Forensics Aided Steganalysis of Heterogeneous Bitmap Images with Different Compression History

Xiaodan Hou, Tao Zhang, Gang Xiong and Baoji Wan
Zhengzhou Information Science and Technology Institute
Zhengzhou, Henan 450002 - P. R. China
[e-mail: {hxd2305, dirker2012}]@163.com, {dr.zhangtao, gangxiong1986}@gmail.com]
*Corresponding author: Xiaodan Hou

Received June 4, 2012; revised July 16, 2012; accepted August 16, 2012; published August 30, 2012

Abstract

In this paper, two practical forensics aided steganalyzers (FA-steganalyzer) for heterogeneous bitmap images are constructed, which can properly handle steganalysis problems for mixed image sources consisting of raw uncompressed images and JPEG decompressed images with different quality factors. The first FA-steganalyzer consists of a JPEG decompressed image identifier followed by two corresponding steganalyzers, one of which is used to deal with uncompressed images and the other is used for mixed JPEG decompressed images with different quality factors. In the second FA-steganalyzer scheme, we further estimate the quality factors for JPEG decompressed images, and then steganalyzers trained on the corresponding quality factors are used. Extensive experimental results show that the proposed two FA-steganalyzers outperform the existing steganalyzer that is trained on a mixed dataset. Additionally, in our proposed FA-steganalyzer scheme, we can select the steganalysis methods specially designed for raw uncompressed images and JPEG decompressed images respectively, which can achieve much more reliable detection accuracy than adopting the identical steganalysis method regardless of the type of cover source.

Keywords: Information hiding, steganalysis, LSB matching, image forensics, forensics aided steganalysis

This work was supported by the National Natural Science Foundation of China under grant No. 60903221.
DOI: 10.3837/tiis.2012.08.003

1. Introduction

As a new research direction of information security field, modern information hiding techniques have attracted extensive attention in academe once brought forward since the mid 1990s. In the past ten years, the battle between steganography and its counterpart steganalysis became more and more drastic. From the literature released in recent years, we can see that the detection techniques for image steganography have achieved fruitful research results, which exhibit excellent detection performance under the laboratory environment. However, the existing steganalysis algorithms are difficult to obtain high detection accuracy when applied to the heterogeneous image sources under the practical network environment, which consist of images generated by various image acquisition devices, equipped with multiplicate image quality, image content and texture and undergoing diverse complex image processing. The main reasons for this phenomenon are shown in the following two aspects:

(1) A wide variety of steganalysis algorithms rely on certain assumptions and restrictions on the statistical properties of cover images, and therefore they are only effective for specific cover image types. For example, some steganalyzers are developed under the assumption that the JPEG stegoimage has been compressed only once, and this is especially true for steganalysis methods based on calibration [1], and thus ignoring the effects of double-compression may lead to extremely inaccurate steganalysis results. Therefore, this issue extremely limits the practical applications of steganalysis algorithms.

(2) Under the practical network environment we have no knowledge of the statistics of the cover images, which is often neglected in the current literature. So this may result in a mismatch between the statistics of the training set and those of the testing set, which can significantly decrease the performance of a steganalyzer [2][3]. For example, the JPEG format accepts the quantization table as a parameter and different tables will induce a change of statistical properties of DCT (discrete cosine transform) coefficients, thus effectively enlarging the space of JPEG covers. So a steganalyzer trained on one quality factor may give less accurate results on images with a different quality factor (see, e.g., [4]). Consequently, it is very difficult to obtain the high detection accuracy for the existing steganalyzers when applied to the actual heterogeneous images.

The first issue tells us that the existing steganalyzers are much sensitive to the cover image type. So how to construct a feature set capable of reliably classifying images from various sources is a way to address this issue. However, cover image types are various and complicate, hence making it more difficult to distinguish them from stego images in this way. The second issue shows that without any knowledge of cover source, the single training set may bring on a significant drop in accuracy. So the widely adopted strategy to handle this issue is to train the steganalyzer on as diverse images as possible, but meanwhile it also complicates the steganalysis method.

An alternative approach to deal with the two issues above is to train a bank of steganalyzers for several image types and equip this bank with a source identification, tampering detection or content-based image retrieval preclassifier that would try to recognize the image type and then send the image to the appropriate steganalyzer explicitly designed to work with images of that class. This approach was lately proposed in [3], but the details of an implementation scheme and its performance were not reported .

Recently, some researchers have paid attention to the approach above and presented some primary research results. Pevný et al. [5] constructed a forensic steganalysis tool for JPEG

images that can properly analyze single- and double-compressed stego images and classify them to selected current steganographic methods. Barni et al. [6] explored the steganalysis problem of images produced by different sources. Firstly, a preclassifier was used to identify image source, and then used a version of the steganalyzer that had been explicitly trained to work with images belonging to the correct class. This scheme was implemented in a simple set up involving only two image classes—computer generated and camera images, achieving better detection performance. Amirkhani et al. [7] proposed a new framework that enables us to employ the content of images in blind steganalysis systems, significantly enhancing the detection accuracy of these systems according to the experimental results. However, the new framework was presented based on the hypothesis that the content class of an image must be irrelevant to its type (i.e., cover or stego).

Accordingly there are still two remaining unsolved problems needed to consider for the alternative approach. So far, most of image forensics techniques were designed under the assumption that the image under investigation is a cover image. However, the message embedding will change the statistics of cover images unavoidably, which may impose an effect on the results of forensics classification. Therefore the first problem is how to improve the existing image forensics methods to handle both cover and stego images. Moreover, how to set the decision threshold of image forensics preclassifier to obtain a trade-off on individual steganalyzers and further to get the best overall detection performance is the second problem.

It is well known that JPEG is the most commonly used compression standard in many image capture devices and softwares (such as most digital cameras, Adobe Photoshop). However, JPEG images are sometimes converted and stored as bitmaps. In that case, we have no idea about the compression history, i.e., whether the bitmap comes from a JPEG image or a raw bitmap image. Because different types of images have different statistical properties, in this paper, we devise two practical FA-steganalyzers to deal with the steganalysis problem of heterogeneous bitmap images including raw uncompressed images and JPEG decompressed images with different quality factors. During the whole analysis process, the two problems above are taken into consideration and analyzed. Finally, compared to the existing steganalyzer that is trained on a mixed dataset (noted by a mixed steganalyzer), our proposed scheme is proved to have superior performance.

The rest of the paper is organized as follows. In Section 2, we first simply describe the proposed FA-steganalyzer of heterogeneous bitmap images, and then detailedly demonstrate the improved image forensics techniques and forensics aided steganalysis techniques which are the key techniques involved in the proposed scheme. Some basic assumptions which are reasonable in practical applications in order to simplify the construction of FA-steganalyzers are firstly given, and then the experimental results and the comparisons with a mixed steganalyzer are presented in section 3. Finally, section 4 concludes this paper and gives the future research direction.

2. The Proposed Scheme

Fig. 1 shows a simple description of the proposed FA-steganalyzer of heterogeneous bitmap images including raw uncompressed images and JPEG decompressed images with different quality factors. In the proposed scheme, we first employ the image forensics classifier to decide the image source, and then send the image to the steganalyzer specially designed to work with images of that class. It is obvious that the image forensics technique is one of the most important techniques in the proposed scheme. Additionally, How to combine the image forensics technique and steganalysis technique is another significant point of the proposed

scheme. Subsequently this paper will demonstrate the detailed image forensics technique and forensics aided steganalysis technique.

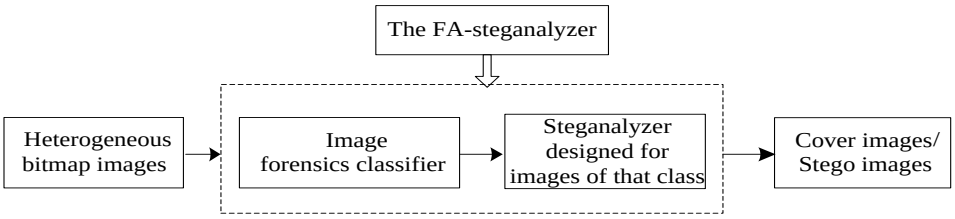


Fig. 1. The FA-steganalyzer of heterogeneous bitmap images

2.1 Image Forensics Analysis

The image forensics techniques involved in the proposed scheme include identifying JPEG decompressed images (i.e., identifying whether a given bitmap image has previously been JPEG compressed), and further detecting quantization table of a JPEG decompressed image (**Fig. 2**).

