is computed, which is called the codeword for that class. The codewords will be used to classify the blocks of a test image using the minimum distortion energy criterion in the feature space.

It is worthwhile to point out another difference between our classification scheme and TSVQ. In TSVQ, each intermediate node of the tree, representing a subset of codewords, is split into 2 sub-classes repeatedly to create a symmetric tree. However, our classification scheme does not demand a symmetric tree. If all blocks within a node are homogeneous enough, we can stop further division. Our stopping criterion is based on the value of $E(S_1, S_2)$. That is, we always split a node with the largest minimum $E(S_1, S_2)$ value. The process is repeated until we have C leaves (or classes).

After getting C codewords to represent C classes from K sampled blocks, all $B \times B$ sample blocks in the cover/stego image pairs of the training set will be classified into one of the C classes. The classification is based on a distortion measure $E_i(f_c, f_s)$, which is defined to be the sum of two energies from a codeword of the i th class:

$$E_i(f_c, f_s) = E_i(f_c) + E_i(f_s), \quad (3)$$

where f_c and f_s are the feature vectors of a block from the cover and the stego images, respectively, and

$$E_i(f_c) = \sum_{k=1}^{274} |f_{c,k} - \mu_{i,k}|^2 \quad (4)$$

is the energy between the 274 merged features of a cover image block and the codeword, μ_i , of the i th class, and $\mu_{i,k}$ is the k th component of μ_i . Similarly, we have

$$E_i(f_s) = \sum_{k=1}^{274} |f_{s,k} - \mu_{i,k}|^2, \quad (5)$$

where $f_{c,k}$ is the k th component of f_c . After computing $E_i(f_c, f_s)$ for $i = 1, \dots, C$, the block pair from the cover image and the corresponding stego image in the training set is classified into class C_j , if $E_j(f_c, f_s)$ has the smallest value among all $E_i(f_c, f_s)$, $1 \leq i \leq C$. Using the features of blocks from the cover and stego images of each class, a specific classifier for each class can be obtained for all C classes.

3.3. Testing process

For a given test image, we can perform exactly the same image decomposition and feature extraction as described in the training process. Each block of the test image is classified into a class using the minimum distortion energy. Depending on the class of each block, the classifier obtained from the training process is applied here. We call them content-dependent classifiers since they are adaptively chosen according to the block class. Content-dependent classifiers are useful because changes of feature values after steganographic embedding have higher correlation with blocks of the same class than those of different classes. For example, the effect of embedding secret messages into smooth blocks should be different from the effect of embedding them into texture blocks.

Each $M \times N$ test image consists of MN/B^2 blocks of size $B \times B$. Based on the proposed steganalysis, we can make a decision whether each block is a block from a cover or stego image. Thus,

the total number of decisions made for a given test image is equal to MN/B^2 . Then, a majority voting rule is adopted to make the final decision on whether a given test image is a cover or stego image. It is declared a cover (or a stego) image if the number of cover blocks is larger (or smaller) than that of stego blocks.

4. Analysis of block size, number and overlapping effects

There exists a relationship between the block size and the block number for a given image. If the block size is smaller, there are more blocks. We may ask “what is the best block decomposition strategy?” In the first two subsections, we examine the non-overlapping block case [15]. Then, in the last subsection, we consider the overlapping block case.

4.1. Analysis of block size effect

We study the block size effect for a fixed block number in this subsection. Intuitively speaking, a larger block size should give better steganalysis performance. To understand the block size effect, we analyze the distribution of feature vectors. If the feature vectors of the cover and stego image blocks are more concentrated, it will be easier to design a classifier with higher discriminative power, which has better steganalysis performance. Among the 274 merged features in [5], we observe that the blockiness features have the largest standard deviations. Thus, we will focus on them in our analysis.

There are two blockiness features B_α with $\alpha = 1, 2$, which are used to measure the inter-block dependency of the JPEG image over all DCT modes between neighboring 8×8 DCT blocks. They are defined as [5]

$$B_\alpha = \frac{C_W(\alpha) + C_H(\alpha)}{W \lfloor (H-1)/8 \rfloor + H \lfloor (W-1)/8 \rfloor}, \quad (6)$$

where H and W are the height and the width of the input image in pixels and

$$C_W(\alpha) = \sum_{i=1}^{\lfloor (H-1)/8 \rfloor} \sum_{j=1}^W |c_{8ij} - c_{8i+1,j}|^\alpha, \quad (7)$$

$$C_H(\alpha) = \sum_{j=1}^{\lfloor (W-1)/8 \rfloor} \sum_{i=1}^H |c_{i,8j} - c_{i,8j+1}|^\alpha \quad (8)$$

and where c_{ij} is the gray value of the (i, j) th pixel in the JPEG image. These features are traditionally extracted from each image frame but they are computed from image blocks in the proposed scheme.

Consider an image block that consists of n neighboring DCT block pairs in both horizontal and vertical directions. Let F_i be a feature value extracted from the i th neighboring DCT block pair. Then, the feature value extracted from the image block, \bar{F} , can be written as

$$\bar{F} = \frac{1}{n} \sum_{i=1}^n F_i.$$

It is a sample mean of feature values from neighboring DCT block pairs. For blockiness features B_α , $C_W(\alpha)$ and $C_H(\alpha)$ represent feature values from neighboring block pairs in vertical and horizontal directions, respectively. Furthermore, by assuming that F_i is an independently and identically distributed (i.i.d.) random variable with mean m and variance σ^2 , we can obtain the mean and the standard deviation of \bar{F} as

$$E[\bar{F}] = m, \quad \text{and} \quad \text{Std}[\bar{F}] = \frac{\sigma}{\sqrt{n}}. \quad (9)$$

Table 1

The standard deviations of blockiness (B_1, B_2) features with different block sizes ($B \times B$).

