1 Introduction

Steganography is a technique of hiding information into innocuous-looking cover media, so as to conceal the very existence of hidden message. The carrier can be many kinds of digital media such as text, image, audio, video, and so on. Recently, JPEG steganography has attracted more and more attention due to the common use of JPEG images. Many JPEG steganographic methods have been proposed, such as J-Steg [1], JPHide [2], F5 [3] and OutGuess [4].

For steganography, the basic requirement is that the modifications caused by embedding should be imperceptible. The initial steganographic algorithms all concentrated on this issue. For example, J-Steg replaces the least significant bits (LSBs) of the quantised discrete cosine transform (qDCT) coefficients with the secret message bits sequentially, and JPHide replaces the LSBs or least two significant bits of the qDCT coefficients with the secret message bits sequentially. For security, modern steganographic algorithms focus on preserving statistical properties of the cover image. Westfeld [3] proposed F5 algorithm. Different from J-Steg algorithm in which the LSBs of the qDCT coefficients are substituted with the secret bits, the absolute value of the randomised qDCT coefficient is decreased by 1 if the coefficient’s LSB does not match the embedded bit. Thus the PoVs do not exist in the obtained stego image, and both the chi-square and the extended chi-square detectors do not work. Combined with the matrix encoding strategy, the embedding efficiency is improved and F5 algorithm can receive considerable capacity besides security.

Provos [4] proposed another JPEG steganography OutGuess. The idea is to divide the cover object into two disjoint parts. The secret bits are embedded into the LSBs of the qDCT coefficients (skipping 0s and 1s) of the first part along a random walk, and then use the second part to perform ‘corrections’ in order to preserve the histogram of qDCT coefficients. The histogram of the stego-image is adjusted to match that of the cover-image. Because the histogram of the final stego-image is similar to that of the cover-image, the stego-image created by OutGuess can avoid the detection of the chi-square and the extended chi-square attacks too.

Although F5 and OutGuess can invalidate the chi-square family attacks effectively, they can be detected by some special calibration-based steganalytic methods [8, 9].
According to [8, 9], through decompressing the stego image, cropping by four pixels in each direction, and recompressing again with the same quality factor, a new calibrated image can be obtained. This newly obtained JPEG image has most macroscopic statistics similar to the original cover image. For F5 algorithm, since the message can be extracted only from the non-zero coefficients at the receiving end, the same message bit must be embedded in the next coefficient again at the transmitting end if the subtraction leads to a zero coefficient. Thus the number of coefficients with value equal to 0 will increase, which is called shrinkage effect. With the help of the calibration technique, this shrinkage effect is analysed and the message length is estimated accurately in [8]. For OutGuess, the embedding mechanism is substitution as J-Steg, that is, overwriting the LSBs of the qDCT coefficients by the secret message bits. Fridrich et al. [9] pointed out the embedding procedure would increase the block effect, that is, the discontinuities in the spatial domain along the boundaries of 8 × 8 JPEG block. However, embedding message into the stego image and cover image will have a different effect since some block effect existed in the stego image may be cancelled out by the repeated LSB substitution procedure. Thus the block effect of the stego image will be smaller than that of the cover image when message bits are re-embedded. This distinguishing statistic can be used to estimate the secret message length with the help of calibration technique. For simplicity, we call these calibration-based statistical attacks S family attacks, and these two schemes for attacking F5 and OutGuess are called S1 and S2, respectively.

Recently, a new high-performance JPEG steganography with a complementary embedding strategy (JPEG-CES) was presented [10]. To counter the detection of the chi-square family and the S family attacks, a novel complementary embedding strategy (CES) is proposed to reduce the loss of statistical property of the cover image. This new algorithm is realised by dividing the qDCT coefficients and the secret bits into two parts according to a predefined partition ratio first. Then the two parts of the secret bits are embedded into the corresponding qDCT coefficient parts with a CES. That is, the secret bits are embedded by subtracting one from one part of coefficients, and adding one to the other part of coefficients. Experimental results have demonstrated that this new strategy can resist the chi-square family and S family attacks successfully.

However, according to our analysis, this new embedding strategy still introduces some disturbances to the cover image. For example, the number of the different qDCT coefficients and the symmetry of the qDCT coefficient histogram both will be disturbed when the message is embedded. Moreover, the intrinsic sign and magnitude dependencies existed in intra-block and inter-block qDCT coefficients will be disturbed too. Thus JPEG-CES may be detected by some state-of-the-art universal steganalysers [11–18] which can catch these two kinds of disturbances, that is, qDCT histogram disturbance and dependency disturbance. In this paper, we present two steganalysers for detecting JPEG-CES. Via exploring the distortions that have been introduced in the qDCT coefficient histogram and the dependencies existed in the intra-block and inter-block sense, respectively, these two alternative steganalysers can detect JPEG-CES effectively. In addition, through merging the features of these two steganalysers, the detection performance can be further improved.

The rest of this paper is organised as follows. In Section 2, the distortions that JPEG-CES may introduce are theoretically analysed. Based on the analysis, two steganalysers are presented to attack JPEG-CES in Section 3. Experimental results are given in Section 4, and the conclusion is drawn in Section 5.