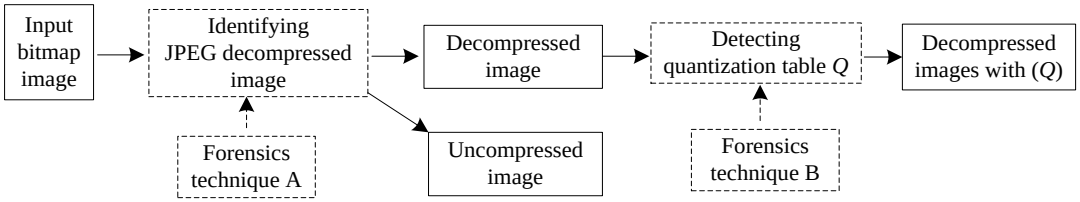


Fig. 2. Image forensics analysis

In [8], Luo et al. developed three novel schemes for image forensics including identifying JPEG decompressed images, estimating quantization steps, and detecting quantization tables from a bitmap image. However these methods were based on the hypothesis that the image under investigation is a cover image. Since the act of embedding further modifies the statistics of cover images , it may impose an effect on the results of forensics classification. From **Fig. 3**, we can observe that the features proposed in [8] between uncompressed cover images and JPEG decompressed stego images are not separated.

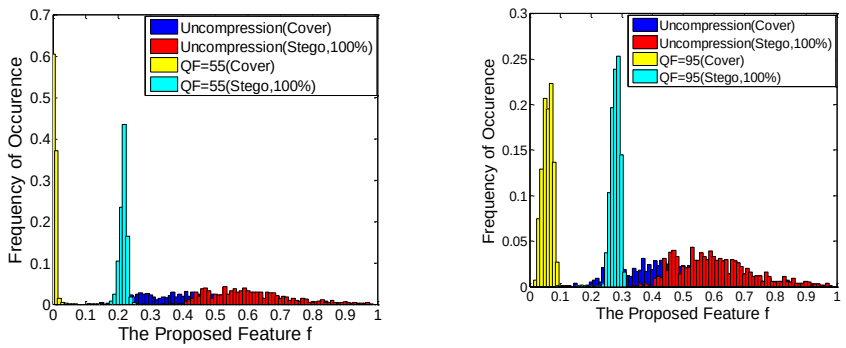


Fig. 3. Histograms of the features f proposed in [8] between uncompressed cover, stego images and JPEG decompressed ones with QFs (quality factor) 55 and 95 at embedding rate 100%

There is a need for methods that can properly identify JPEG decompressed images and detect quantization tables in cover and stego images simultaneously. Based on the methods in [8], this paper presents the improved methods to identify JPEG decompressed images, and detect quantization tables from bitmap images independent of their types (i.e., covers or stegos).

2.1.1 Identifying JPEG Decompressed Images

Firstly, we briefly outline the basic process of JPEG . During JPEG compression, an image I is first split into disjoint 8×8 pixel blocks, and then the DCT of each block is computed. Next, each DCT coefficient is quantized by dividing it by its corresponding entry in a quantization table Q, such that a DCT coefficient d at the block position (i, j) is quantized to the value $D=\text{round}\left(d/Q_{i,j}\right)$. Finally, an entropy coding is applied to the quantized coefficients and the image is said to be JPEG compressed one. In JPEG decompression, the sequence of quantized DCT coefficients is entropy decoded and then rearranged into its original ordering, Dequantization is performed by multiplying each quantized coefficient by its corresponding entry in the quantization table Q, resulting in the dequantized coefficient $\tilde{d}=Q_{i,j}D$. Finally, the inverse DCT (IDCT) of each block of DCT coefficients is computed and the resulting pixel values are rounded to the nearest integer. Pixel values greater than 255 or less than 0 are truncated to 255 or 0 respectively, yielding the decompressed image J .

In this paper, the LSB matching steganography [9] is considered as the representative of additive noise steganography, the basic model of which is shown in **Fig. 4**. To elaborate let J_{C} be JPEG decompressed cover image, and then let J_{S} be JPEG decompressed stego image.

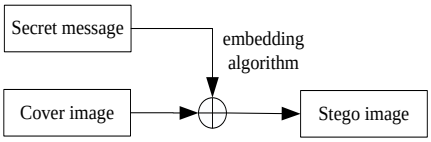


Fig. 4. Additive noise steganography model

namely,

$$J_{\text{S}}=J_{\text{C}}+\eta; \tag{1}$$

Where η is stegonoise, and according to the embedding rule of LSB matching, the probability mass function (PMF) of stegonoise η is as follows:

$$F(\eta)=\begin{cases} r/4, & \eta=-1; \\ 1-r/2, & \eta=0; \\ r/4, & \eta=+1. \end{cases} \tag{2}$$

Please note that r is embedding rate, and thus the mean and the variance of the stegonoise η are $E(\eta)=0,\sigma^2(\eta)=\frac{r}{2}$. The DCT coefficients of J_{C} and J_{S} are denoted by random variable d_{C} and d_{S}, namely, $d_{\text{C}}=\text{DCT}(J_{\text{C}})$, $d_{\text{S}}=\text{DCT}(J_{\text{S}})$, according to (1), we have:

$$d_{\text{S}}=\text{DCT}(J_{\text{S}})=\text{DCT}(J_{\text{C}}+\eta)=\text{DCT}(J_{\text{C}})+\text{DCT}(\eta)=d_{\text{C}}+\gamma \tag{3}$$

where $\gamma=\text{DCT}(\eta)$ represents the DCT coefficients of stegonoise η. According to the Central

Limit Theorem, we can conclude that γ is an approximate Gaussian distribution with mean 0 and variance $\frac{r}{2}$. Based on the error analysis in [8], we have:

$$d_S = \mathrm{DCT}(J_S) = \mathrm{DCT}(J_C + \eta) = \mathrm{DCT}(J_C) + \mathrm{DCT}(\eta) = d_C + \gamma = \tilde{d} + \varepsilon + \gamma = \tilde{d} + \theta \quad (4)$$

Where ε denotes the DCT coefficients of the rounding errors introduced by previous JPEG decompression, and approximately obeys the Gaussian distribution with mean 0 and variance $\frac{1}{12}$, and thus the variable θ $(\theta = \varepsilon + \gamma)$ also approximately follows the Gaussian distribution with $E(\theta) = 0, \mathrm{var}(\theta) = \frac{1}{12} + \frac{r}{2} (0 \le r \le 1)$. The probability density function (pdf) and definite integral of the variable θ are shown in **Fig. 5** and **Table 1**.

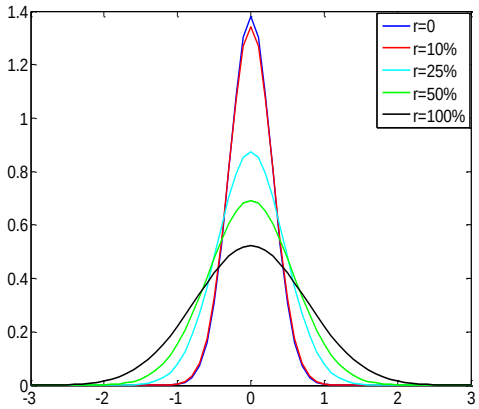


Fig. 5. Pdfs of variable θ at different embedding rates

Table 1. Definite integrals of variable θ at different embedding rates

r	$\int_{-2}^{2} p_\theta(y)dy$
0	1.0000
0.1	1.0000
0.25	1.0000
0.5	0.9995
1	0.9911

From **Table 1**, we have:

$$\int_{-2}^{2} p_\theta(y)dy \ge 99.11\%. \quad (5)$$

Let p_S and $p_{\tilde{d}}$ be the pdfs of d_S and $\tilde{d}$, respectively. Combining (1)-(5), we obtain the relationship between $p_{\tilde{d}}$ and p_S as follows:

$$\int_{kq-2}^{kq+2} p_S(y)dy \approx p_{\tilde{d}}(kq), k \in \square, q \ge 4. \quad (6)$$

Where q is quantization step ($q = Q_{i,j}$). So we consider the percentage of the ac coefficients of

a given test image in the following two specific regions, that is:

$$R_1 = (-2,+2) \ \ \& \ \ R_2 = (-3,-2] \cup [+2,+3).$$

The relationship between the dequantized coefficient $\tilde{d}$ and the ac coefficient d in the natural image in previous JPEG compression is as follows:

$$p_{\tilde{d}}(x) = \begin{cases} \int_{kq+\frac{q}{2}}^{kq-\frac{q}{2}} p_d(y)\,dy, & x = kq, k \in \mathbb{Z} \\ 0, & \text{otherwise.} \end{cases} \tag{7}$$

Where p_d is the pdf of the ac coefficient d. Based on (6) and (7), we have:

$$\int_{R_1} p_S(y)\,dy = \int_{-2}^{2} p_S(y)\,dy \approx p_{\tilde{d}}(0) = \int_{-\frac{q}{2}}^{\frac{q}{2}} p_d(y)\,dy \geq \int_{-2}^{2} p_d(y)\,dy = \int_{R_1} p_d(y)\,dy, \quad q \geq 4 \tag{8}$$

$$\int_{R_2} p_S(y)\,dy = \int_{-3}^{-2} p_S(y)\,dy + \int_{+2}^{+3} p_S(y)\,dy \approx 0 + 0 \leq \int_{R_2} p_d(y)\,dy, \quad q \geq 4 \tag{9}$$

Therefore, an improved 1-D feature s can be obtained as

$$s = \frac{\int_{R_2} p_{ac}(y)\,dy}{\int_{R_1} p_{ac}(y)\,dy} \qquad R_1 = (-2,+2) \ \ \& \ \ R_2 = (-3,-2] \cup [+2,+3) \tag{10}$$

Where p_{ac} denotes the pdf of all the ac coefficients of the test image regardless of its type (i.e., cover or stego). It is obvious that the feature value of a JPEG decompressed image(cover or stego) is close to zero, which is much smaller than that of an uncompressed image.