Block size	Standard deviations	
	B_1	B_2
64×64	1.98	187.87
128×128	1.09	95.55
256×256	0.67	56.98

In words, the mean of \bar{F} is the same as the mean of F_i while its standard deviation is reduced by a factor of $1/(\sqrt{n})$. If the block size becomes larger (i.e., a larger value of n), the number of DCT blocks in the image is the same but the number of DCT blocks for each block increases. Then, the standard deviations of feature values become smaller, and it is easier to design a classifier which differentiates stego images from cover images. Note that the feature values also go through a calibration process [5] to improve their sensitivity to steganographic embedding. Since the statistical properties of DCT coefficients remain about the same after the calibration process, the analytical result in Eq. (9) still holds after the calibration process.

We conduct experiments to verify the relationship between the standard deviations of blockiness features and the block size as derived above. The results are shown in Table 1, where the block size is chosen to be 64×64 , 128×128 and 256×256 . The blockiness features are extracted from horizontally and vertically neighboring image block pairs in 200 JPEG images. As shown in Table 1, the standard deviations of blockiness features decrease with an increased block size, which is approximated well by the relationship in Eq. (9). Clearly, larger block sizes result in higher discriminative power of extracted features.

4.2. Analysis of block number effect

In this subsection, we study the block number effect for a fixed block size. Intuitively speaking, the performance of the block-based steganalysis should be better if more blocks are involved in the decision process. This will be demonstrated below.

Consider a test image that consists of N blocks, and the cover/stego decision is made for each individual block based on the extracted features, and the majority voting rule is adopted in the testing process to fuse these N block decisions. If N is an odd number, we need at least $(N + 1)/2$ correct decisions in order to obtain a correct majority voting result. Then, the probability of making a correct decision for the test image can be expressed as

$$P = P(X \geq (N + 1)/2) = 1 - P(X \leq (N - 1)/2), \quad (10)$$

where X is a random variable denoting the number of correct block decisions. If the random variable of making a correct decision for each block is i.i.d., the cumulative distribution function of obtaining less than or equal to k correct decisions from N block decisions can be expressed as

$$P(X \leq k) = F(k; N, p) = \sum_{i=0}^k \binom{N}{i} p^i (1-p)^{N-i}, \quad (11)$$

where p is the probability of correct decision for each block. Clearly, the probability of correct decision, P , for the test image is closely related to the probability of correct block decision, p , as well as the number of block decisions, N . This relationship between P and N parameterized by a fixed value of p will be examined below.

By using the Hoeffding inequality

$$F(k; N, p) \leq \exp\left(-2 \frac{(Np - k)^2}{N}\right), \quad (12)$$

we can determine the upper bound of the cumulative distribution function in Eq. (11) as

$$P(X \leq (N - 1)/2) = F((N - 1)/2; N, p) \leq \exp\left(-2 \frac{(Np - (N - 1)/2)^2}{N}\right). \quad (13)$$

For the majority voting rule to work properly, p should be greater than 0.5 (50%), or

$$p = 0.5 + \varepsilon \quad (0 < \varepsilon < 0.5). \quad (14)$$

The limit of the exponential term in Eq. (13) can be computed as

$$\lim_{N \rightarrow \infty} \exp\left(-2 \frac{(Np - (N - 1)/2)^2}{N}\right) = \lim_{N \rightarrow \infty} \exp(-2(\varepsilon^2 N + 1/4N + \varepsilon)) = 0. \quad (15)$$

The above equation, together with Eq. (13), leads to

$$\lim_{N \rightarrow \infty} P(X \geq (N + 1)/2) = 1 - \lim_{N \rightarrow \infty} P(X \leq (N - 1)/2) = 1. \quad (16)$$

This means that the probability of making a correct decision from N block decisions, P , using the majority voting converges to 1 (100% detection accuracy) as the block number, N , goes to the infinity. We plot the image decision accuracy, P , as a function of the block number, N , parameterized by the p value using the majority voting rule in Fig. 3, where $p = 51\%$, 55% , 60% . As shown in the figure, we get a higher decision accuracy for a test image if we have a larger block number. In practice, the block decision is not an independent event, and the block decision accuracy, p , is not identical since it depends on the block class (e.g., smooth, edged and textured regions). Although being over-simplified, the above analysis does provide a general trend.

4.3. Analysis of block overlapping effect

Although it is beneficial to have a large block size and a large block number for the block-based image steganalysis, there exists a trade-off between the block size and the block number for image decomposition with non-overlapping blocks. Although overlapping blocks are not independent, the use of overlapping blocks provides an alternative to increase the block number for a fixed image size.

