An Adaptive JPEG Steganographic Method Based on Weight Distribution for Embedding Costs

Yi Sun[1*], Guangming Tang[2], Yuan Bian[1] and Xiaoyu Xu[1]

[1] Zhengzhou Information Science and Technology Institute, P.R. China
[e-mail: mickyfaith@163.com, xxyin1992@163.com]

[2]Department of Information Security
Zhengzhou Information Science and Technology Institute, P.R. China
[tgm1983@sina.com]

*Corresponding author: Yi Sun

Received July 4, 2016; revised January 10, 2017; accepted February 10, 2017; published May 31, 2017

Abstract

Steganographic schemes which are based on minimizing an additive distortion function defined the overall impacts after embedding as the sum of embedding costs for individual image element. However, mutual impacts during embedding are often ignored. In this paper, an adaptive JPEG steganographic method based on weight distribution for embedding costs is proposed. The method takes mutual impacts during embedding in consideration. Firstly, an analysis is made about the factors that affect embedding fluctuations among JPEG coefficients. Then the Distortion Update Strategy (DUS) of updating the distortion costs is proposed, enabling to dynamically update the embedding costs group by group. At last , a kind of adaptive JPEG steganographic algorithm is designed combining with the update strategy and well-known additive distortion function . The experimental result illustrates that the proposed algorithm gains a superior performance in the fight against the current state-of-the-art steganalyzers with high-dimensional features.

Keywords: Information security, Information hiding, Adaptive Steganography, JPEG

1. Introduction

Steganography is an important branch of information hiding. It is a covert communication approach which changes the original digital media slightly in order to hide secret messages without causing suspicions. The digital media can be various such as text, images, audio, video, etc. Image is currently the most widely used vector format, therefore, steganography based on image is a hot spot in the present study.

Steganography embeds secret messages by modifying the cover image. The greater the influence caused by embedding operation, the more likely to be detected. Currently, the adaptive steganography [1][2] is the most effective steganographic schemes. It is based on minimizing the additive distortion function, which defines the distortion as the sum of embedding cost for individual image element. The key is to design and minimize the distortion function, combining with the steganographic codes, in order to achieve the purpose of reducing the detection rate and improving security. In [3], T.Filler et.al. propose syndrome-trellis coding (STC), which enable secret message embedding under additive distortion asymptotically approach the theoretical bound. Therefore, the research for properly distortion function gradually becomes a domain of extensive research instead of improving the coding scheme. WOW (Wavelet Obtained Weights) [4], UNIWARD (UNIversal WAvelet Relative Distortion) [5]and HILL (HIghpass, Low-pass, and Low-pass) [6] define the cost of individual image element using directional filters. They assign low costs for the noise and texture area and high costs for smooth area, hence they have improved security performance of embedding. In [7], V.Sedighi et.al. model the image elements as a series of independent non-identically distributed generalized Gaussian random variables, then embed secret messages using STC codes, improving the performance of statistical undetectability for steganography.UED (Uniform Embedding Distortion) [8] and its improved version UERD(Uniform Embedding Revisited Distortion) [9] introduce the uniform embedding strategy in the framework of minimal distortion embedding, which enables the modification uniformly dispersed in the DCT coefficients, leading to less detectability of steganalysis significantly. The above algorithms have good performance in steganographic security. However, these algorithms define the distortion as the sum of embedding costs for individual image element, and ignore the interaction during the process of secret messages embedding. The consideration of influential factors about distortion designing is not comprehensive enough, and the definition of distortion function remains to be better.

Due to the correlation among image elements, during secret messages embedding, when one of image elements is modified, the statistical properties of other image elements will be affected. So it is unadvisable to simply define the embedding distortion as the sum of embedding costs for individual image element. In addition, the modern steganalysis schemes usually extract features that reflect the correlations among image elements. Therefore, the interaction among the image elements during secret message embedding should be taken into consideration.