2.1.2 Detecting Quantization Table

In this subsection, we are going to estimate the quantization table of a JPEG decompressed image with an unknown embedding rate ranging from 0 to 1. Here, we assume that quantization tables are standard tables with quality factors from 1 to 100.

We define a similar measure R between two images I_1 and I_2 with the same size of $M \times N$ as follows:

$$R(I_1, I_2) = \frac{|E|}{MN}, \ E = \{(x,y) | I_1(x,y) = I_2(x,y), 1 \leq x \leq M, 1 \leq y \leq N\} \tag{11}$$

So for a given decompressed image J_1 (cover or stego), we first recompress it with all candidate tables, i.e., quality factors ranging from 1 to 100, and obtain the corresponding decompressed images $J_2(i)$. Then the detected quality factor $\hat{QF}$ of a decompressed image J_1 regardless of cover and stego can be defined as:

$$\hat{QF} = \arg\max_i \left(Q(J_1, J_2(i))\right). \tag{12}$$

Where $Q(J_1, J_2(i)) = \left\{ R(J_1, J_2(i)) \middle| \begin{matrix} \left(R(J_1, J_2(i)) - R(J_1, J_2(i-1))\right) \geq 0; \\ \left(R(J_1, J_2(i)) - R(J_1, J_2(i+1))\right) \geq 0. \end{matrix} \right\} (i = 1,2,...,100)$

Fig. 6 shows the similar measure R as a function of quality factors for JPEG decompressed images with embedding rates 25% and 50%. It is observed that the position at which the maximum value of the peak values appears is the corresponding quality factor.

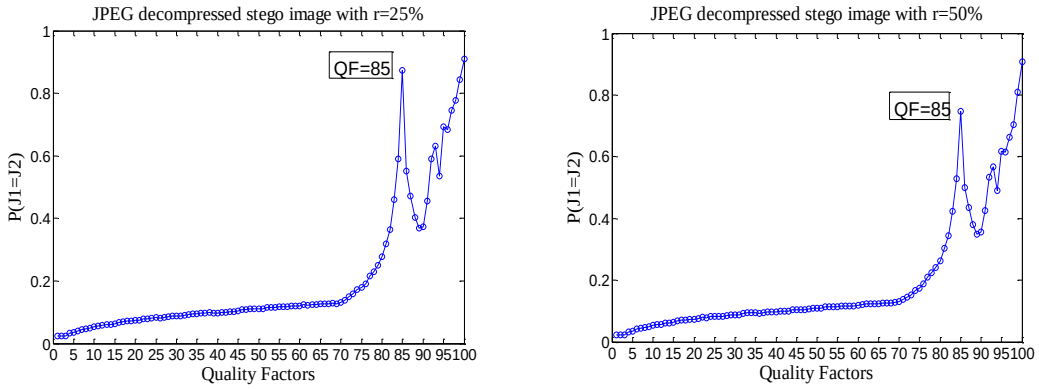


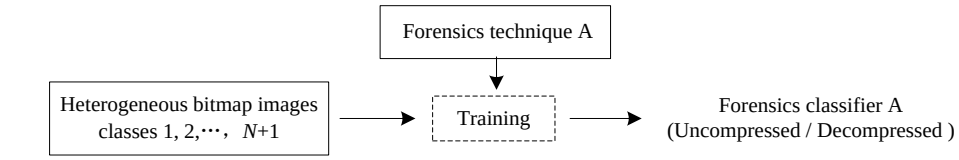
Fig. 6. Percentages of the pixel values as functions of quality factors for JPEG decompressed images with the quality factor 85

2.2 Forensics-aided Steganalysis

2.2.1 Structure of Proposed FA-steganalyzer

In this part, combining the image forensics techniques presented in section 2.1, two practical FA-steganalyzers for heterogeneous bitmap images are constructed, which can properly handle steganalysis problems for mixed image sources consisting of raw uncompressed images and JPEG decompressed images with different quality factors.

The overall architectures of the proposed two FA-steganalyzers called S1 and S2 are depicted in **Figs. 7** and **8**. As for the first FA-steganalyzer scheme, in the training phase, two versions of the same or different steganalyzers trained on images belonging to raw uncompressed images and mixed JPEG decompressed images with different quality factors are built (**Fig. 7(b)**). Let us call the two steganglyzers SA_1, SA_2. At the same time, a JPEG decompressed image identifier i.e., the forensics classifier A is trained to distinguish between images belonging to the two classes (**Fig. 7(a)**). In the testing phase, we first use a JPEG decompressed image identifier to classify the image at hand as one of the two classes, and then use the version of the steganalyzer that was trained on the correct class of images (**Fig. 8**). For the second FA-steganalyzer scheme, in the training phase, different from the first FA-steganalyzer, N versions of the same or different steganalyzers trained on JPEG decompressed images with corresponding quality factors are established (**Fig. 7(c)**). Let us call such steganalyzers $SB_1, SB_2, ..., SB_N$. In the testing phase, we further estimate quality factors of JPEG decompressed images, and then send the images to the steganalyzers that were trained on the corresponding quality factors (**Fig. 8**).



(a) Forensics classifier A

(b) Steganalyzers for uncompressed / JPEG decompressed images

(c) Steganalyzers for JPEG decompressed images with N kinds of different quality factors

Fig. 7. Structures of the two FA-steganalyzers: training phase

As for the first FA-steganalyzer S1, the key steps of the core training algorithm are summarized as follows:

Step 1: for heterogeneous bitmap images in the training set, extract improved features s according to equation (10), and then train the forensics classifier A using the features s above;

Step 2: for uncompressed images in the training set, extract certain steganalytic features (such as WAM, LLTCF, LLTPDF and RDIH in section 3.1), and then train the steganalyzer SA_1 using the steganalytic features above;

Step 3: for mixed JPEG decompressed images with N kinds of different quality factors in the training set, extract certain steganalytic features (such as WAM, LLTCF, LLTPDF, RDIH, 1D and CAM), and then train the steganalyzer SA_2 using the steganalytic features above;

As for the second FA-steganalyzer S2, the first two steps are identical with those of the first FA-steganalyzer S1, while the following steps are listed as follows:

Step 3: for JPEG decompressed images with a specified quality factor Q_j ($j=1,2,...,N$) in the training set, extract certain steganalytic features (such as WAM, LLTCF, LLTPDF, RDIH, 1D and CAM in section 3.1), and train the steganalyzers $SB_1, SB_2, ..., SB_N$, respectively.

It should be noted that the steganalytic feature for uncompressed images and that for JPEG decompressed images could be same or different. Morover,the training processes of forensics classifier A and various steganalyzers $SA_1, SA_2, SB_1, SB_2, ..., SB_N$ are independent mutually.