For overlapping blocks, the step size is used to measure the degree of overlap between two neighboring overlapping blocks in both the horizontal and vertical directions. An example is illustrated in Fig. 4, where the image size is 512×512 and the block size is 256×256 . The overlap size, O , is the overlapped distance between two neighboring overlapping blocks while the step size,

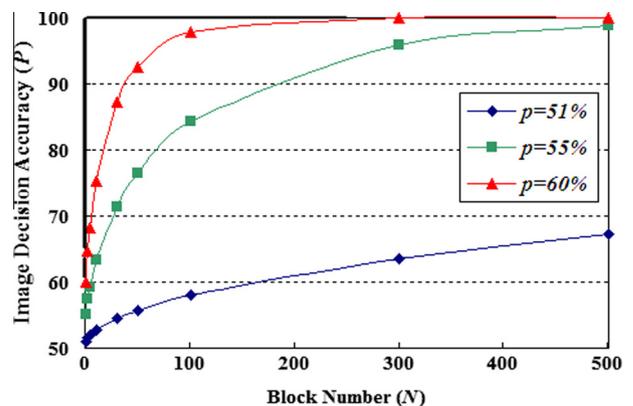


Fig. 3. The image decision accuracy (P) as a function of the block number (N) parameterized by the block decision accuracy $p = 51\%$, 55% , 60% .

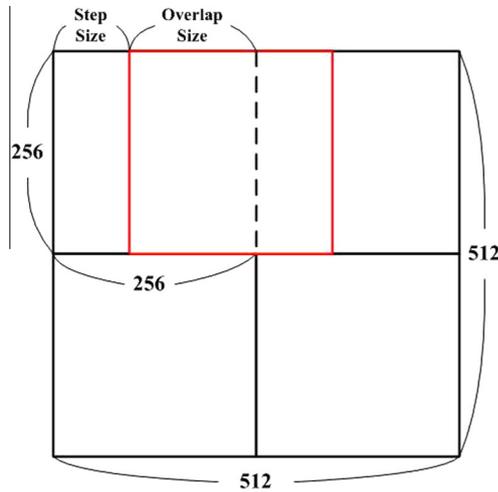


Fig. 4. Illustration of the overlap size (O) and the step size (S) for the overlapping block case.

S , is the displacement of two neighboring blocks. Clearly, $O + S = B$. For block size $B \times B$ and step size S , we can compute the block number as

$$N = [(W - B)/S + 1] \times [(H - B)/S + 1], \tag{17}$$

where H and W are the height and the width of the image, respectively. The block number in an 512×512 image with different block sizes and step sizes is given in Table 2. For a block of size $B \times B$, the block number for 3 different step sizes is computed: non-overlapping blocks ($S = B$), overlapping blocks with a step size set to one half of the block size ($S = B/2$) and one quarter of the block size ($S = B/4$).

The advantage of using overlapping blocks in block-based steganalysis is shown in Fig. 5. By reducing the step size from B to one half and one quarter of B , we obtain more block samples. As we have larger block numbers with smaller step sizes, the curve in Fig. 5 moves towards the upper right direction. Intuitively, for a given block size, if there are more block samples, the classifier can provide a better decision. For example, for a block size of 64×64 , the total number of blocks is 64 with non-overlapping blocks ($S = B$). With overlapping blocks, the total number of blocks increases to 225 and 841 for step size equal to 32 ($S = B/2$) and 16 ($S = B/4$), respectively.

5. Fusion of block decisions

It is often beneficial to combine multiple local decisions to make a single global decision in decision making [16,17]. The majority voting method was considered in the last two sections. There are more decision fusion methods such as weighted majority voting, Bayesian decision fusion, and the Dempster-Shafer theory of

Table 2
The block number (N) in 512×512 image with different block sizes ($B \times B$) and step sizes (S).

Block size	Block number		
	$S = B$	$S = B/2$	$S = B/4$
256×256	4	9	25
128×128	16	49	169
64×64	64	225	841
32×32	256	961	3721

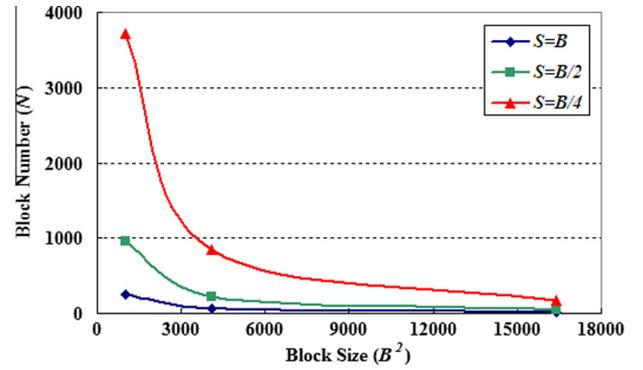


Fig. 5. The block number (N) in a 512×512 image for different block sizes ($B \times B$) and step sizes (S).

evidence. We will examine them in this section and see how they affect the final decision accuracy in the next section.

For the binary classifier case, there are only two decisions ($L = 2$): cover image ($l = 1$) and stego image ($l = 2$). For the general L -classifier case, where $L \geq 2$ is an integer, we can determine the applied steganographic algorithms for stego images as well. Although we focus on the case of $L = 2$, the following discussion on decision fusion is applicable to any L .

5.1. Weighted majority voting

The simple majority voting method can be modified by taking the reliability of each block decision into account. The weight of each block decision can be derived from the block classification performance. The block decision accuracy is defined as

$$P(\text{actual} = I_l | \text{decide} = I_l), \quad l = 1, 2, \dots, L, \tag{18}$$

which is the conditional probability of a block is actually from class I_l given that it is classified to class I_l . Then, the decision for a block that is classified to type I_l is weighted by its block decision accuracy as defined in Eq. (18). The weight is used to reflect the reliability of block decisions in the majority voting rule.