2 Embedding strategy and security analysis of JPEG-CES

In this section, the embedding strategy of JPEG-CES is introduced first. Then theoretical analysis is given to demonstrate the distortions that may be left by this new algorithm.

2.1 Brief overview of JPEG-CES

In this new JPEG steganography, the secret message bits are embedded into the qDCT coefficients of the JPEG image directly. The main steps of JPEG-CES are as follows.

1. The QDCT coefficients are permuted with a stego-key K1 and then divided into two parts Q1 and Q2 according to a predefined partition ratio α, that is, \( \text{length}(Q_1) : \text{length}(Q_2) = \alpha : 1 \), where the function \( \text{length}(\cdot) \) is used to compute the length of the sequence \( Q_1 \) and \( Q_2 \).
2. The original message is encrypted to generate the secret bit stream, and then the secret bit stream is divided into two parts \( M_1 \) and \( M_2 \) according to the same predefined partition ratio \( \alpha \).
3. The bits in \( M_1 \) are embedded into \( Q_1 \) according to the embedding algorithm \( E_1 \), and then the bits in \( M_2 \) are embedded into \( Q_2 \) according to the embedding algorithm \( E_2 \). The embedding algorithm \( E_1 \) and \( E_2 \) are described briefly in Figs. 1a and b, respectively, where the lengths of bars are proportional to the quantities of qDCT coefficients. For simplicity, we only illustrate the qDCT coefficients whose values belong to the range \([-5, 5]\). In these two figures, the secret bit ‘0’ or ‘1’ is illustrated at the end of the arrowed line, and the arrowhead points to the new value of the qDCT coefficient after secret message embedding. For example, in Fig. 1a, the qDCT coefficient with value of 1 may change to –1 if a secret bit ‘0’ is embedded; otherwise, it remains at 1 if the secret bit is ‘1’. We note that in the algorithm \( E_1 \), one section of the qDCT coefficients with value of –2 after embedding should be changed to 1 again to preserve the histogram of qDCT coefficients. The number of bits that need to be changed is \( \beta \cdot \text{length}(M_1) \), where \( \beta \in (0, 1) \) is a secret parameter.
4. After data embedding, the obtained DCT coefficients \( Q_1' \) and \( Q_2' \) containing the secret message are concatenated, de-permutated and re-coded to obtain the JPEG stego-image.

2.2 Security analysis of JPEG-CES

The philosophy behind JPEG-CES steganography [10] is simple but effective. In order to invalidate some specific steganalysers such as the chi-square family and \( S \) family detectors, a complementary strategy is adopted in the embedding algorithm \( E_1 \) and \( E_2 \). As described in Fig. 1, if one secret bit is embedded in \( Q_1 \) part, algorithm \( E_1 \) is executed and the value of the coefficient will be preserved or subtracted by one. On the contrary, if the secret bit is embedded in \( Q_2 \) part, algorithm \( E_2 \) should be implemented and the value of the coefficient will be preserved or added by one. Through using this new CES together with carefully selected parameters \( \alpha \) and \( \beta \), the histogram of the qDCT coefficients can be preserved to some extent. Moreover, both of the two embedding algorithms \( E_1 \) and \( E_2 \)
are different from the LSB substitution strategy adopted in J-Steg, JPHide and OutGuess. For example, in algorithm $E_1$ described in Fig. 1a, if one secret bit ‘1’ is embedded into the coefficient with value of $-1$, this coefficient will be changed to $-2$. Conversely, whether the secret bit ‘0’ or ‘1’ is embedded into the coefficient with value of $-2$, this coefficient will not be changed to $-1$ again. Thus the PoVs existed in LSB replacement scheme disappeared and the chi-square family attacks are effectively invalidated. In addition, since the embedding strategy of JPEG-CES is not LSB substitution, the block effect existed in the stego image may not be cancelled out as in OutGuess after re-LSB substitution, the block effect existed in the stego image with respect to the corresponding cover image. Through analysing the histogram distribution and the correlation existed in the intra-block and inter-block qDCT coefficients, the distortions introduced by JPEG-CES can be discovered.

2.2.1 Histogram distribution analysis: Let $h_d(d)$, $h_d(d) (d \in Z)$ denote the total number of qDCT coefficients with value of $d$ in the cover image and its corresponding stego image, respectively. In the follow equations, $\alpha$ and $\beta$ represent the predefined partition ratio and the secret parameter used in the embedding procedure of JPEG-CES, and $p (0 \leq p \leq 1)$ represents the embedding rate, that is, the bpc (bit per non-zero DCT coefficients) value. We assume that the message bits are encrypted first, and in the obtained secret message bits ‘0’ and ‘1’ are uniformly distributed. Then for a non-zero coefficient in the cover image, the probability that it will be modified is $p/2$, and the probability that it will be preserved is $(1-p/2)$. We analyse the quantities of the coefficients with different values separately as follows.