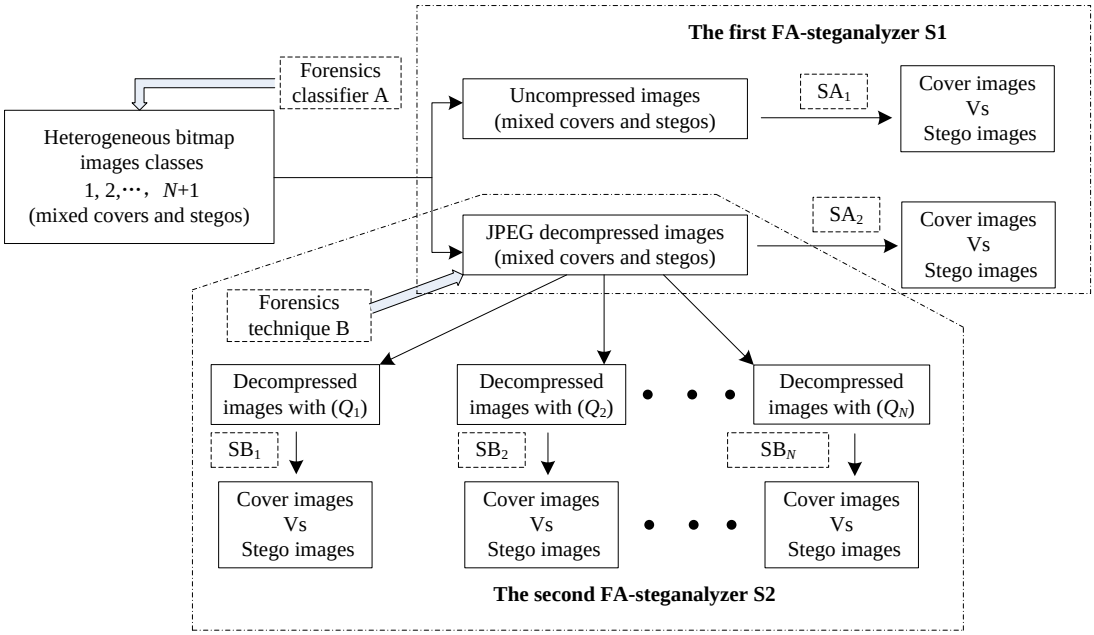


Fig. 8. Structures of the two FA-steganalyzers: testing phase

2.2.2 Error Probability of Proposed FA-steganalyzer

The performances of the two FA-steganalyzers depend on several factors, including the error probability of the forensics classifier A, the error probabilities of the various steganalyzers when applied to images belonging to the various classes, and the error probability of the quantization table detector. To elaborate let P_e^{S1} and P_e^{S2} be the overall error probabilities of the two FA-steganalyzers. Let $P(I_i)$ be the prior probability of the i-th class image ($i=1,2,...,N+1$). Where $I_1, I_2, ..., I_N$ stand for JPEG decompressed images with N kinds of different quality factors, while I_{N+1} stands for the uncompressed image. Let then $P^{C_A}(C_k|i)$ ($k=1,2$) be the probability that a JPEG decompressed image identifier classifies an image coming from I_i as the uncompressed image (denoted by C_1) or the JPEG decompressed image (denoted by C_2). $P_e^{SA_k}(i)$ or $P_e^{SB_j}(i)$ is the probability that the steganalyzer SA_k or SB_j makes an error when asked to classify an image belonging to I_i. Finally, $P^{C_B}(Q_j|i)$ is the probability that the quantization table detector detects the quality factor of an image belonging to I_i as Q_j $(j=1,2,...,N)$.

The overall error probabilities of two FA-steganalyzers are derived in the following forms:

$$P_e^{S1} = \sum_{i=1}^{N+1}\sum_{k=1}^{2} P_e^{SA_k}(i) P^{C_A}(C_k|i) P(I_i) \tag{13}$$

$$P_e^{S2} = \sum_{i=1}^{N+1} P_e^{SA_1}(i) P^{C_A}(C_1|i) P(I_i) + \sum_{i=1}^{N+1}\sum_{j=1}^{N} P_e^{SB_j}(i) P^{C_B}(Q_j|i) P^{C_A}(C_2|i) P(I_i) \tag{14}$$

If the forensics classifier A in charge of identifying JPEG decompressed images is balanced, i.e. it has the same error probability regardless of the class the image belongs to, and then we assume that the prior probabilities of the $N+1$ classes are equal, we have:

$$P^{C_A}(C_2|N+1) = P^{C_A}(C_1|1,2,...,N) = \frac{1}{N}\sum_{i=1}^{N} P^{C_A}(C_1|i) \tag{15}$$

The correct probabilities of the forensics classifier A are also same, namely,

$$P^{C_A}(C_1|N+1) = P^{C_A}(C_2|1,2,...,N) = \frac{1}{N}\sum_{i=1}^{N} P^{C_A}(C_2|i) \tag{16}$$

Take P_e^{S1} for example, and based on (15) and (16), we have:

$$\begin{aligned}
P_e^{S1} &= \sum_{i=1}^{N+1}\sum_{k=1}^{2} P_e^{SA_k}(i) P^{C_A}(C_k|i) P(I_i) \\
&= \frac{1}{N+1}\left(\sum_{k=1}^{2} P_e^{SA_k}(N+1) P^{C_A}(C_k|N+1) + \sum_{i=1}^{N}\sum_{k=1}^{2} P_e^{SA_k}(i) P^{C_A}(C_k|i) \right) \\
&= \frac{1}{N+1}\left(P_e^{SA_2}(N+1) P^{C_A}(C_2|N+1) + P_e^{SA_1}(N+1) P^{C_A}(C_1|N+1) + \sum_{i=1}^{N}\sum_{k=1}^{2} P_e^{SA_k}(i) P^{C_A}(C_k|i) \right) \\
&= \frac{1}{N(N+1)}\left(P_e^{SA_2}(N+1)\sum_{i=1}^{N} P^{C_A}(C_1|i) + P_e^{SA_1}(N+1)\sum_{i=1}^{N} P^{C_A}(C_2|i) \right) + \frac{1}{N+1}\sum_{i=1}^{N}\sum_{k=1}^{2} P_e^{SA_k}(i) P^{C_A}(C_k|i) \\
&= \sum_{i=1}^{N} P^{C_A}(C_2|i)\left(\frac{1}{N(N+1)} P_e^{SA_1}(N+1) + \frac{1}{N+1} P_e^{SA_2}(i) \right) + \sum_{i=1}^{N} P^{C_A}(C_1|i)\left(\frac{1}{N(N+1)} P_e^{SA_2}(N+1) + \frac{1}{N+1} P_e^{SA_1}(i) \right)
\end{aligned} \tag{17}$$

Where $P^{C_A}(C_2|i)$ and $P^{C_A}(C_1|i)$ indicate the probabilities that the forensics classifier A makes a correct and a wrong decision for JPEG decompressed images, respectively. Since we assume that $P_e^{SA_1}(N+1) < P_e^{SA_2}(N+1)$ and $P_e^{SA_2}(i) < P_e^{SA_1}(i)(i=1,2,...,N)$, it is evident that the higher the error rate of the forensics classifier A the worse the performance of the first FA-steganalyzer. We expect that the observation obtained above can also be applied to the second FA-steganalyzer. Additionally, it is expected the second FA-steganalyzer S2 has a superior detection performance in comparison with the first steganalyzer S1, since the match between the training set and the testing set is much more exact.

3. Experimental Results

3.1 Experimental Setup

In our experiment, we first give some basic assumptions which are reasonable in practical applications in order to simplify the construction of FA-steganalyzers. The first assumption concerns the source of cover images. We assume cover images have been preclassified by a source identification forensics tool before, and since most of images are acquired by digital cameras, the cover images under investigation were taken from several common cameras like Canon, Nikon, Sony and so on. The second assumption concerns the selection of quality factors. We assume that quantization tables are standard tables with quality factors from 50 to 95 at intervals of five as widely used in many other steganalysis and forensics works.

Based on the assumptions above, the CAMERA [10] database is used as the image source in our experiment and 1600 images are randomly selected from it. Please note that in the beginning, the images are divided into a training set containing 600 raw bitmap images and a testing set containing 1000 raw bitmap images. Moreover, half of the training set is used to train the forensics classifier A, while the remaining is used to train each homogeneous steganalyzer. The following image processing operations are performed on the training set and the testing set in exactly the same way.

These original color images are first center-cropped into 256×256 pixels, and then converted into gray scales. Next, the JPEG compression is applied to them with quality factors from 50 to 95 at intervals of five. Finally we get the final JPEG decompressed images after decompression.

The cover database contains both uncompressed bitmap images and corresponding JPEG decompressed bitmap images with ten kinds of different quality factors. Then we perform LSB matching steganography with embedding rate 10%, 25%, 50% and 100% on the cover database to obtain the stego database.

We use a classifier based on Fisher Linear discriminant to train and test. The total number of images in the training set is (600+600×10)×(4+1)=33000, while the total number of images in the testing set is (1000+1000×10)×(4+1)=55000.

For our experiments, two targeted steganalyzers (named LLTCF [11] and RDIH [12]) for LSB matching steganography, one targeted steganalyzer (named CAM [13]) designed for LSB matching steganography in JPEG decompressed images, one blind steganalyzer (named 1D [14]) for additive noise steganography in JPEG decompressed images and two blind steganalyzers (named WAM [15] and LLTPDF [16]) are taken into consideration.

(1) LLTCF: local linear transform and weighted features of characteristic functions;
(2) RDIH: the peak-value and renormalized histogram of difference images;
(3) 1D: the area ratio between different ranges of normalized ac coefficients histogram;
(4) CAM: the first 10 order central absolute moments of noise residuals in DCT domain of

JPEG decompressed images;

(5) WAM: the higher-order absolute moments of the noise residual in the wavelet domain;

(6) LLTPDF: normalized histogram of the local linear transform coefficients of the image.