5.2. Bayesian decision fusion

The basic idea of the Bayesian decision fusion [17] can be stated as follows. After obtaining N block decision results $c = [c_1, \dots, c_N]$ from a test image, we would like to decide which class this test image belongs to. This can be done by computing the posterior probability $P(w_l|c)$ for all the classes w_1, \dots, w_L and choosing the class that maximizes the value of $P(w_l|c)$.

If the total number of blocks in the training set is N and the number of blocks classified into class w_l is N_l , then N_l/N provides an estimate of the prior probability of class w_l , which is denoted by $P(w_l)$. The stability of the prior probability is important in order to get accurate result with Bayesian decision fusion. This is another reason why the block-based approach is useful. As the frame-based approach deals with an image as a whole, we only have one sample from each image. However, we are getting numerous samples from each image with the block-based approach, which enables the prior probability value to be stable. For example, if we decompose an image with size 384×512 into smaller blocks with size 32×32 , then we have 192 blocks from each image. If there are 1,000 images in the training set, then we already have 192,000 sample blocks from the training set, which should be enough samples to make the prior probability value stable. In addition, these smaller blocks are more homogeneous compared to original images, which makes it easier to aggregate blocks with similar properties into the same block class.

Under the assumption of independent block decisions, the conditional joint probability density $P(c|w_k)$ can be written as the product of the marginal conditional probabilities as

$$P(c|w_j) = P(c_1, \dots, c_N|w_j) = \prod_{n=1}^N P(c_n|w_j). \quad (19)$$

Although block decisions are not totally independent, the above equation still holds approximately [18]. Furthermore, by assuming that the marginal conditional probabilities $P(c_n|w_j)$ for $n = 1, \dots, N$ are i.i.d., we can obtain their values from the training data set.

Finally, the posterior probability can be expressed as

$$P(w_j|c) = \frac{P(c|w_j)P(w_j)}{P(c)} \quad (20)$$

and the fused Bayesian decision is chosen to be the following class

$$w_j^* = \arg \max_{w_j} P(w_j|c) \quad (21)$$

$$= \arg \max_{w_j} \frac{P(c|w_j)P(w_j)}{P(c)} \quad (22)$$

$$= \arg \max_{w_j} P(c|w_j)P(w_j), \quad (23)$$

where the last equality holds since $P(c)$ is independent of w_j and can be dropped in the optimization formulation.

5.3. Fusion via Dempster–Shafer theory of evidence

The Dempster–Shafer theory of evidence is a methodology to compute and accumulate belief functions according to Dempster's rule [19,20,17]. The degree of belief of an event is different from its probability since its probability can be non-zero even its degree of belief is zero.

We first introduce two concepts: decision templates and decision profiles. The decision template DT^j for class w_j is an $N \times L$ matrix with its n th row being the decision result for the n th block, consisting of marginal conditional probabilities, $P(c_n|w_j)$, with c_n takes values of w_1, \dots, w_L . The decision template can be obtained using the training data set. Note that $P(c_n|w_j)$ can be estimated with block decision accuracy from the training set. The block decision accuracy is the probability of blocks classified into the c_n th class when they actually belong to the w_j th class.

The decision profile (DP) is an $N \times L$ matrix in form of

$$DP = \begin{bmatrix} S_1 \\ \dots \\ S_n \\ \dots \\ S_N \end{bmatrix} = \begin{bmatrix} S_{1,1} \cdots S_{1,j} \cdots S_{1,L} \\ \dots \\ S_{n,1} \cdots S_{n,j} \cdots S_{n,L} \\ \dots \\ S_{N,1} \cdots S_{N,j} \cdots S_{N,L} \end{bmatrix}, \quad (24)$$

where

$$S_{nj} = \begin{cases} 1, & \text{if output of the } n\text{th block decision is class } w_j \\ 0, & \text{otherwise} \end{cases} \quad (25)$$

is the degree of support to class w_j with the n th block decision.

Next, we define two quantities based on decision templates and decision profiles: the similarity and the degree of belief. The similarity between the decision profile of the n th block in the w_j th class and the decision template can be measured as

$$\Phi_{n,j} = \frac{\left(1 + \left(\|DT_n^j - DP_n\|\right)^2\right)^{-1}}{\sum_{k=1}^L \left(\left(1 + \left(\|DT_n^k - DP_n\|\right)^2\right)^{-1}\right)}, \quad (26)$$

where DP_n represents the n th row of DP and DT_n^j represents the n th row of DT_j belonging to class w_j , and $\|\cdot\|$ is a matrix norm. The degree of belief for the decision that the n th block is in class w_j is defined as

$$b_{n,j} = \frac{\Phi_{n,j} \left[\prod_{k=1, k \neq j}^L (1 - \Phi_{n,k}) \right]}{1 - \Phi_{n,j} \left[\prod_{k=1, k \neq j}^L (1 - \Phi_{n,k}) \right]}. \quad (27)$$

It is worthwhile to point out that both the degree of belief and the similarity metric become larger as the decision profile is more similar to the decision template. However, they are different in the sense that the degree of belief considers taking the distribution of dissimilar classes into account while the similarity metric does not. For a given similarity metric, $\Phi_{n,j}$, the degree of belief, $b_{n,j}$, can still vary. It will give the maximum value if the remaining similarity values are equal. On the other hand, it will yield a smaller value if the distribution of remaining similarity values is skewed.

Finally, the accumulated degree of belief for each class w_j , $j = 1, \dots, L$ from all block decisions can be computed using Dempster's rule as

$$g_j = \prod_{i=1}^N b_{i,j}. \quad (28)$$

A test image is classified into class w_j if its associated g_j value is the largest among all values of $j = 1, \dots, L$. We will examine detection accuracy using different decision fusion methods in the next section.