1. The coefficients with value of 0.

Since the qDCT coefficients whose values are equal to 0 remain untouched when the secret message bits are embedded, $h_0(0)$ is equal to $h_0(0)$ and the histogram of the qDCT coefficients with value equal to 0 is well preserved. That is

$$h_s(0) = h_c(0) \quad (1)$$

2. The coefficients with value of −1.

For the qDCT coefficients whose values are equal to −1, we can obtain

$$h_s(-1) = h_c(-1) - \frac{p}{2} h_c(-1) + \frac{p}{2} \frac{\alpha}{\alpha + 1} h_c(1) + \frac{1}{2} \frac{\alpha}{\alpha + 1} h_c(-2) \quad (2)$$

Since the statistics of the DCT coefficients are best approximated by a general Gaussian distribution [19], there exists $h_c(1) \simeq h_c(-1)$ and $h_c(-2) < h_c(-1)$. From (2) we can obtain

$$h_s(-1) \leq h_c(-1) - \frac{p}{2} h_c(-1) + \frac{p}{2} \frac{\alpha}{\alpha + 1} h_c(1) + \frac{1}{2} \frac{\alpha}{\alpha + 1} h_c(-1) \approx h_c(-1) \quad (3)$$

Equation (3) means that the qDCT coefficients with value equal to −1 cannot be preserved after embedding the secret message bits.

3. The coefficients with value of $d(d \neq 0, -1)$.

For the qDCT coefficients whose values are equal to $d(d \neq 0, -1)$, we have the following equations.

$$h_s(d) = h_c(d) - \frac{p}{2} h_c(d) + \frac{p}{2} \frac{\alpha}{\alpha + 1} h_c(2) + \frac{p}{2} \frac{1}{\alpha + 1} h_c(-1) + \beta p \frac{\alpha}{\alpha + 1} \left( \sum_d h_c(d) - h_c(0) \right) \quad (4)$$
distribution of DCT coefficients [19], there exists disturbed too. According to the general Gaussian message is embedded. Furthermore, we can find that the different qDCT coefficients will change when the secret |

Generally, (7)–(9) cannot hold true simultaneously since there are only two variables \( \alpha \) and \( \beta \) in this series of equations. That is to say, the coefficients with value equal to \( d(d \neq -1, 0) \) cannot be fully preserved.

From (4)–(6), we can deduce that in order to preserve the coefficients whose values are equal to \( d(d \neq -1, 0) \), that is, \( h_s(d) \approx h_c(-d) \) for the cover image. In order to preserve the symmetry of the qDCT coefficient histogram \( h_s(d) \) needs to be satisfied in the corresponding stego image. For JPEG-CEs, \( h_s(1) \approx h_c(-1) \) and \( h_s(2) \approx h_c(-2) \) may hold true by chance through carefully selecting \( \alpha \) and \( \beta \) values. However, for the other coefficients with value equal to \( d(d > 2) \), according to (6) we can obtain the following equations.

\[
\begin{align*}
    h_s(d) &= h_c(-d) - \frac{p}{2} h_s(d) + \frac{p \alpha}{2 \alpha + 1} h_s(d + 1) \\
    &+ \frac{p}{2 \alpha + 1} h_c(d - 1) \quad (|d| > 2)
\end{align*}
\]

In order to preserve the symmetry of the qDCT coefficient histogram in the stego image, (11) needs to be satisfied.

\[
    h_s(d) = h_c(-d) \quad (|d| > 2)
\]

That is

\[
\begin{align*}
    h_s(d) &= \frac{p}{2} h_c(d) + \frac{p \alpha}{2 \alpha + 1} h_c(d + 1) + \frac{1}{2 \alpha + 1} h_c(d - 1) \\
    &= h_c(-d) - \frac{p}{2} h_c(-d) + \frac{p \alpha}{2 \alpha + 1} h_c(-d + 1) \\
    &+ \frac{1}{2 \alpha + 1} h_c(-d - 1) \quad (|d| > 2)
\end{align*}
\]

Since \( h_s(d) \approx h_c(-d) \), \( h_s(d + 1) \approx h_c(-d - 1) \) and \( h_s(d - 1) \approx h_c(-d + 1) \) according to [19], (12) is simplified as

\[
h_s(d + 1) \approx h_c(-d - 1) \quad (|d| > 2)
\]

Generally, Eq. (13) cannot hold true according to [19]. Thus we can conclude that the symmetry of the qDCT coefficient histogram will be disturbed too.

2.2.2 Dependency analysis: According to [20], there exist three kinds of dependencies in the qDCT coefficients, that is, intra-block correlation, inter-block correlation and sign correlation. For easier explanation of these three kinds of dependencies, we make a few alterations to the qDCT coefficient matrix first. Suppose that the test JPEG image \( I_{tes} \) has the dimension of \( M \times N \) when decompressed into spatial domain. Without loss of generality, we assume that \( M \) and \( N \) are the multiples of 8. Consider a matrix \( J_{tes} \) consisting of all of the \( 8 \times 8 \) qDCT coefficients, which has been quantised with the quantisation table and not zig-zag scanned. This qDCT coefficient matrix \( J_{tes} \) has the same size as the test image \( I_{tes} \) and thus there are \( N_B = (M/8) \times (N/8) \) blocks in it, which is shown in Fig. 2.

Expand each \( 8 \times 8 \) qDCT coefficients in \( J_{tes} \) into a 1-D column vector according to zig-zag scanning sequence. Then arrange all these column vectors by the two scanning patterns as shown in Figs. 3a and b. The row scanning pattern matrix \( J_{tes}^r \) and column scanning pattern matrix \( J_{tes}^c \) can be obtained, as shown in Figs. 4a and b, respectively. In Fig. 4, \( J_{tes}^r(i,j) \) represents \( i \)th coefficient in the \( j \)th block of the row scanning pattern matrix, and \( J_{tes}^c(i,j) \) represents \( i \)th coefficient in the \( j \)th block of the column scanning pattern matrix.