Filler and Fridrich [10] first put forward the thought of dynamic update embedding distortion. Firstly, the distortion function is supposed as the sum of the costs(namely local potentials) for cliques(a set of pixels) .Then the STC codes for minimizing additive distortion can be used. Secondly, the cover image is divided into a series of sub-lattices. Cost assignment and secret message embedding are carried out sequentially in each sub-lattice. When secret message embedding is completed for a sub-lattice, use Gibbs construction to update the distortion in the remaining sub-lattices. By this means, the interaction among the image elements during secret message embedding is taken into account. CMD (Clustering

Modification Directions) [11] proposed by Bin Li is a kind of spatial steganography algorithm which can dynamic update embedding costs. It takes the modification direction of neighboring pixels into consideration when computing pixel distortion, updating the embedding costs dynamically and improving the resistance of steganalysis markedly. W. Tang et.al. propose CMD - C (Clustering Modification Directions for Color components) [12] for color components, which is the expansion of CMD. It divides cover image into a series of sub-images and embedding secret message successively. When computing embedding costs of a sub-image, the correlation both within and among color channels is taken into account. The algorithms above are all aimed at spatial images. However, since JPEG（Joint Photographic Experts Group）is a popular format for image storage and transmission, it is more widely used in our daily life. In this paper, we put forward a distortion update strategy(DUS) for JPEG, and implement an adaptive steganography method combined with the strategy. Firstly, we preprocess the cover image. Specifically, we divide the DCT coefficients of the cover image into several sub-images, and generate embedding sub-blocks based on sub-images. The secret messages are also divided into several parts corresponding to the number of embedding sub-blocks. Secondly, the embedding costs are initialed for cover image using well-known additive steganographic methods such as J-UNIWARD [5] and UED [8] so that STC codes can be employed. Then the first part of the secret messages is embedded into the first embedding sub-block of cover image using STC codes. Thirdly, when calculating the embedding costs of the rest embedding sub-blocks according to the scan sequence which is specified in advance, we consider the impacts caused by both inter- and intra-block neighboring DCT coefficients during embedding, and assign different weights for embedding costs according to DCT coefficients' properties. Then, Similarly, we use STC codes to embed the rest secret messages. Experimental results show that the proposed algorithm can effectively keep the correlation of DCT coefficients and gain a significant performance in the fight against the current state-of-the-art steganalyzers with high-dimensional features such as CC-JRM-22510D [13] and DCTR[14].

The main contributions of our paper are as follows.(1) A distortion update strategy(DUS) was put forward for ternary embedding considering mutual impacts of DCT coefficients, and it is able to increase the security of steganography. (2)The proposed method is so far the first attempt to consider mutual impacts during embedding in DCT domain.

The remainder of the paper is organized as follows. In Section 2, the minimal-distortion embedding framework and STC code are briefly reviewed. After that, we analyze the factors that affect embedding fluctuations and propose the distortion update strategy in Section 3. The proposed adaptive JPEG steganographic algorithm is presented in Section 4. Experiment results and analysis are included in Section5. Finally, the concluding remarks are drawn in Section 6.

2. Related Work

2.1 Minimal distortion embedding framework

In steganography, the transmitter hide secret messages into seemingly innocent media, such as digital images, so that she can communicate with the receiver without being perceived. By this means, it is not easy to distinguish the stego media from the cover one. The message is generally hidden (embedded) in the cover image by slightly modifying some individual elements of cover, such as LSBs of pixels and quantized DCT coefficients. The problem of minimizing the embedding impact for single-letter distortion is well formulated in [3]. Let

the binary vector $x=(x_1,x_2,...,x_n), y=(y_1,y_2,...,y_n)\in(0,1)^n$ and $m=(m_1,m_2,...,m_k)\in(0,1)^k$ represent the LSB of cover x, LSB of stego y and message m, respectively. We can define the additive cost function as

$$D(x,y)=\sum_{i=1}^{n}\rho_i(x,y_i) \tag{1}$$

where $\rho_i(x,y_i)$ represent the cost of changing the i th cover element x_i to y_i .With the syndrome coding, the minimal distortion embedding framework is formulated as

$$Emb(x,m)=\arg\min_{y\in C(m)} D(x,y) \tag{2}$$

$$and\ Hy=m \tag{3}$$

where H is parity-check matrix of the code C and $C(m)$ is the coset corresponding to syndrome m.

2.2 STC Code

There are many well-known steganographic codes in the minimal distortion embedding framework, such as Hamming code, BCH code and STC code. Among these codes, STC behaves the best. It enables embedding under additive distortion asymptotically approach the theoretical bound. Both the payload-limited sender (minimizing the total costs while embedding a fixed payload)and the distortion-limited sender (maximizing the payload while introducing a fixed total costs) are considered.