6. Performance evaluation

The performance of block-based image steganalysis for a binary classifier (either stego or cover image) will be studied in this section. We will compare the proposed block-based approach with the frame-based approach. We will provide experimental results by varying parameters in block-based image steganalysis so as to understand the effects of block sizes, block numbers, and block overlapping.

The performance of blind steganalysis is measured by the average detection accuracy:

$$A_{detect} = 1 - P_{error}, \quad (29)$$

where P_{error} is the average error probability. There are two types of errors in the decision process: false positives and false negatives. Blind steganalysis attempts to minimize these two errors in order to obtain higher detection accuracy. False positives (false alarms) happen when a secret message is detected from a given cover image. In contrast, false negatives (misses) occur when a secret message is not detected from a given stego image. With these two types of errors, the average error probability P_{error} can be written as

$$P_{error} = \frac{1}{2}(P_{FP} + P_{FN}), \quad (30)$$

where P_{FP} is the probability of false positives and P_{FN} is the probability of false negatives. Thus, we have

$$A_{detect} = 1 - \frac{1}{2}(P_{FP} + P_{FN}). \quad (31)$$

6.1. Experimental set-up

In the experiment, we consider training and testing images of dimension $M \times N = 384 \times 512$ and decompose each image into blocks of size $B \times B$. After extracting 274 merged features from



Fig. 6. Sample images from the Uncompressed Colour Image Database (UCID) and the INRIA Holidays dataset.

each block, $K = 20,000$ sample blocks are selected from cover and stego images in the training set by random sampling. These sample blocks are classified into C classes and a classifier is obtained for each class.

The uncompressed colour image database (UCID) [21] was used as the cover images in the training set. The INRIA Holidays dataset [22] was used as the cover images in the test set. The UCID image database consists of 1338 images, and the Holidays image database has 1491 images, which have diverse subjects such as natural scenes and artificial objects as shown in Fig. 6. Although the original images were color images of different sizes, all images have been changed into 384×512 gray-level images and saved as JPEG files with a quality factor of 85 with JPEG compression.

After obtaining cover images from the image databases, the model-based steganography (MBS) method [23] and the perturbed quantization (PQ) method [24] were used to embed a secret message into the cover images to create the corresponding stego images. While the MBS method uses the original JPEG images obtained with a quality factor of 85 for cover images, the PQ method demands double-compressed JPEG images. In our experiment, the original JPEG images were compressed once again with a quality factor of 70 for the PQ method. As different images may have different embedding capacity, the embedding strength for each image is measured in units of BPC (bits per non-zero DCT AC coefficients). Unless explicitly stated, the default BPC value was set to 0.20 for both MBS and PQ methods.

6.2. Comparison of frame-based and block-based image steganalysis

The detection accuracy of the proposed block-based image steganalysis is reported in this subsection. In the experiment, the MBS method [23] and the PQ method [24] were used to create stego images from cover images with 5 embedding rates (0.05, 0.10, 0.20, 0.30, and 0.40 BPC). We decompose each image from the training set into blocks of size $B \times B = 64 \times 64$. For the classifier design, 16 different linear Bayes classifiers are obtained

Table 3

Performance comparison of Pevny's method and the proposed block-based image steganalysis.

Steganography	BPC	Pevny's	Proposed
MBS	0.05	55.94	65.79
MBS	0.10	62.58	75.42
MBS	0.20	74.75	89.57
MBS	0.30	83.37	95.00
MBS	0.40	89.34	98.09
PQ	0.05	55.37	58.22
PQ	0.10	55.70	60.36
PQ	0.20	56.04	63.65
PQ	0.30	57.08	66.50
PQ	0.40	58.12	69.42

for $C = 16$ classes with regularization parameter $R = S = 0.001$. The majority voting scheme was adopted to fuse block decision results to make final decision.

For the benchmarking purpose, detection accuracy of the merged features in [5] using the linear Bayes classifier is also given. This frame-based approach is referred to as Pevny's method. The performance of these two methods is shown in Table 3. As the PQ method is known to be more secure than the MBS method, we see that the detection accuracy of Pevny's and the proposed methods is significantly lower with respect to the PQ method. Detection accuracy improves with higher embedding rates since it becomes easier to differentiate stego images from cover images when a larger amount of hidden information is embedded. The proposed block-based image steganalysis has better detection accuracy than Pevny's method regardless of steganographic algorithms and embedding rates. The maximum performance improvement of the proposed method over Pevny's method is close to 15% for the MBS method with an embedding rate of 0.20 BPC.

When the majority voting is used for decision fusion, the ratio of the number of correct decisions and the total number of

Table 4
Relationship between decision reliability and voting difference.

Voting difference	Correct decisions	Incorrect decisions	Decision reliability
0–5	432	122	77.98
6–10	717	73	90.76
11–15	541	15	97.30
16–20	656	6	99.09
21–48	419	1	99.76

decisions offers a reliability measure of the decision. Intuitively speaking, the voting difference between the numbers of cover and stego blocks serves as an indicator. That is, if the voting difference is larger, the decision is more reliable. We show the relationship between decision reliability and the voting difference in Table 4, which is obtained using the MBS method with an embedding rate of 0.20 BPC. It is clear that detection reliability improves with larger voting difference. The decision reliability increases from 77.98% with 0–5 voting difference to 99.76% with 21–48 voting difference. For a given test image, the traditional frame-based steganalysis cannot provide the measure of detection reliability.