As we can see, in these two \( 64 \times N_B \) matrices \( J_{tes}^r \) and \( J_{tes}^c \), the coefficients of the same block are in the same column and the coefficients of the same frequency are in the same row. For example, matrices \( J_{tes}^r(1,i) \) and \( J_{tes}^r(1,i+1) \) represent the two neighbouring coefficients inside the \( 8 \times 8 \) block, \( J_{tes}^c(i,j) \) and \( J_{tes}^c(i,j+1) \) represent the same

<table>
<thead>
<tr>
<th>8.8</th>
<th>8.8</th>
<th>...</th>
<th>8.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.8</td>
<td>\text{\textemdash}</td>
<td>...</td>
<td>8.8</td>
</tr>
<tr>
<td>\text{\textemdash}</td>
<td>\text{\textemdash}</td>
<td>\text{\textemdash}</td>
<td>8.8</td>
</tr>
<tr>
<td>8.8</td>
<td>...</td>
<td>...</td>
<td>8.8</td>
</tr>
</tbody>
</table>

Fig. 2 qDCT coefficient matrix
frequency coefficients in the two neighbouring blocks according to the row scanning pattern. The three kinds of dependencies described in [20] can be easily explained in these two matrices. The inter-block dependency represents the correlation among the coefficients in the row, and intra-block dependency represents the correlation among the coefficients within the column, respectively. Moreover, since all elements in these two matrices \( J_{tes}^{r} \) and \( J_{tes}^{c} \) are qDCT coefficients, they have sign and magnitude characteristics. Thus intra-block and inter-block correlation both include sign and magnitude dependencies.

For JPEG-CES, the secret message bits are randomly embedded into the qDCT coefficients of the cover image. The host qDCT coefficients will plus one or minus one according to the coefficient value and embedded message bit, the correlation among the neighbouring coefficients of \( J_{tes}^{r} \) and \( J_{tes}^{c} \) is not considered. Thus the intrinsic magnitude dependency existed in the intra-block and inter-block qDCT coefficients of the cover image will be disturbed. Moreover, the coefficients with value equal to 1 may jump to −1 directly, and vice versa. Thus the sign dependency belonging to the neighbouring coefficients of \( J_{tes}^{r} \) and \( J_{tes}^{c} \) will be disturbed too. That is to say, all those three kinds of intrinsic dependencies described in [20] will be disturbed when the secret message is embedded using JPEG-CES.

According to the above analysis, although the presence of the embedded messages is imperceptible to the human eye, the qDCT coefficient histogram and the dependencies existed in intra-block and inter-block qDCT coefficients both will be disturbed when the message is embedded. Thus if we can extract some features to measure these statistical differences between the cover and stego image, the existence of hidden message using JPEG-CES might be detected.

### 3 New detection approach

In this section, two steganalytic approaches are presented, which are based on the qDCT histogram (denoted by Histogram Detector) and dependencies existed in intra-block and inter-block qDCT coefficients (denote by Dependency Detector), respectively. In order to further improve the detection accuracy rate, the calibration technique firstly presented in [8] is also adopted in these two steganalytic approaches, whereas the calibrated image is realised by cropping the test image with four rows and four columns, and then recompressing again with the same quality factor. Thus these two presented detectors both have two feature sets. The first one is extracted from the test image directly, and the second one is extracted as a difference between the features extracted from the test image and those extracted from the calibrated image.

#### 3.1 Histogram detector

According to the analysis in Section 2.2, we can find that the quantities of the qDCT coefficients with different values and the symmetry of the qDCT coefficient histogram are disturbed when the message is embedded. In this section, our main purpose is to propose some new features from the qDCT coefficient histogram to explore the distortion. Without loss of generality, we suppose that the test JPEG image has the dimension of \( M \times N \) when decompressed into spatial domain. Let \( h_{tes}(i), h_{qdb}(i) (i \in Z) \) denote the number of qDCT coefficients whose values are equal to \( i \) in the test image and its corresponding calibrated image, respectively. The two feature sets of Histogram Detector, denoted by HisSet and CldHisSet, are illustrated as follows.

1. **HisSet**: The features in **HisSet** are about the number of the different qDCT coefficients, which are extracted from the test image. Considering that the test image may have different dimension sizes, we do not compute the quantities of different qDCT coefficients directly. Instead, we compute the ratio of the number of different qDCT coefficients to the total number of qDCT coefficients. The first eight features in **HisSet** are expressed as follows.

\[
\frac{h_{tes}(i)}{M \times N}, \quad (i = -4, -3, -2, -1, 1, 2, 3, 4)
\]

The rest features in **HisSet** include four features about the symmetry properties of the qDCT coefficient histogram of the test image. It is represented as

\[
\frac{|h_{tes}(i) - h_{tes}(-i)|}{\min((h_{tes}(i), h_{tes}(-i))), \quad (i = 1, 2, 3, 4)}
\]

**Fig. 3** Two scanning patterns

* a Row scanning pattern
* b Column scanning pattern

**Fig. 4** Two scanning pattern matrices

* a Row scanning pattern matrix
* b Column scanning pattern matrix

© The Institution of Engineering and Technology 2011

where $|\cdot|$ is the absolute function and $\min(\cdot)$ is the minimum function.