3.2 Image Forensics Analysis

3.2.1 Identifying JPEG Decompressed Images

According to (10), we calculate the features s for the original uncompressed images and their different JPEG compressed versions and show the corresponding histograms in **Figs. 9** and **10**. **Fig. 9** shows the histograms among mixed covers and stegos at embedding rates 25% and 100% between uncompressed images and JPEG decompressed images with quality factors 90 and 95. We can note that even for 100% embedding the features are also mostly disjoint. To further show the effectiveness of the improved feature, we randomly select the quality factors in the range of 50-95. The histograms of the features at different embedding rates 10%, 25%, 50% and 100% are presented in **Fig. 10**, which indicates our improved feature is less sensitive to the embedding message even for 100% embedding,while the feature proposed in [8] is easy to influnced by the embedding message(see **Fig. 3**). So our improved feature could obtain good results in mixed covers and stegos.

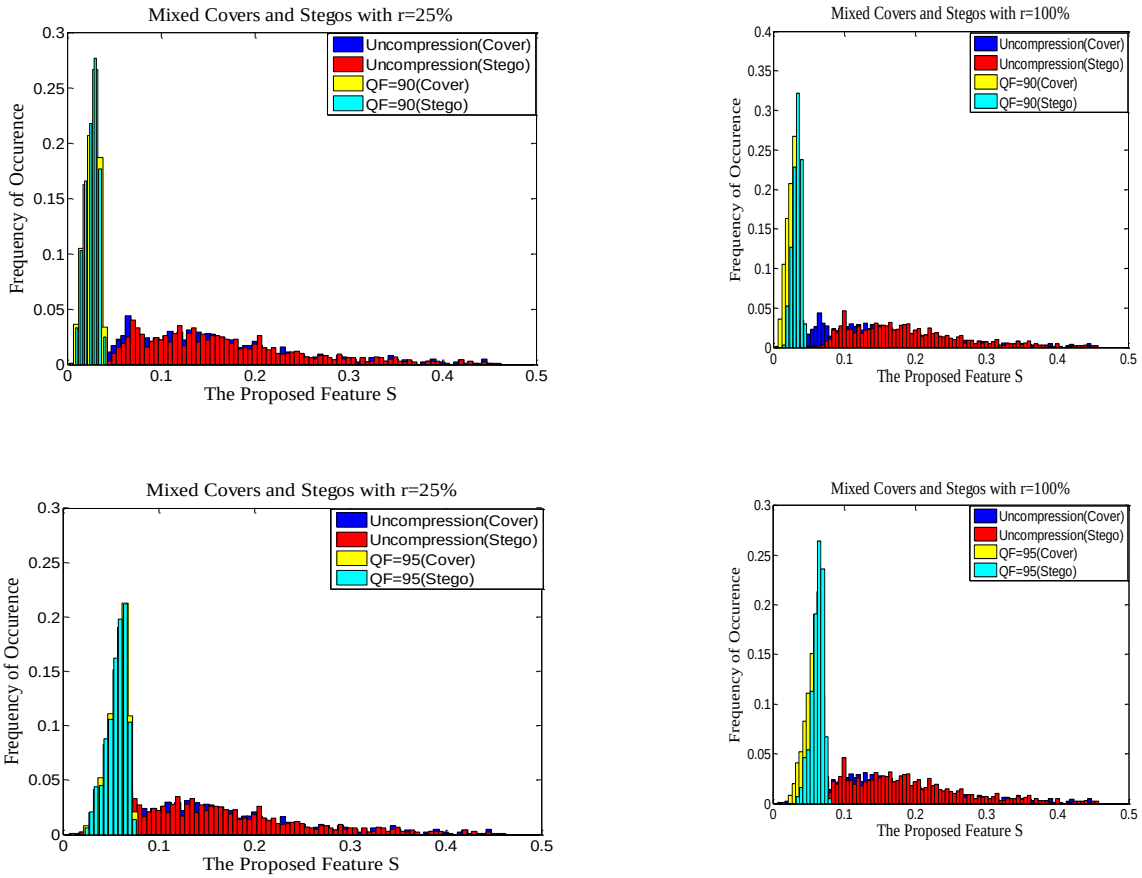


Fig. 9. Histograms of the features s for mixed uncompressed cover, stego images and corresponding JPEG decompressed ones with QFs=90 and 95 at different embedding rates 25% and 100%

To properly test the improved feature s, we first use a minimal error probability rule to find a threshold t. For a given embedding rate in the training stage, half of the uncompressed images (covers and stegos) and the corresponding JPEG decompressed images (covers and stegos) with QF=95, the highest quality factor the proposed feature can detect reliably, are employed to obtain a proper threshold. These thresholds are then used to detect the rest of the JPEG decompressed images with QF=95, and all the other JPEG decompressed images with QFs from 50 to 90 at intervals of five. The experimental results are shown in **Table 2**. Here we define p_{Tp} as the probability of JPEG decompressed images being correctly determined as JPEG decompressed images while p_{Fp} is the probability of uncompressed images being wrongly determined as JPEG decompressed images and p_{Fn} is the probability of JPEG decompressed images being wrongly determined as uncompressed images. From **Table 2**, we can observe that our improved method can achieve satisfactory accuracy of around 98% even with the embedding rate 100%. It can be expected that the good performance of the forensics classifier A will be beneficial to the following steganalysis.

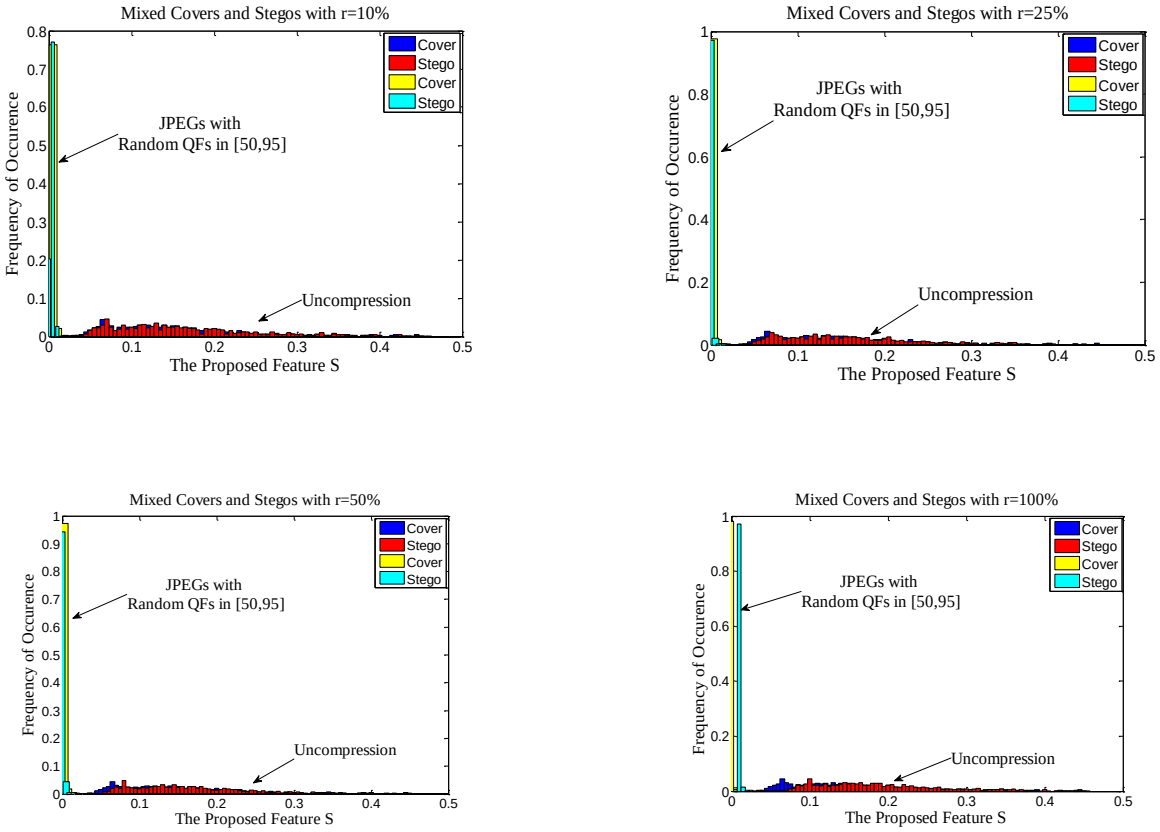


Fig. 10. Histograms of the features s for mixed uncompressed cover, stego images and corresponding JPEG decompressed ones with QFs randomly selected in [50,95] at different embedding rates 10%, 25%, 50% and 100%

Table 2. p_{Tp} (%) for JPEG decompressed image identification between mixed covers and stegos. The thresholds are **0.0742, 0.0730, 0.0737** and **0.0777** for different embedding rates, and the p_{Fp} (%) we obtained are **16.79, 14.75, 12.47** and **10.38**

Embedding Rate	Quality Factor									
	50	***55***	***60***	***65***	***70***	***75***	***80***	***85***	***90***	***95***
10%	100	100	100	100	100	100	100	100	100	98.73
25%	100	100	100	100	100	100	100	100	100	98.49
50%	100	100	100	100	100	100	100	100	100	99.07
100%	100	100	100	100	100	100	100	100	100	99.58

3.2.2 Detecting Quantization Table

In our experiment, for a given JPEG decompressed image (cover and stego), we recompress it with all the candidate tables and obtain the corresponding recompressed versions in the spatial domain, and thus (12) is employed for the quality factor estimation. To show the effectiveness of our improved method, we compare our improved method with [17] proposed by Luo et al. and present the experimental results in **Table 3**.