STC code is a special matrix embedding. Its main idea is using parity-check matrix H to establish the codes' graphical representation, namely syndrome trellis, and converting the problem of minimizing embedding costs into the problem of striving for the shortest path. The latter can be solved optimally through the Viterbi decoding algorithm. The embedding costs ρ_i can be defined according to the specific situation, without having to share them with the receiver. The parity-check matrix H is generated by jointing a small submatrix $\hat{H}$ of size $h\times w$ along the main diagonal. The submatrices $\hat{H}$ are placed next to each other and shifted down by one row leading to a sparse and banded H . The height h affects speed and efficiency of the algorithm, and the value of width w is determined by the embedding rate. The form of H was shown in **Fig. 1**.

$$\hat{H}=\begin{pmatrix}1&0\\1&1\end{pmatrix}\rightarrow H=\begin{pmatrix}1&0&&&&&&\\1&1&1&0&&&&\\&&1&1&&&&\\&&&&\ddots&&&\\&&&&&1&0&\\&&&&&1&1&1&0\end{pmatrix}$$

Fig. 1. The form of parity-check matrix H

3 Proposed Distortion Update Strategy

Most existing steganographic algorithms are based on the minimal-distortion embedding framework. They suppose that the image elements are independent of each other, and define distortion as the sum of embedding costs for individual image element, ignoring the mutual impacts during embedding. However, in the process of practical steganography, there is correlation among the image elements. The operation of embedding on an image element will affect the statistical features of other neighbouring elements, influencing the calculation

of embedding costs. In this section, we first analyze the factors that affect embedding fluctuations among DCT coefficients. Then we propose a distortion update strategy called DUS which is based on weight distribution for JPEG. The strategy is based on the correlation properties of JPEG and enables to dynamically update the embedding costs group by group.

3.1 Factors that Affect Embedding Fluctuations

In spatial image, there is strong correlation among adjacent pixels. After converted to JPEG images, this correlation will be largely retained. For spatial image, the pixel correlation mainly behaves between the center pixel and four-neighborhood pixels. And in the four-neighborhood pixels of the center pixel, the pixels at different location make approximately the same contribution to embedding fluctuation.

However, correlation of DCT coefficient in JPEG image is more complicated than the correlation of pixel in spatial image. The operation of block dividing makes JPEG images have not only the correlation in a block but also the correlation among blocks. The inter-block correlation mainly behaves as the correlation between the center DCT coefficient and four-neighborhood DCT coefficients. The intra-block correlation mainly behaves as the correlation between the center DCT coefficient and four DCT coefficients with the same frequency as center DCT coefficient in four-neighborhood blocks. In addition, due to the property of energy concentration for JPEG images, the contribution that DCT coefficients at different location make to embedding fluctuation is distinct. Therefore it is necessary to consider the location of DCT coefficient which affects the embedding fluctuation. In this subsection, two main factors are considered in our proposed distortion update strategy, i.e., the quantization step (QS), and the absolute value of the quantized DCT coefficient to be modified (VQ).

[1] quantization step (QS)

JPEG compression is an information-reducing operation. Quantization is essential for JPEG to control the compression rate. JPEG uses a quantization and rounding formula as follows

$$F_q(u,v) = \left\lfloor \frac{F(u,v)}{Q(u,v)} \right\rceil \tag{4}$$

In (4), the integer-valued coefficient $F_q(u,v)$ is the DCT coefficients after quantified, and $F(u,v)$ is the DCT coefficients before quantified. $Q(u,v)$ is a quantization table. $\lfloor x \rceil$ rounds the element x to its nearest integer. **Fig. 2** illustrates the standard JPEG quantization table corresponding to the quality factor (QF) of 80.

$$\begin{bmatrix} 6 & 4 & 4 & 6 & 10 & 16 & 20 & 24 \\ 5 & 5 & 6 & 8 & 10 & 23 & 24 & 22 \\ 6 & 5 & 6 & 10 & 16 & 23 & 28 & 22 \\ 6 & 7 & 9 & 12 & 20 & 35 & 32 & 25 \\ 7 & 9 & 15 & 22 & 27 & 44 & 41 & 31 \\ 10 & 14 & 22 & 26 & 32 & 42 & 45 & 37 \\ 20 & 26 & 31 & 35 & 41 & 48 & 48 & 40 \\ 29 & 37 & 38 & 39 & 45 & 40 & 41 & 40 \end{bmatrix}$$

Fig. 2. Standard JPEG quantization table corresponding to $QF = 80$

As seen in the **Fig. 2**, the quantization steps corresponding to different frequencies are different. Specifically, the quantization steps corresponding high frequencies are larger than those with the low frequencies. In addition, DCT transform is known to provide good decorrelation and energy compactification for images of natural scenes. After DCT transform, energy of an image is mainly focused on the dc coefficients and low frequency ac coefficients according to the zig-zag order. So we can conclude that the DCT coefficients which have smaller quantization step contain higher image energy. As a result, embedding secret information on the DCT coefficients which have smaller QS leads to larger image fluctuations.