2. **ClbHisSet:** All these features are extracted as a difference between the features extracted from the test image and those extracted from the calibrated image. The first eight features in ClbHisSet are represented as

$$h_{tes}(l) - h_{clb}(l) \quad (i = -4, -3, -2, -1, 1, 2, 3, 4)$$

The rest four features in ClbHisSet are represented as

$$\frac{|h_{tes}(l) - h_{tes}(-l)| - |h_{clb}(l) - h_{clb}(-l)|}{\min((h_{tes}(l), h_{tes}(-l)))} \quad (i = 1, 2, 3, 4)$$

In order to reduce the dimensionality of the feature vector, in these two feature sets, only the DCT coefficients whose values belonging to the range $[-4, 4]$ are considered. There are totally 24 features in Histogram Detector.

### 3.2 Dependency Detector

Keeping the same notation as in the previous section, let $J'_{tes}$ and $J'_{clb}$ denote the row pattern and column scanning pattern matrices of the test image. In the same manner, $J_{clb}$ and $J_{tes}$ can be obtained, which represent row scanning pattern and column scanning pattern matrices of the calibrated image. As in [12–15], the Markov process is adopted to model the dependencies existed in the intra-block and inter-block qDCT coefficient. Since JPEG-CES not only changes the magnitude but also the sign of the qDCT coefficients, in our method the existed sign and magnitude dependencies both have been explored by the Markov process. Before modelling the dependencies through the Markov empirical transition matrices, the threshold technique [13–16] is applied to reduce the feature dimension and computational complexity. That is, in these four matrices $J'_{tes}$, $J_{tes}$, $J_{clb}$, and $J_{clb}$, if the element is larger than $T$ or smaller than $-T$, it is truncated to $T$ and $-T$, respectively. Otherwise, the elements with value belonging to $[-T, T]$ do not change. The Markov transition matrices are computed as follows. For example, for the row scanning matrix $J'_{tes}$, the inter-block dependency is computed as

$$M_h(m, n; J_{tes}) = \frac{\sum_{i=1}^{64} \sum_{j=1}^{N_x} \delta(J'_{tes}(i, j) = m, J_{tes}(i, j + 1) = n; J_{tes}(i, j + 1) = m)}{\sum_{i=1}^{64} \sum_{j=1}^{N_x} \delta(J'_{tes}(i, j) = m)}$$

where $J'_{tes}(i, j)$ represents the coefficient value at the position $(i, j)$ in matrix $J'_{tes}$, and $m, n \in [-T, T]$. The $\delta(x, y)$ is the impulse response function.

$$\delta(x = m, y = n) = \begin{cases} 1, & \text{if } x = m \text{ and } y = n \\ 0, & \text{otherwise} \end{cases}$$

Also the intra-block dependency is measured by

$$M_h(m, n; J_{clb}) = \frac{\sum_{i=1}^{64} \sum_{j=1}^{N_x} \delta(J'_{clb}(i, j) = m, J_{clb}(i, j + 1) = n)}{\sum_{i=1}^{64} \sum_{j=1}^{N_x} \delta(J'_{clb}(i, j) = m)}$$

In the same manner, the dependency matrices $M_h(m, n; J_{tes}^c)$, $M_h(m, n; J_{clb}^c)$, $M_h(m, n; J_{tes}^c)$, and $M_h(m, n; J_{clb}^c)$ for $(m, n) \in \{-T, T\}$ can be easily computed according to (14) and (15). There exists $M_h(m, n; J_{tes}) = M_h(m, n; J_{tes}^c)$ and $M_h(m, n; J_{clb}) = M_h(m, n; J_{clb}^c)$, since $M_h(m, n; J_{tes})$ and $M_h(m, n; J_{clb})$ both represent the intra-block dependency in the test image, $M_h(m, n; J_{tes}^c)$ and $M_h(m, n; J_{clb}^c)$ both represent the intra-block dependency in the calibrated image.

After these dependency matrices have been computed, the features can be easily obtained. The proposed Dependency Detector also contains two sets of features, denoted by DepSet and ClbDepSet, respectively.

1. **DepSet:** The features in DepSet are extracted directly from the test image, which is used to explore the original magnitude and sign correlation existed in the intra-block and inter-block sense. The first $(2T + 1) \times (2T + 1)$ features in DepSet are described as

$$M_v(m, n; J_{tes}^c), (m, n) \in \{-T, T\}$$

and the rest $(2T + 1) \times (2T + 1)$ features in DepSet are described as

$$M_h(m, n; J_{tes}) + M_h(m, n; J_{tes}^c), (m, n) \in \{-T, T\}$$

2. **ClbDepSet:** The calibrated features in ClbDepSet are calculated as a difference between the features extracted from the test image and those from its corresponding calibrated image. The first $(2T + 1) \times (2T + 1)$ features in ClbDepSet are described as

$$M_v(m, n; J_{tes}^c) - M_v(m, n; J_{tes}), (m, n) \in \{-T, T\}$$

and the rest $(2T + 1) \times (2T + 1)$ features in ClbDepSet are described as

$$M_h(m, n; J_{tes}) + M_h(m, n; J_{tes}^c) - 2 \frac{M_h(m, n; J_{tes}^c)}{2}, (m, n) \in \{-T, T\}$$

As in Histogram Detector, the threshold value is selected as 4 to reduce the dimensionality of the feature vector and computational complexity. Therefore there are totally 324 features in Dependency Detector.