Table 3. Accuracies (%) for quantization table detection for decompressed images with different quantization tables and embedding rates using the two methods

Embedding Rate	Detection Method	Quality Factor									
		50	***55***	***60***	***65***	***70***	***75***	***80***	***85***	***90***	***95***
Cover	Luo [17]	14.2	89.6	72.7	93.1	87.5	32.8	91.6	78.5	98.7	97.4
	Proposed	**83.3**	**100**	**99.7**	**100**	**100**	**93.1**	**100**	**100**	**100**	**100**
10%	Luo [17]	68.2	95.1	93.5	96	96.2	83.1	98.1	99.2	100	100
	Proposed	**82.9**	**100**	**99.7**	**100**	**100**	**93.1**	**100**	**100**	**100**	**100**
25%	Luo [17]	73.2	96	95.8	97.3	97.5	86.9	98.7	99.6	100	100
	Proposed	**82.9**	**99.7**	**99.7**	**100**	**99.7**	**93**	**100**	**100**	**100**	**100**
50%	Luo [17]	78.3	98	97.5	98.2	98.6	89.3	99.5	99.7	99.8	**99.9**
	Proposed	**82.7**	**99.7**	**99.7**	**100**	**99.6**	**93**	**100**	**100**	**100**	96
100%	Luo [17]	**81.5**	99.5	99.2	99.5	99.5	91.3	99.7	99.6	55.8	**99.9**
	Proposed	81.2	**99.8**	**99.4**	**99.9**	**99.7**	**92.4**	**99.8**	**99.8**	**80**	58.7

From **Table 3**, it is obvious that our improved method outperforms the existing method [17] significantly in most cases. The highest accuracy for a given quality factor is in boldface. Please note that the accuracy is relatively lower for detecting the JPEG decompressed images with QFs=50 and 75. The reason is that the first 19 quantization steps (along the zigzag scanning order) in the quantization tables with quality factors 49, 50, and 51 are exactly the same. As for JPEG decompressed images with QF=75, according to experimental results we find JPEG decompressed images with QF=75 are wrongly detected as QF=73 or 74. So it does not much influence the performance of steganalysis. and thus the error of detecting quantization table can be neglected. So in this paper we only focus on the error of identifying JPEG decompressed images in the part of image forensics analysis.

3.3 Forensics-aided Steganalysis

In our experiment, our proposed FA-steganalyzers will be compared to the existing steganalyzer that is trained on a mixed dataset (noted by a mixed steganalyzer) (**Fig. 11**).

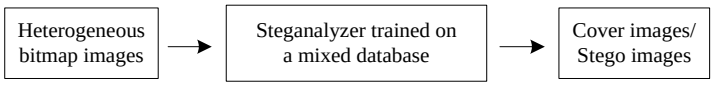


Fig. 11. Structure of a mixed steganalyzer

To evaluate the performances of the proposed two FA-steganalyzers, it is necessary to set the decision thresholds of the corresponding classifiers including the forensics classifier A and various steganalyzers. Then, the various error probabilities and overall error probabilities will be obtained within the equations (13) and (14). Take $P_{\mathrm{e}}^{\mathrm{S1}}$ for example, firstly, let $A_{i,k}$ be the number that a JPEG decompressed image identifier assigns cover images coming from I_i to SA_k, while $B_{i,k}$ stands for the number that a JPEG decompressed image identifier assigns stego images coming from I_i to SA_k. Then, $H_{i,k}$ indicates the number that the steganalyzer SA_k makes an error when asked to classify cover images belonging to I_i, while $L_{i,k}$ is the number that the steganalyzer SA_k makes an error when asked to classify stego images belonging to I_i. Finally, M is the number of cover images or stego images belonging to I_i ($1 \le i \le N+1$, $k = 1,2$), and thus we have,

$$
\begin{aligned}
P_{\mathrm{e}}^{\mathrm{S1}} &= \sum_{i=1}^{N+1}\sum_{k=1}^{2} P_{\mathrm{e}}^{\mathrm{SA}_k}(i) P^{\mathrm{C_A}}(C_k|i) P(I_i) \\
&= \frac{1}{N+1}\left(P_{\mathrm{e}}^{\mathrm{SA}_1}(N+1) P^{\mathrm{C_A}}(C_1|N+1) + P_{\mathrm{e}}^{\mathrm{SA}_2}(N+1) P^{\mathrm{C_A}}(C_2|N+1) + \sum_{i=1}^{N} P_{\mathrm{e}}^{\mathrm{SA}_1}(i) P^{\mathrm{C_A}}(C_1|i) + \sum_{i=1}^{N} P_{\mathrm{e}}^{\mathrm{SA}_2}(i) P^{\mathrm{C_A}}(C_2|i) \right) \\
&= \frac{1}{N+1}\left(\frac{H_{N+1,1}+L_{N+1,1}}{A_{N+1,1}+B_{N+1,1}} \frac{A_{N+1,1}+B_{N+1,1}}{2M} + \frac{H_{N+1,2}+L_{N+1,2}}{A_{N+1,2}+B_{N+1,2}} \frac{A_{N+1,2}+B_{N+1,2}}{2M} + \sum_{i=1}^{N}\left(\frac{H_{i,1}+L_{i,1}}{A_{i,1}+B_{i,1}} \frac{A_{i,1}+B_{i,1}}{2M} \right) + \sum_{i=1}^{N}\left(\frac{H_{i,2}+L_{i,2}}{A_{i,2}+B_{i,2}} \frac{A_{i,2}+B_{i,2}}{2M} \right) \right) \\
&= \frac{1}{2M(N+1)}\left(H_{N+1,1}+L_{N+1,1}+\sum_{i=1}^{N}\left(H_{i,1}+L_{i,1}\right) \right) + \frac{1}{2M(N+1)}\left(H_{N+1,2}+L_{N+1,2}+\sum_{i=1}^{N}\left(H_{i,2}+L_{i,2}\right) \right) \\
&= \frac{A_{N+1,1}+B_{N+1,1}+\sum_{i=1}^{N}\left(A_{i,1}+B_{i,1}\right)}{2M(N+1)} \left(\frac{A_{N+1,1}+\sum_{i=1}^{N}A_{i,1}}{A_{N+1,1}+B_{N+1,1}+\sum_{i=1}^{N}\left(A_{i,1}+B_{i,1}\right)} \frac{H_{N+1,1}+\sum_{i=1}^{N}H_{i,1}}{A_{N+1,1}+\sum_{i=1}^{N}A_{i,1}} + \frac{B_{N+1,1}+\sum_{i=1}^{N}B_{i,1}}{A_{N+1,1}+B_{N+1,1}+\sum_{i=1}^{N}\left(A_{i,1}+B_{i,1}\right)} \frac{L_{N+1,1}+\sum_{i=1}^{N}L_{i,1}}{B_{N+1,1}+\sum_{i=1}^{N}B_{i,1}} \right) \\
&+ \frac{A_{N+1,2}+B_{N+1,2}+\sum_{i=1}^{N}\left(A_{i,2}+B_{i,2}\right)}{2M(N+1)} \left(\frac{A_{N+1,2}+\sum_{i=1}^{N}A_{i,2}}{A_{N+1,2}+B_{N+1,2}+\sum_{i=1}^{N}\left(A_{i,2}+B_{i,2}\right)} \frac{H_{N+1,2}+\sum_{i=1}^{N}H_{i,2}}{A_{N+1,2}+\sum_{i=1}^{N}A_{i,2}} + \frac{B_{N+1,2}+\sum_{i=1}^{N}B_{i,2}}{A_{N+1,2}+B_{N+1,2}+\sum_{i=1}^{N}\left(A_{i,2}+B_{i,2}\right)} \frac{L_{N+1,2}+\sum_{i=1}^{N}L_{i,2}}{B_{N+1,2}+\sum_{i=1}^{N}B_{i,2}} \right) \\
&= \mu_1\left(\alpha_1 P_{\mathrm{Fp}}^{1} + \beta_1 P_{\mathrm{Fn}}^{1}\right) + \mu_2\left(\alpha_2 P_{\mathrm{Fp}}^{2} + \beta_2 P_{\mathrm{Fn}}^{2}\right) = \sum_{k=1}^{2}\mu_k\left(\alpha_k P_{\mathrm{Fp}}^{k} + \beta_k P_{\mathrm{Fn}}^{k}\right)
\end{aligned}
\tag{18}
$$

Where μ_k is the proportion of the total number of testing set on the steganalyzer SA_k to entire testing set, while α_k and β_k represent the ratios of cover and stego images on the steganalyzer SA_k. P_{Fp}^{k} and P_{Fn}^{k} stand for the probability of false positive (detecting cover as stego) and

probability of missed detection (false negative) on the steganalyzer SA_k .