6.3. Performance study of block-based image steganalysis

For the performance study of block-based image steganalysis, 200 images from the uncompressed colour image database (UCID) [21] and the INRIA Holidays dataset [22] were used as cover images in the training set and the testing set, respectively. The MBS method [23] was used to create stego images with an embedding rate of 0.20 BPC. In the experiment, blocks were classified into $C = 8$ classes and 8 linear Bayes classifiers were obtained with regularization parameters $R = S = 0.001$.

6.3.1. Effect of block sizes

First, we study the effect of block sizes. We would like to check whether the merged features from blocks of a larger size have better discriminative power to differentiate cover and stego images. For each block size, we counted the number of correct and incorrect block decisions from all blocks obtained from 200 test images to compute the average block decision accuracy (p). The discriminative power of merged features for 4 block sizes (32×32 , 64×64 , 128×128 , 256×256) is shown in Table 5. Note that overlapping block decomposition is used for block size 256×256 . As shown in this table, the discriminative power of merged features from a larger block is better than that of merged features from a smaller block. The average block decision accuracy increases from 56.62% to 62.54% when the block size increases from 32×32 to 256×256 .

6.3.2. Effect of block numbers

Next, we study the effect of block numbers. In the experiment, a block size of $B \times B = 32 \times 32$ was used for images of size 384×512 . Then, each image consists of 192 blocks. Among these 192 blocks, a different number of blocks was randomly selected

Table 5
The average block decision accuracy (p) with different block sizes ($B \times B$).

Block size	Block number	No. of Block decisions		Decision accuracy
		Correct	Incorrect	
32×32	192	43,486	33,314	56.62
64×64	48	11,254	7946	58.61
128×128	12	2962	1838	61.71
256×256	6	1501	899	62.54

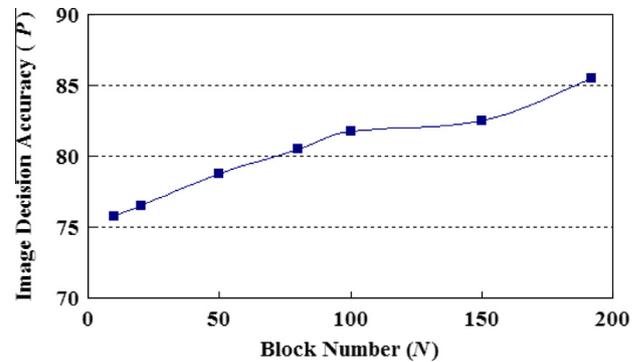


Fig. 7. The image decision accuracy, P , as a function of the block number, N .

Table 6

The average image decision accuracy (P) for non-overlapping block decomposition with fixed image size 384×512 .

Block size	Block number	Detection accuracy
32×32	196	81.16
64×64	48	82.16
128×128	12	69.50
256×256	2	59.25

for majority voting in the testing process. The average image decision accuracy, P , is plotted as a function of the block number, N in Fig. 7. We see from this figure that the average image decision accuracy, P , improves as more blocks are selected from the test image. The detection accuracy increases from 75.75% to 85.50% when the block number increases from 10 to 192. This experimental result clearly demonstrates the advantage of having a larger block number in block-based image steganalysis.

6.3.3. Effect of block overlapping

There exists a trade-off between the block size and the block number in non-overlapping block decomposition. If the block size becomes smaller, the block decision accuracy gets lower. On the other hand, if the block decision accuracy becomes higher with a larger block size, only a small number of blocks are available for the majority voting process. For this experiment, 200 images were used for the training set and the testing set, respectively. The average image decision accuracy P (detection accuracy) with different block sizes ($B \times B$) for the non-overlapping block decomposition case is shown in Table 6.

Among 4 different block sizes, the block-based image steganalysis with block size 64×64 has the best detection accuracy of 82.16%. If the block size is larger than 64×64 , the detection accuracy decreases due to a smaller block number. The detection accuracy also decreases when the block size is less than 32×32 due to lower block decision accuracy.

The advantage of using overlapping blocks is shown in Table 7. In this experiment, 400 images were used for the training set and the testing set, respectively. If the step size is the same as the block size ($S = B$), it is the same as the non-overlapping block case. With the use of overlapping blocks, the average image decision accuracy (the average detection accuracy) increases from 71.82% to 80.96% for block size of 128×128 , and from 79.22% to 82.66% for block size of 64×64 . Overall, we can achieve a detection accuracy slightly over 80% using block-based image steganalysis with overlapping blocks. Furthermore, we see that a larger block number contributes more to detection accuracy than a larger block size. For example, the detection accuracy increases from 80.96% to

Table 7

The average image decision accuracy (P) with different block sizes ($B \times B$) and different step sizes (S).

Block size	Step size	Overlap size	Block number	Detection accuracy
128×128	128	0	12	71.82
128×128	32	96	117	79.92
128×128	16	112	425	80.96
64×64	64	0	48	79.22
64×64	32	32	165	80.55
64×64	16	48	609	82.66

Table 8

Detection accuracy with different number of block classes.

Number of classes	Detection accuracy		
	Cover image	Stego image	Total
2	64.52	78.27	71.40
4	73.98	75.45	74.71
8	81.29	82.29	81.79
16	86.32	85.11	85.71
32	86.92	88.26	87.59
64	90.48	86.65	88.56

Table 9

Performance comparison of block-based image steganalysis with different fusion methods.