### 4 Experimental results

Several experiments have been conducted to examine the performance of the proposed steganalyzers. Our test image set consists of 5000 uncompressed images. Among them, 2631 images were taken by us in different places with different cameras, 1543 images were downloaded from natural resources conservation service (NRCS) [21], and the other 1096 images are from CorelDraw [22]. All the 5000 images are central-cropped into the size of $512 \times 512$ and then JPEG compressed with quality factor 75.

According to [10], JPEG-CES steganography can confuse the chi-square family and $S$ family attacks effectively by using $3/\alpha \leq \beta \leq 5/\alpha$ together with an adjustment parameter $\beta$, and a high security performance will be achieved when setting $\alpha = 4/3$ and $\beta = 1/3$. In our experiments, we have tested the security performance of JPEG-CES under two
cases. In the first case, JPEG-CES is conducted while choosing $\alpha = 4/1$ and $\beta = 1/3$. In the second case, the values of $\alpha$ is randomly selected from $A = 3, 4, 5$ and $\beta$ is randomly selected from $B = 1/2, 1/3, 1/4, 1/5, 1/6, 1/7, 1/8, 1/9, 1/10$, respectively. That is, in the second case, the predefined partition ratio $\alpha$ and the secret parameter $\beta$ are randomly selected from $A$ and $B$ for each image. In our experiments, the training set for every classifier contained 4000 cover images and their corresponding 4000 stego images, which are selected randomly. The remaining 1000 cover and 1000 stego images are used for test. As we can see, in Case 1 a specific classifier corresponding to $\alpha = 4/1$ and $\beta = 1/3$ is obtained, and in Case 2 a general classifier corresponding to the randomly selected $\alpha$ and $\beta$ is achieved.

The security performance of JPEG-CES with different embedding rates (represented by bpcn values) is tested in our experiments. The TNR, TPR represent the true negative rate and true positive rate, respectively, and AR (AR = (TNR + TPR)/2) represents the accuracy rate. The LibSVM [23] is adopted as the classifier. For a fair comparison, the second-order polynomial kernel is selected in all our next experiments.

### 4.1 Experimental results of histogram detector

We test the security performance of JPEG-CES with the Histogram Detector that has presented in Section 3.1. The experimental results are demonstrated in Table 1. It is observed from Table 1 that even the embedding rate of JPEG-CES is as low as 0.02 bpcn the detection accuracy rates of our method are better than random guessing under the two cases. We also conduct some other experiments in order to examine the contributions made by different feature sets. It is observed that the calibrated features may have a bit more contribution to the final detection performance, and combining these two feature sets has enhanced the detection accuracy rates in attacking JPEG-CES.

### 4.2 Experimental results of dependency detector

The detection performance of Dependency Detector presented in Section 3.2 is also tested. The experimental results are shown in Table 2. It is observed from Table 2 that Dependency Detector is better than Histogram Detector in detecting JPEG-CES. Even the embedding rate is as low as 0.01 bpcn, the detection accuracy rates are better than random guessing under the two cases. The contributions made by the different feature sets are also illustrated in Table 2. It is observed from Table 2 that the features in DepSet and ClbDepSet have the similar contribution to the final detection performance, and combining these two feature sets has enhanced the detection accuracy rates.

### 4.3 Testing results of combined detector

In this section, all the features of Histogram Detector and Dependency Detector are merged together and a composite detector is constructed. There are 348 features in this Combined Detector. The testing results are shown in Table 3. It is observed via comparing Table 3 with Tables 1 and 2 that the detection accuracy rate can be improved further by this Combined Detector.

We also compared the detection performance of our Combined Detector with that of MP-324 [14], MP-486 [15] and JFMP-274 [12], respectively, where 324, 486 and 274 represent the total number of features corresponding to different steganalytic methods, and MP stands for Markov process and JF for JPEG features [11]. To our knowledge, these three steganalysers are among the best steganalytic methods in detecting JPEG-CES (Some other experiments about the steganalysers [16–18] have also been conducted and the experimental results demonstrate that these three JPEG steganalysers [12, 14, 15] can detect JPEG-CES more effectively.) It is observed from Table 3 that our Combined Detector outperforms these three state-of-the-art JPEG steganalysers in detecting JPEG-CES. However, compared with JFMP-274, the improvement is rather limited. It is not surprising to us since JFMP-274 considers the qDCT coefficient histogram distribution and dependencies existed in the intra-block and inter-block qDCT coefficients simultaneously as our combined method. For today’s steganalysers, another factor we should consider is the computational complexity. Since the classifier is trained offline in general, the efficiency of the steganalysers is mainly determined by the feature extraction time. In the last line in Table 3, the average feature extraction time (per image) of these four steganalysers on our personal computer (Dual-Core P8600, 2.4GHZ, 2GB RAM) is listed. As we can see, even the number of features in our method is more than that of JFMP-274’s, the feature extraction time of our method is about 1/8 of JFMP-274’s. Compared with MP-324 and MP-486, the computational payload of our method is acceptable considering about the improvement in detection accuracy rate.