But please note that all the combinations of decision thresholds within the considered interval will tend to be too broad, thereby resulting in great complexity and large storage. So in this paper, we first set the decision threshold of the forensics classifier A, and then μ_1, μ_2 will be obtained, and based on (18) we have,

$$P_{\mathrm{Err}} = \min(P_{\mathrm{e}}^{\mathrm{S1}}) = \mu_1 \min\left(\alpha_1 P_{\mathrm{Fp}}^1 + \beta_1 P_{\mathrm{Fn}}^1\right) + \mu_2 \min\left(\alpha_2 P_{\mathrm{Fp}}^2 + \beta_2 P_{\mathrm{Fn}}^2\right) = \mu_1 P_{\mathrm{Err}}^1 + \mu_2 P_{\mathrm{Err}}^2 = \sum_{k=1}^{2} \mu_k P_{\mathrm{Err}}^k \quad (19)$$

Where P_{Err}^k is the minimal average decision error of the steganalyzer SA_k .

We expect that the derivation process above can also be applied to the second FA-steganalyzer. So the entire minimal average decision error of the FA-steganalyzer can be calculated in the following expressions under the assumption that N is 10 in section 3.1:

$$P_{\mathrm{Err}} = \min\left(P_{\mathrm{e}}^{\mathrm{Sx}}\right) = \sum_{i=1}^{M_x} \mu_i P_{\mathrm{Err}}^i, \quad M_x = \begin{cases} 2, & x{=}1 \\ N+1=11, & x{=}2 \end{cases}, \quad P_{\mathrm{Err}}^i = \min\left(\alpha_i P_{\mathrm{Fp}}^i + \beta_i P_{\mathrm{Fn}}^i\right) \quad (20)$$

Where M_x is the total number of steganalyzers, μ_i is the proportion of the total number of testing set which has been preclassified on the i-th homogeneous steganalyzer to entire testing set, and P_{Err}^i is the minimal average decision error of the i-th homogeneous steganalyzer. In addition, P_{Fp}^i and P_{Fn}^i stand for the probability of false positive and probability of false negative on the i-th homogeneous steganalyzer while α_i and β_i represent the ratios of cover and stego images on the i-th homogeneous steganalyzer.

The minimal average decision error of a mixed steganalyzer noted by S3 will be calculated in the following equation under equal probability of cover and stego images:

$$P_{\mathrm{Err}} = \frac{1}{2}\min\left(P_{\mathrm{Fp}} + P_{\mathrm{Fn}}\right) \quad (21)$$

As is known to all, a mismatch between the statistics of the training set and those of the testing set can significantly decrease the performance of a steganalyzer, so how to set the decision threshold of the forensics classifier A to balance each homogeneous steganalyzer and further to get the best overall detection performance is a key issue. We adopt an experimental procedure to explore this issue by designing the following three setups L1, L2 and L3.

(a) L1: providing the forensics classifier A makes a fully correct classification;

(b) L2: using a minimal error probability rule ($P\_\mathrm{Err} = p(C_{\mathrm{uncom}})\,p_{\mathrm{Fp}} + p(C_{\mathrm{decom}})\,p_{\mathrm{Fn}}$) to find a threshold t in the training stage;

(c) L3: using almost equal error ($p_{\mathrm{Fp}} \approx p_{\mathrm{Fn}}$) rule to find a threshold t in the training stage, where $p(C_{\mathrm{uncom}})$, $p(C_{\mathrm{decom}})$ are the prior probabilities of the two classes.

According to three setups L1, L2, L3 above, we can obtain corresponding decision thresholds for different embedding rates respectively, which are then used to preclassify the images of testing set .After that, α_i , β_i , P_{Fp}^i , P_{Fn}^i , μ_i will be computed, which are used within the equation (20) to obtain the overall minimal average decision errors P_{Err} of the two FA-steganalyzers. The experimental results are shown in **Table 4**, **5** and **6**. Please note that the

best detection accuracies for different embedding rates are in boldface.

Table 4. Minimal average decision errors (%) of two FA-steganalyzers (**S1 and S2**) equipped with an error-free forensics classifier A (**L1**) and a mixed steganalyzer (**S3**) at four different embedding rates for different steganalyzers

Embedding Rate		Steganalyzer					
		WAM	***LLTCF***	***LLTPDF***	***RDIH***	***LLTCF +1D***	***LLTCF +CAM***
10%	S2	14.428	**3.212**	3.571	10.166	4.532	**3.702**
	S1	18.122	**3.751**	5.032	14.083	8.026	**4.626**
	S3	22.227	9.882	9.458	17.372		
25%	S2	7.709	**0.846**	1.473	4.422	**0.487**	0.501
	S1	10.019	**1.035**	2.347	6.198	3.669	**0.549**
	S3	12.193	3.175	4.655	8.500		
50%	S2	5.531	**0.273**	0.846	2.207	0.151	**0.141**
	S1	7.167	**0.388**	1.386	3.235	0.161	**0.138**
	S3	8.971	0.973	2.694	3.981		
100%	S2	4.176	**0.090**	0.498	1.381	**0.028**	0.034
	S1	4.755	**0.150**	0.735	1.654	**0.030**	0.033
	S3	6.187	0.355	1.638	1.819		

Table 5(a). p_{Tp}, p_{Fp}, P_Err (%) for JPEG decompressed image identification between mixed covers and stegos .The thresholds are **0.0746, 0.0731, 0.0733** and **0.0775** for different embedding rates according to minimal error probability rule (**L2**) in the training phase

Embedding Rate	p_{Tp} (%)	p_{Fp} (%)	P_Err (%)
10%	99.950	16.850	1.577
25%	99.865	14.650	1.454
50%	99.890	12.100	1.200
100%	99.975	10.500	0.977

Table 5(b). Minimal average decision errors (%) of two FA-steganalyzers (**S1 and S2**) and a mixed steganalyzer (**S3**) at four different embedding rates for different steganalyzers

Embedding Rate		Steganalyzer					
		WAM	***LLTCF***	***LLTPDF***	***RDIH***	***LLTCF +1D***	***LLTCF +CAM***
10%	S2	14.849	**3.841**	4.178	10.792	5.211	**4.394**
	S1	18.636	**4.436**	5.706	14.638	8.731	**5.282**
	S3	22.227	9.882	9.458	17.372		
25%	S2	8.275	**1.401**	1.843	5.077	**1.275**	1.291
	S1	10.627	**1.618**	2.840	6.929	4.414	**1.283**
	S3	12.193	3.175	4.655	8.500		
50%	S2	6.121	**0.371**	0.943	2.280	0.896	**0.668**
	S1	7.891	**0.461**	1.616	3.383	0.912	**0.859**
	S3	8.971	0.973	2.694	3.981		
100%	S2	4.830	**0.105**	0.541	1.385	**0.330**	0.503
	S1	5.488	**0.163**	0.758	1.689	0.793	**0.693**
	S3	6.187	0.355	1.638	1.819		

Table 6(a). p_{Tp}, p_{Fp}, p_{Fn}, P_Err (%) for JPEG decompressed image identification between mixed covers and stegos. The thresholds are **0.0568, 0.0586, 0.0596** and **0.0629** for different embedding rates according to equal error probability rule (**L3**) in the training phase

Embedding Rate	p_{Tp} (%)	p_{Fp} (%)	p_{Fn} (%)	P_Err (%)
10%	94.430	5.600	5.570	5.572
25%	95.050	5.350	4.950	4.981
50%	95.545	4.800	4.455	4.486
100%	95.605	4.900	4.395	4.440

Table 6(b). Minimal average decision errors (%) of two FA-steganalyzers (**S1 and S2**) and a mixed steganalyzer (**S3**) at four different embedding rates for different steganalyzers