Decision fusion techniques	Detection accuracy		
	Cover image	Stego image	Total
Weighted majority voting	78.54	84.91	81.72
Bayesian decision fusion	78.74	85.38	82.06
Dempster–Shafer theory of evidence	79.28	85.51	82.39

82.66% as the block size decreases from 128×128 to 64×64 when overlapping blocks with step size 16 were used. This result shows that the detection accuracy can be improved by using overlapping blocks even though they are not independent.

6.3.4. Effect of block class number

The performance of block-based image steganalysis depends on the number of block classes, C . The more block classes we have, more codewords can be used to make the average distance between the codeword and block samples smaller. Thus, detection accuracy is expected to improve with a higher block class number. The detection accuracy with different numbers of block classes is shown in Table 8. We see that detection accuracy increases with the block class number. As the block class number increases from 2 to 64, detection accuracy increases from 71.40% to 88.56%. However, the performance improvement saturates as the block class number reaches 32 and beyond.

6.3.5. Effect of decision fusion schemes

The majority voting scheme was adopted to fuse block decision results to make final decision for a given test image in the above subsections. Here, we compare detection accuracy of block-based image steganalysis with three decision fusion schemes (namely, weighted majority voting, Bayesian decision fusion and Dempster–Shafer theory of evidence) in Table 9, where the block class number was chosen to be 8. In the experiment, the MBS method [23] was used to create stego images with an embedding rate 0.20 BPC. We decompose each image into blocks of size $B \times B = 64 \times 64$. We see slight performance improvement with the Bayesian decision fusion and the Dempster–Shafer theory of evidence over the weighted majority voting. The overall detection accuracy increases from 81.72% to 82.06% and 82.39%, respectively, which is less than 1%. This indicates that the performance of the proposed block-based image steganalysis is robust and it is not much affected by the specific decision fusion rule applied.

6.4. Effect of classifiers

A linear Bayes classifier was used in all experiments in Sec. 6.3. In this subsection, we will compare the performance of block-based image steganalysis with different classifiers (including the linear Bayes classifier, the Fisher linear discriminant classifier and the logistic classifier) and show the results in Table 10. In the experiment, the MBS method [23] was used to create stego images with an embedding rate of 0.20 BPC. We decompose each image from the training set and the testing set into blocks of size

Table 10

The performance improvement of block-based image steganalysis with different classifiers for MBS.

Classifier type	Number of classes	Detection accuracy		
		Cover image	Stego image	Total
Linear Bayes classifier	8	81.29	82.29	81.79
Logistic classifier	8	97.38	90.54	93.96
Fisher linear discriminant classifier	8	97.59	90.14	93.86
Linear Bayes classifier	16	85.24	87.86	86.55
Logistic classifier	16	96.31	93.63	94.97
Fisher linear discriminant classifier	16	96.85	93.36	95.10

Table 11

The performance comparison of block-based image steganalysis with different classifiers under the PQ method.

Classifier type	Number of classes	Detection accuracy		
		Cover image	Stego image	Total
Linear Bayes classifier	8	56.07	59.02	57.55
Logistic classifier	8	70.49	58.42	64.45
Fisher linear discriminant classifier	8	64.92	64.12	64.52
Linear Bayes classifier	16	56.00	60.43	58.22
Logistic classifier	16	68.88	59.29	64.08
Fisher linear discriminant classifier	16	65.12	64.52	64.82

$B \times B = 64 \times 64$. Sample blocks are classified into $C = 8, 16$ classes and a classifier is obtained for each class. The majority voting scheme was adopted to fuse block decision results to make the final decision.

We see that both the logistic classifier and the Fisher linear discriminant classifier outperform the linear Bayes classifier by a significant margin. When the number of block classes is 8, the detection accuracy improves from 81.79% to 93.96% and 93.86% and, when the number of classes is 16, the detection accuracy improves from 86.55% to 94.97% and 95.10%, for the logistic classifier and the Fisher linear discriminant classifier, respectively.

We also observe performance improvement for the PQ method with different classifiers. The performance comparison of block-based image steganalysis for the PQ method with different classifiers is given in Table 11, where the embedding rate was set to 0.2 BPC. As the PQ method is known to be more secure than the MBS method, the detection accuracy is lower regardless of classifier type and the class number. When the block class number is 8, detection accuracy improves from 57.55% to 64.45% and 64.52% and, when the number of classes is 16, detection accuracy improves from 58.22% to 64.08% and 64.82%, for the logistic classifier and the Fisher linear discriminant classifier, respectively. The performance improvement is around 6% for both cases, which is smaller than that of the MBS method.

7. Conclusion and future extension

A block-based image steganalysis system was proposed in this work, and extensive performance evaluation of block-based image steganalysis was conducted. It was shown by experimental results that the proposed method offers a significant improvement in detection accuracy when compared to prior art using a frame-based approach. Besides, block-based image steganalysis offers decision reliability information even with only one test image given, which is not available with the frame-based approach.

We studied the performance of the block-based steganalysis by varying different parameters, including the block size, the block number, the effect of block overlapping, the block class number, the decision fusion scheme and the classifier choice. It was observed that the performance of block-based image steganalysis is less sensitive to the decision fusion methods but more sensitive to the classifier choice. Specifically, the Fisher linear discriminant classifier and the logistic classifier outperforms the linear Bayes classifier by a substantial margin.