From Table 3, we can also find out that through utilising additional 162 features which can catch the inter-block dependency among the qDCT coefficients, MP-486 outperforms MP-324, generally. Moreover, through exploring the qDCT histogram disturbance and dependency disturbance simultaneously, JFMP-274 outperforms MP-324 and MP-486 in all cases. This observation verified our

### Table 1 Detection results of histogram detector (TNR: true negative rate; TPR: true positive rate; AR: accuracy rate)

<table>
<thead>
<tr>
<th>$\alpha$, $\beta$</th>
<th>bpcn</th>
<th>TNR</th>
<th>TPR</th>
<th>AR</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\alpha = 4/1$, $\beta = 1/3$</td>
<td>0.01</td>
<td>58.2</td>
<td>58.2</td>
<td>58.2</td>
</tr>
<tr>
<td></td>
<td>0.02</td>
<td>66.1</td>
<td>67.4</td>
<td>66.8</td>
</tr>
<tr>
<td></td>
<td>0.05</td>
<td>81.9</td>
<td>84.4</td>
<td>83.2</td>
</tr>
<tr>
<td></td>
<td>0.10</td>
<td>96.8</td>
<td>96.9</td>
<td>96.9</td>
</tr>
<tr>
<td>randomly selected</td>
<td>0.01</td>
<td>58.9</td>
<td>59.9</td>
<td>59.4</td>
</tr>
<tr>
<td></td>
<td>0.02</td>
<td>66.5</td>
<td>69.0</td>
<td>67.8</td>
</tr>
<tr>
<td></td>
<td>0.05</td>
<td>84.6</td>
<td>87.5</td>
<td>86.1</td>
</tr>
<tr>
<td></td>
<td>0.10</td>
<td>97.2</td>
<td>98.6</td>
<td>97.6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$\alpha$, $\beta$</th>
<th>bpcn</th>
<th>TNR</th>
<th>TPR</th>
<th>AR</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\alpha = 4/1$, $\beta = 1/3$</td>
<td>0.01</td>
<td>48.6</td>
<td>62.7</td>
<td>55.7</td>
</tr>
<tr>
<td></td>
<td>0.02</td>
<td>60.9</td>
<td>63.4</td>
<td>62.2</td>
</tr>
<tr>
<td></td>
<td>0.05</td>
<td>74.4</td>
<td>75.5</td>
<td>75.0</td>
</tr>
<tr>
<td></td>
<td>0.10</td>
<td>89.9</td>
<td>92.4</td>
<td>91.2</td>
</tr>
<tr>
<td>randomly selected</td>
<td>0.01</td>
<td>51.1</td>
<td>62.8</td>
<td>57.0</td>
</tr>
<tr>
<td></td>
<td>0.02</td>
<td>61.9</td>
<td>64.4</td>
<td>63.2</td>
</tr>
<tr>
<td></td>
<td>0.05</td>
<td>77.0</td>
<td>77.6</td>
<td>77.3</td>
</tr>
<tr>
<td></td>
<td>0.10</td>
<td>92.2</td>
<td>92.6</td>
<td>92.4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$\alpha$, $\beta$</th>
<th>bpcn</th>
<th>TNR</th>
<th>TPR</th>
<th>AR</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\alpha = 4/1$, $\beta = 1/3$</td>
<td>0.01</td>
<td>52.9</td>
<td>60.6</td>
<td>56.8</td>
</tr>
<tr>
<td></td>
<td>0.02</td>
<td>61.2</td>
<td>64.9</td>
<td>63.1</td>
</tr>
<tr>
<td></td>
<td>0.05</td>
<td>77</td>
<td>83.2</td>
<td>80.1</td>
</tr>
<tr>
<td></td>
<td>0.10</td>
<td>93.7</td>
<td>95.9</td>
<td>94.8</td>
</tr>
<tr>
<td>randomly selected</td>
<td>0.01</td>
<td>55.6</td>
<td>60.4</td>
<td>58.0</td>
</tr>
<tr>
<td></td>
<td>0.02</td>
<td>62.7</td>
<td>68</td>
<td>65.4</td>
</tr>
<tr>
<td></td>
<td>0.05</td>
<td>79.3</td>
<td>85.0</td>
<td>82.2</td>
</tr>
<tr>
<td></td>
<td>0.10</td>
<td>95.6</td>
<td>96.3</td>
<td>96.0</td>
</tr>
</tbody>
</table>
previous analysis too. That is, the qDCT coefficient histogram and dependencies existed in the intra-block and inter-block qDCT coefficients both have been disturbed by JPEG-CES. Thus if we can find some features to explore these disturbances, JPEG-CES will be defeated.

4.4 Testing results with general classifier

From the experimental results in Table 1–3, we can conclude that if the values of $\alpha$ and $\beta$ are known to us, a specific classifier can be designed and reliable detection performance can be achieved. However, since the selected values of $\alpha$ and $\beta$ are usually unknown to the potential attacker, the specific classifier may be invalid in practice. In order to achieve a more reasonable result, we further test the efficiency of our general classifier. The experimental results are shown in Table 4, in which we use the general classifier achieved in Case 2 to detect the test images achieved in Case 1. It is observed from Table 4 that our general classifier can also achieve a reliable detection performance.