Embedding Rate		Steganalyzer					
		WAM	***LLTCF***	***LLTPDF***	***RDIH***	***LLTCF +1D***	***LLTCF +CAM***
10%	S2	16.545	**5.923**	5.980	12.710	**6.134**	6.404
	S1	20.158	**6.410**	7.410	15.630	8.283	**7.317**
	S3	22.227	9.882	9.458	17.372		
25%	S2	9.987	**2.311**	3.168	6.355	**2.031**	2.152
	S1	12.169	**2.583**	4.285	8.023	3.196	**2.195**
	S3	12.193	3.175	4.655	8.500		
50%	S2	7.250	**0.378**	1.889	2.410	0.573	**0.438**
	S1	8.834	**0.474**	2.630	3.362	0.582	**0.548**
	S3	8.971	0.973	2.694	3.981		
100%	S2	5.538	**0.102**	0.837	1.412	**0.056**	0.175
	S1	5.980	**0.165**	1.063	1.727	0.349	**0.309**
	S3	6.187	0.355	1.638	1.819		

According to the experimental results, we can draw the following conclusions:

(1) With regard to the selection of decision thresholds of the forensics classifier A, from **Table 4**, **5** and **6**, we can observe that when the decision thresholds found using a minimal error probability rule in the training stage are employed to preclassify the testing set, the overall minimal average decision errors of the two FA-steganalyzers are mostly close to that under the assumption that the forensics classifier A makes a fully correct decision. It means that the set up L2 could provide a more reliable detection than L3.

(2) From **Table 5(b)**, we can conclude that the detection performances of our proposed FA-steganalyzers outperform significantly a mixed steganalyzer. Take WAM for example, when the embedding rate is 10%, the minimal average decision error of the second FA-steganalyzer S2 reduces by up to 7%. Furthermore, as already expected the detection power of the second FA-steganalyzer S2 is better than that of the first FA-steganalyzer S1 in most circumstances.

(3) In the last two columns of **Table 5(b)**, for uncompressed images, we adopt the targeted steganalyzer LLTCF because of its good performance across a wide variety of steganalyzers [11], while for the kind of JPEG decompressed images, we select the steganalyzers named by 1D and CAM. Experimental results show that the detection performance of LLTCF+1D or LLTCF+CAM is almost best among all the steganalyzers except for LLTCF in some cases, which demonstrates the validity of such combination i.e., easing the steganalysis of

heterogeneous images with different compression history.

In a word, the main contributions of this paper can be summarized as follows: (1) the forensics classifier A and quantization table detector can recognize the type of the testing image, thus ensuring a match between the statistics of the taining set and those of the testing set; (2) instead of trying to construct a steganlyzer capable of handling heterogeneous images, we only need to use steganalyzers specially designed for uncompressed images and JPEG decompressed images respectively.

4. Conclusions

In this paper, we devise two efficient forensics-aided steganalyzers to deal with the heterogeneous bitmap images including uncompressed bitmap images and decompressed bitmap ones with different quality factors. Moreover, we also explore image forensics techniques under the assumption that the images under investigation are mixed covers and stegos, and how to set the decision threshold of image forensics classfier to balance each homogeneous steganalyzer. Experimental results show that the detecting performances of the two FA-steganalyzers are relatively best when we use a minimal error probability rule to find a threshold in the training stage and our proposed two forensics-aided steganalyzers outperform a mixed steganalyzer; Finally, it should be noted that selecting the best steganalysis algorithm for the particular cover class can achieve much more reliable detection than employing the same steganalysis algorithm in spite of the type of cover source preconditioned by good performance of image forensics classifier. The development of FA-steganalyzers capable of handling more complex heterogeneous images is our future research direction.

References

[1] J. Fridrich, M. Goljan and D. Hogea, "Steganalysis of JPEG images: Breaking the F5 algorithm," in *Proc. of 5th International Workshop on Information Hiding*, pp. 310-323, Oct. 2002. Article (CrossRef Link).

[2] G. Cancelli, G. Doerr, I. Cox and M. Barni, "A comparative study of ±1 steganalyzers," in *Proc. of IEEE International Workshop on Multimedia Signal Processing*, pp. 791-796, Oct. 2008. Article (CrossRef Link).

[3] T. Pevný, P. Bas and J. Fridrich, "Steganalysis by subtractive pixel adjacency matrix," *IEEE Transaction on Information Forensics and Security*, vol. 5, no. 2, pp. 215-224, Mar. 2010. Article (CrossRef Link).

[4] T. Pevný and J. Fridrich, "Determining the stego algorithm for JPEG images," *Special Issue of IEE Processing Information Security*, vol. 153, no. 3, pp. 77-86, Sep. 2006.

[5] T. Pevný and J. Fridrich, "Multiclass detector of current steganographic methods for JPEG format," *IEEE Transaction on Information Forensics and Security*, vol. 3, no. 4, pp. 635-650, Dec. 2008. Article (CrossRef Link).

[6] M. Barni, G. Cancelli and A. Esposito, "Forensics aided steganalysis of heterogeneous images," in *Proc. of IEEE Conf. on Acoustic Speech, Signal Processing*, pp. 1690-1693, Mar. 2010. Article (CrossRef Link).

[7] H. Amirkhani and M. Rahmati, "New framework for using image contents in blind steganalysis systems," *Journal of Electronic Imaging*, vol. 20, no. 1, pp. 1-14, Mar. 2011. Article (CrossRef Link).

[8] W. Luo, F. Huang and J. Huang, "JPEG error analysis and its applications to digital image forensics," *IEEE Trans. on Information Forensics and Security*, vol. 5, no. 3, pp. 480-491, Sep. 2010. Article (CrossRef Link).

[9] T. Sharp, "An Implementation of key-based digital signal steganography," in *Proc. of 4th*

International Workshop on Information Hiding, pp. 13-26, Apr. 2001. Article (CrossRef Link).
[10] G. Doërr, Image Database for Steganalysis Studies [Online]. Available: http://www.cs.ucl.ac.uk/staff/I.Cox/Content/Downloads.html.
[11] E. Zheng, X. Ping and T. Zhang, "Local linear transform and new features of histogram characteristic functions for steganalysis of least significant bit matching steganography," *KSII Transaction on Internet and Information System*, vol. 5, no. 4, pp. 840-855, Apr. 2011. Article (CrossRef Link).
[12] K. Cai, X. Li and T. Zeng, "Reliable histogram features for detecting LSB matching," in *Proc. of IEEE Conf. on Image Processing*, pp. 1761-1764, Sep. 2010. Article (CrossRef Link).
[13] J. Zhang and D. Zhang, "Detection of LSB matching steganography in decompressed images," *IEEE Signal Processing Letters*, vol. 17, no. 2, pp. 141-144, Feb. 2010. Article (CrossRef Link).
[14] X. Li, T. Zhang, Y. Zhang, W. Li and K. Li, "A novel blind detector for additive noise steganography in JPEG decompressed images," *Multimedia Tools and Applications*, published online, May. 2012. Article (CrossRef Link).
[15] M. Goljan, J. Fridrich and T. Holotyak, "New blind steganalysis and its implications," in *Proc. of SPIE Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VIII*, pp. 1-13, Jan. 2006. Article (CrossRef Link).
[16] B. Li, J. Huang and Y. Q. Shi, "Textural features based universal steganalysis," in *Proc. of SPIE Security, Forensics, Steganography and Watermarking of Multimedia*, pp. 1201-1212, Jan. 2008. Article (CrossRef Link).
[17] W. Luo, Y. Wang and J. Huang, "Security analysis on spatial ±1 steganography for JPEG decompressed images," *IEEE Signal Processing Letters*, vol. 18, no. 1, pp. 39-42, Jan. 2011. Article (CrossRef Link).

Xiaodan Hou received her B.S. in Electronic Information Engineering from Zhengzhou Information Science and Technology Institute, Zhengzhou, China, in 2010, and is currently pursuing the M.S. degree. Her research interests include steganalysis, digital image forensics, image processing.

Tao Zhang received his M.S. and Ph.D. degrees in Signal and Information Processing from Zhengzhou Information Science and Technology Institute in 2000 and 2003, respectively. He is currently an Associate Professor with Department of Information Science. His research interests include information hiding, image processing and pattern recognition.

Gang Xiong received his M.S. in Signal and Information Processing from Zhengzhou Information Science and Technology Institute in 2012, and is currently pursuing the Ph.D. degree. His research interests include steganalysis, digital forensics, image processing.

Baoji Wan received his B.S. in Electronic Information Engineering from Zhengzhou Information Science and Technology Institute, Zhengzhou, China, in 2008, and is currently pursuing the M.S. degree. His research interests include steganalysis, digital image forensics, image processing.