One possible future extension is to use adaptive block decomposition. In the current system, images are decomposed into smaller blocks of the same size. However, not all blocks are homogenous with a fixed block size depending on block characteristics. Thus, it would be beneficial to consider adaptive block decomposition, which changes the block size adaptively based on block characteristics. In this paper, we assumed that block decisions are independent when we use multiple block decisions to make a final decision for a given test image. As block decisions are dependent especially when we consider overlapping blocks, it

will be interesting to analyze the performance of block-based image steganalysis more accurately by taking the dependency of block decisions into account. Furthermore, although we have achieved excellent steganalysis performance for the MBS method with a correct detection rate in the range of 95%, the detection rate for the PQ method is still in the range of 65%. Thus, more efforts have to be done in this area in the future.

References

- [1] A. Cheddad, J. Condell, K. Curran, P. Mc Kevitt, Digital image steganography: survey and analysis of current methods, *EURASIP Journal on Signal Processing* 90 (3) (2010) 727–752.
- [2] I. Cox, M. Miller, J. Bloom, J. Fridrich, T. Kalker, *Digital Watermarking and Steganography*, Morgan Kaufman, 2007.
- [3] J. Fridrich, Feature-based steganalysis for JPEG images and its implications for future design of steganographic schemes, in: *Proc. Int. Workshop on Information Hiding Toronto, Canada, 2004*.
- [4] Y. Shi, C. Chen, W. Chen, A Markov process based approach to effective attacking JPEG steganography, in: *Proc. Int. Workshop on Information Hiding, Old Town Alexandria, VA, 2006*.
- [5] T. Pevný, J. Fridrich, Merging Markov and DCT features for multi-class JPEG steganalysis, in: *Proc. SPIE Conf. Security, Watermarking, and Steganography, San Jose, CA, 2007*.
- [6] B. Rodriguez, G. Peterson, K. Bauer, S. Agaian, Steganalysis embedding percentage determination with learning vector quantization, in: *Proc. IEEE Int. Conf. Systems Man and Cybernetics, Taipei, Taiwan, 2006*.
- [7] S. Cho, B.-H. Cha, J. Wang, C.-C.J. Kuo, Block-based image steganalysis: algorithm and performance evaluation, in: *Proc. IEEE Int. Symp. Circuits and Systems Paris, France, 2010*.
- [8] C. Chen, Y. Shi, JPEG image steganalysis utilizing both intrablock and interblock correlations, in: *Proc. IEEE Int. Symp. Circuits and Systems Seattle, WA, 2008*.
- [9] J. Kodovský, J. Fridrich, Calibration revisited, in: *Proc. ACM Multimedia & Security Workshop, Princeton, NJ, 2009*.
- [10] T. Pevný, P. Bas, J. Fridrich, Steganalysis by subtractive pixel adjacency matrix, in: *Proc. ACM Multimedia & Security Workshop, Princeton, NJ, 2009*.
- [11] J. Kodovský, J. Fridrich, Modern Steganalysis Can Detect YASS, in: *Proc. SPIE Conf. Electronic Imaging, Media Forensics and Security, San Jose, CA, 2010*.
- [12] K. Solanki, A. Sarkar, B. Manjunath, Yass: yet another steganographic scheme that resists blind steganalysis, *Information Hiding, Springer, 2007*.
- [13] Y. Wang, P. Moulin, Steganalysis of block-structured stegotext, in: *Proc. SPIE Conf. Security, Watermarking, and Steganography, San Jose, CA, 2004*.
- [14] S. Cho, B.-H. Cha, J. Wang, C.-C.J. Kuo, Block-based image steganalysis for a multi-classifier, in: *Proc. IEEE Int. Conf. Multimedia and Expo, Singapore, 2010*.
- [15] S. Cho, B.-H. Cha, J. Wang, C.-C.J. Kuo, Performance study on block-based image steganalysis, in: *Proc. IEEE Int. Symp. Circuits and Systems, Rio de Janeiro, Brazil, 2011*.
- [16] C. Kraetzer, J. Dittmann, The impact of information fusion in steganalysis on the example of audio steganalysis, in: *Proc. Media Forensics and Security XI, IS&T/SPIE Electronic Imaging Conference San Jose, CA, 2009*.
- [17] A. Ross, K. Nandakumar, A. Jain, *Handbook of Multibiometrics, International Series on Biometrics, Springer Verlag, 2006*.
- [18] P. Domingos, M. Pazzani, On the optimality of the simple bayesian classifier under zero-one loss, *Machine Learning* 29 (2) (1997) 103–130.
- [19] G. Rogova, Combining the results of several neural network classifiers, *Neural Networks* 7 (5) (1994) 777–781.
- [20] L. Kuncheva, Using measures of similarity and inclusion for multiple classifier fusion by decision templates, *Fuzzy Sets and Systems* 122 (3) (2001) 401–407.
- [21] G. Schaefer, M. Stich, UCID – An uncompressed colour image database, in: *Proc. SPIE Conf. Storage and Retrieval Methods and Applications for Multimedia, San Jose, CA, 2004*.
- [22] H. Jégou, M. Douze, C. Schmid, Hamming embedding and weak geometric consistency for large scale image search, in: *European Conf. Computer Vision Marseille, France, 2008*.
- [23] P. Sallee, Model-based steganography, in: *Proc. Int. Workshop on Digital Watermarking Seoul, Korea, 2003*.
- [24] J. Fridrich, M. Goljan, D. Soukal, Perturbed quantization steganography, *ACM Multimedia System Journal* 11 (2) (2005) 98–107.