[2] absolute value of the quantized DCT coefficient to be modified (VQ)

Image energy is not only related with the quantization step, but also related to the absolute value of the quantized DCT coefficient to be modified. The larger the absolute value of a quantized DCT coefficient is, the higher the image energy it contains. Therefore, embedding secret information on the DCT coefficients which have larger absolute value may lead to larger image fluctuations.

The quantized DCT coefficients of a 8×8 block in a JPEG image is shown in **Fig. 3**, which illustrates that the DCT coefficients with larger absolute value are distributed in the low frequency area of the block. It also shows that the quantized DCT coefficient value also reflects the energy of image. Thus we can obtain the relationship between QS and VQ, that is they have negative correlation. As a result, embedding secret messages on the DCT coefficients with larger VQ will cause larger image fluctuations.

$$\begin{bmatrix} -26 & -3 & -6 & 2 & 2 & -1 & 0 & 0 \\ 0 & -2 & -4 & 1 & 1 & 0 & 0 & 0 \\ -3 & 1 & 5 & -1 & -1 & 0 & 0 & 0 \\ -4 & 1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Fig. 3. The quantized DCT coefficients of a 8×8 block in a JPEG image

3.2 Proposed Distortion Update Strategy

Combining with the analysis of the factors that affect embedding fluctuations in the previous subsection, in this subsection, we propose the distortion update strategy. The main ideas of this strategy is dynamically update the embedding costs group by group and assign different weights for embedding costs according to the location of DCT coefficients, so as to maintain the correlations of the DCT coefficients.

The definition of embedding fluctuation in this paper is given below.

Definition:

Let the symbols $X=(x_{ij}), Y=(x_{ij})$ represent the cover and stego image. $D=Y-X=(d_{ij})$ represents the difference matrix. We discuss the ternary embedding case in this paper, where the magnitude of the change is limited to 1, so $d_{ij}\in\{+1,0,-1\}$. We define the embedding fluctuation caused by secret messages embedding as

$$\sigma_{ij} = \frac{d_{ij} \times |V_{ij}|}{q_{ij}} \tag{5}$$

where $|V_{ij}| / q_{ij}$ represents the weight used to measure the degree of the fluctuations. q_{ij} and $|V_{ij}|$ represents the QS and VQ for x_{ij}.

Suppose the embedding fluctuations' sum of x_{ij} and its both inter- and intra-block neighboring DCT coefficients is W. In order to keep the correlation among the DCT coefficients after embedded, the value of W should be as small as possible. As proved in the following formula (For simplicity, we take inter-block neighboring DCT coefficients as example, the proof process of intra-block is similar to it).

$$\begin{aligned} &\min W = |\sigma_{i-1,j} - \sigma_{ij}| + |\sigma_{i,j-1} - \sigma_{ij}| + |\sigma_{i,j+1} - \sigma_{ij}| + |\sigma_{i+1,j} - \sigma_{ij}| \\ &\Rightarrow (\sigma_{i-1,j} - \sigma_{ij})^2 + (\sigma_{i,j-1} - \sigma_{ij})^2 + (\sigma_{i,j+1} - \sigma_{ij})^2 + (\sigma_{i+1,j} - \sigma_{ij})^2 \\ &= 4\sigma_{ij}^2 - 2\sigma_{ij}(\sigma_{i-1,j} + \sigma_{i,j-1} + \sigma_{i,j+1} + \sigma_{i+1,j}) + (\sigma_{i-1,j}^2 + \sigma_{i,j-1}^2 + \sigma_{i,j+1}^2 + \sigma_{i+1,j}^2) \end{aligned} \tag{6}$$

Suppose the above formula is conducted when the embedding operation of x_{ij}'s neighboring DCT coefficients has completed. So only σ_{ij} is unknown in the formula, the rest can be regarded as constants stabilizing the numerical calculations. Therefore, when W takes the minimum value, the value of σ_{ij} is as follows:

$$\sigma_{ij} = \frac{1}{4}(\sigma_{i-1,j} + \sigma_{i,j-1} + \sigma_{i,j+1} + \sigma_{i+1,j}) \tag{7}$$