5 Conclusions

In this paper, a new presented JPEG steganography JPEG-CES is studied. Our theoretical analysis demonstrates that the proposed complementary strategy cannot fully preserve the statistical properties of the cover image. The distribution of qDCT coefficient histogram and the intrinsic sign and magnitude dependencies existed in intra-block and inter-block qDCT coefficients will be disturbed when the message is embedded.

Based on the analysis, two new feature-based steganalysers are presented. Through exploring the features which can measure the difference between the cover and stego image, both of these two steganalysers are able to detect JPEG-

---

### Table 2 Detection results of dependency detector (TNR: true negative rate; TPR: true positive rate; AR: accuracy rate)

<table>
<thead>
<tr>
<th>$\alpha$, $\beta$</th>
<th>bpnc</th>
<th>Dependency detector</th>
<th>DepSet</th>
<th>ClbDepSet</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>TNR</td>
<td>TPR</td>
<td>AR</td>
<td>TNR</td>
</tr>
<tr>
<td>$\alpha = \frac{4}{1}$ $\beta = \frac{1}{3}$</td>
<td>0.01</td>
<td>64.5</td>
<td>62.6</td>
<td>63.6</td>
</tr>
<tr>
<td></td>
<td>0.02</td>
<td>76.6</td>
<td>74.3</td>
<td>75.5</td>
</tr>
<tr>
<td></td>
<td>0.05</td>
<td>95.9</td>
<td>95.8</td>
<td>95.9</td>
</tr>
<tr>
<td>randomly selected</td>
<td>0.10</td>
<td>99.7</td>
<td>99.6</td>
<td>99.7</td>
</tr>
<tr>
<td></td>
<td>0.01</td>
<td>66.5</td>
<td>62.5</td>
<td>64.5</td>
</tr>
<tr>
<td></td>
<td>0.02</td>
<td>78.2</td>
<td>76.4</td>
<td>77.3</td>
</tr>
<tr>
<td></td>
<td>0.05</td>
<td>97.1</td>
<td>97.0</td>
<td>97.1</td>
</tr>
<tr>
<td></td>
<td>0.10</td>
<td>99.6</td>
<td>99.8</td>
<td>99.7</td>
</tr>
</tbody>
</table>

### Table 3 Comparison with other universal steganalysers (TNR: true negative rate; TPR: true positive rate; AR: accuracy rate)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>TNR</td>
<td>TPR</td>
<td>AR</td>
<td>TNR</td>
<td>TPR</td>
</tr>
<tr>
<td>$\alpha = \frac{4}{1}$ $\beta = \frac{1}{3}$</td>
<td>0.01</td>
<td>58.8</td>
<td>56.4</td>
<td>57.6</td>
<td>62.1</td>
</tr>
<tr>
<td></td>
<td>0.05</td>
<td>81.5</td>
<td>80.8</td>
<td>81.2</td>
<td>91.3</td>
</tr>
<tr>
<td>randomly selected</td>
<td>0.01</td>
<td>57.9</td>
<td>57.6</td>
<td>57.8</td>
<td>61.2</td>
</tr>
<tr>
<td></td>
<td>0.05</td>
<td>85.8</td>
<td>82.4</td>
<td>84.1</td>
<td>93.4</td>
</tr>
<tr>
<td>time(s) per image</td>
<td>0.74s</td>
<td>1.08s</td>
<td>9.45s</td>
<td>1.28s</td>
<td></td>
</tr>
</tbody>
</table>

### Table 4 Detection results with general classifier and specific test image data sets (TNR: true negative rate; TPR: true positive rate; AR: accuracy rate)

<table>
<thead>
<tr>
<th>Bpnc</th>
<th>General combined classifier</th>
<th>General dependency detector</th>
<th>General histogram detector</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>TNR</td>
<td>TPR</td>
<td>AR</td>
</tr>
<tr>
<td>0.01</td>
<td>65.4</td>
<td>63.0</td>
<td>64.2</td>
</tr>
<tr>
<td>0.02</td>
<td>79.2</td>
<td>72.2</td>
<td>75.7</td>
</tr>
<tr>
<td>0.05</td>
<td>97.4</td>
<td>93.5</td>
<td>95.5</td>
</tr>
<tr>
<td>0.10</td>
<td>99.8</td>
<td>99.6</td>
<td>99.7</td>
</tr>
</tbody>
</table>
CES better than random guessing even with a very low embedding rate. Moreover, through merging the features of these two steganalysers, a more efficient classifier can be obtained.

Our theoretical analysis and experimental results also indicate that the secure steganographic methods for JPEG images should preserve both the statistics of qDCT coefficient histogram and the dependencies existed in the intra-block and inter-block qDCT coefficient simultaneously. Otherwise, it may be easily detected by some state-of-the-art blind JPEG steganalysers.

6 Acknowledgments

This work was supported by the National Basic Research Program of China (No. 2006CB303104), the National Natural Science Foundation of China (Nos. 90604008 and 60633030), the Doctoral Program of Higher Education of China (No. 20070558054), and the China Postdoctoral Science Foundation (No. 20080440795).

7 References

2. http://linux01.gwdg.de/~alatham/stego.html