Considering both inter- and intra-block neighboring DCT coefficients, we obtain the final value of σ_{ij} is as follows:

$$\sigma_{ij} = \frac{1}{4}(\sigma_{i-1,j} + \sigma_{i,j-1} + \sigma_{i,j+1} + \sigma_{i+1,j} + \sigma_{i-8,j} + \sigma_{i,j-8} + \sigma_{i,j+8} + \sigma_{i+8,j}) \tag{8}$$

Since the weight $|V_{ij}| / q_{ij}$ is positive, for ternary embedding, the sign of σ_{ij} should be the same as the direction of modification. Here the direction means the choice of positively or negatively changing the intensity of a DCT coefficient. That is, when the value of W is positive, negative or zero, accordingly, d_{ij} is $+1$、-1、0, respectively.

Through the above analysis, we put forward the following embedding solution:

Firstly, the DCT coefficients of the cover image are divided into several sub-images, then the embedding sub-blocks is obtained based on sub-images. Accordingly, the secret messages are also divided into several parts corresponding to the number of embedding sub-blocks. The first segment of the secret messages is embedded into the first part of the cover image according to the initial additive steganographic method such as UED [8]. Secondly, the embedding costs of the DCT coefficients in other embedding sub-blocks are updated according to the sub-blocks that have already been embedded. Next, the remaining message secret messages are sequentially embedded into the remaining parts of the cover image with the updated costs in sequence.

The detail of DUS is as follows:

Supposed the DCT coefficients of the cover image are divided into n embedding sub-blocks which is denoted by S_t, $t \in \{1,2,...,n\}$. The initial additive steganographic method is denoted by $F = (f_{ij})$. Take ternary embedding as example. The embedding cost of the DCT coefficients at the location of (i, j) is $\rho_{ij} = (\rho_{ij}^{+}, \rho_{ij}^{-}, \rho_{ij}^{0})$, where ρ_{ij}^{+}、ρ_{ij}^{-}、ρ_{ij}^{0}

represent the embedding cost when d_{ij} is $+1$、-1、0, respectively, $\rho_{ij}^{0}=0$.

1) If $t=1$, set $\rho_{ij}^{+}=\rho_{ij}^{-}=f_{ij}$.

2) Otherwise, update the embedding costs according to $D=Y-X$. We use

$$\rho_{ij}^{+}=\begin{cases} f_{ij}/\alpha & \sum_{d_{ia}\in N_{ia}}\left(\frac{d_{ia}\times|V_{ia}|}{q_{ia}}+\frac{d'_{ir}\times|V_{ir}|}{q_{ir}}\right)>0 \\ f_{ij} & otherwise \end{cases} \tag{9}$$

$$\rho_{ij}^{-}=\begin{cases} f_{ij}/\alpha & \sum_{d_{ia}\in N_{ia}}\left(\frac{d_{ia}\times|V_{ia}|}{q_{ia}}+\frac{d'_{ir}\times|V_{ir}|}{q_{ir}}\right)<0 \\ f_{ij} & otherwise \end{cases} \tag{10}$$

For any $d_{ir}\in N_{ir}$, we set

$$d'_{ir}=\frac{1}{4}\sum_{d_{irr}\in N_{irr}} d_{irr} \tag{11}$$

where α is a scaling factor, $N_{ia}=\{d_{i+1,j},d_{i-1,j},d_{i,j+1},d_{i,j-1}\}$ represents the four-neighborhood DCT coefficients of d_{ij}, as shown in **Fig. 4**. $N_{ir}=\{d_{i+8,j-8},d_{i-8,j-8},d_{i+8,j+8},d_{i-8,j+8}\}$ represents the DCT coefficients with the same frequency as d_{ij} in four-neighborhood blocks, $N_{irr}=\{d_{i+1,r},d_{i-1,r},d_{i,r+1},d_{i,r-1}\}$ represents the four-neighborhood DCT coefficients of d_{ir}.

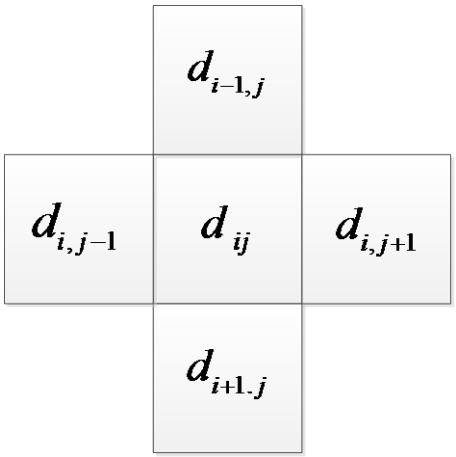


Fig. 4. The four-neighborhood DCT coefficients of d_{ij}

Through the above strategy, the modification direction of the center DCT coefficient will tend to be the same as the fluctuation direction of the neighboring DCT coefficients. So as to achieve the aim of improving the ability of resist steganalysis.

4 The Proposed Dus Algorithm

Combining with the DUS strategy in the above section, we propose an adaptive JPEG steganographic method based on weight distribution for embedding costs in this section. The

algorithm takes the interaction during embedding into account. The algorithm is mainly divided into three parts. The first part is the original image preprocessing. Firstly, we divide the cover image into several sub-images, and generate embedding sub-blocks based on sub-images. The secret messages are also divided into several parts corresponding to the number of embedding sub-blocks. The second part is embedding the first part of the secret message into the first embedding sub-block of cover image according to the initial additive steganographic method such as UED [8]. In the third part, the remaining message secret messages are sequentially embedded into the remaining parts of the cover image with the updated costs in sequence. At the end of this section, we set an example to visualize the process of updating costs in the algorithm.

4.1 Secret Messages Embedding

The detailed steps of the proposed algorithm are as follows.

Part 1: Preprocessing.

Step 1: For JPEG image, entropy decoding is applied to generate the quantized DCT coefficients.

Step 2: Supposed the size of cover image is $n_1 \times n_2$, divide the DCT coefficients of the cover image into disjoint sub-images sized $L_1 \times L_2$, where $L_1, L_2 \geq 1$. **Fig. 5** is an example of the division of an 4×4 image into 2×2 disjoint sub-images.

$x_{1,1}$	$x_{1,2}$	$x_{1,3}$	$x_{1,4}$
$x_{2,1}$	$x_{2,2}$	$x_{2,3}$	$x_{2,4}$
$x_{3,1}$	$x_{3,2}$	$x_{3,3}$	$x_{3,4}$
$x_{4,1}$	$x_{4,2}$	$x_{4,3}$	$x_{4,4}$

Fig. 5. An example of the division of an 4×4 image into 2×2 disjoint sub-images

Step 3: Generate embedding sub-blocks based on sub-images. For instance, in **Fig. 6**, four embedding sub-blocks are generated based on sub-images in **Fig. 5**. The formula of generating embedding sub-blocks can be represented by

$$\begin{aligned} S_{a,b} &= \{(i,j) | i = a + \tau_a L_1, j = b + \tau_b L_2\} \\ a &= \{1,\ldots,L_1\}, \tau_a \in \left\{0,1,\ldots,\left\lfloor \frac{n_1}{L_1} \right\rfloor - 1\right\} \\ b &= \{1,\ldots,L_2\}, \tau_b \in \left\{0,1,\ldots,\left\lfloor \frac{n_2}{L_2} \right\rfloor - 1\right\} \end{aligned} \tag{12}$$

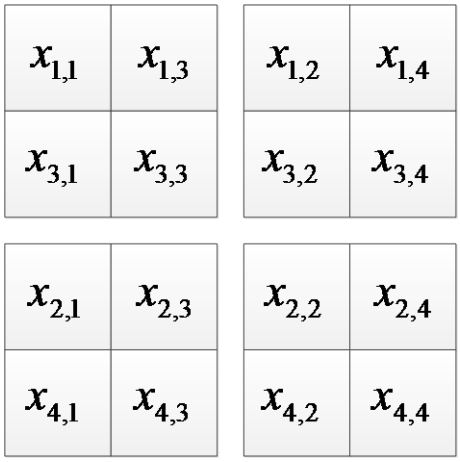


Fig. 6. An example of generating embedding sub-blocks

Step 4: Divide the secret messages m into $L_1 \times L_2$ parts. Each part contains $m/(L_1 \times L_2)$ bits.

Step 5: Determine the embedding sequence for the embedding sub-blocks. For convenience, we choose a horizontal zig-zag order as the embedding order as shown in **Fig. 7**.

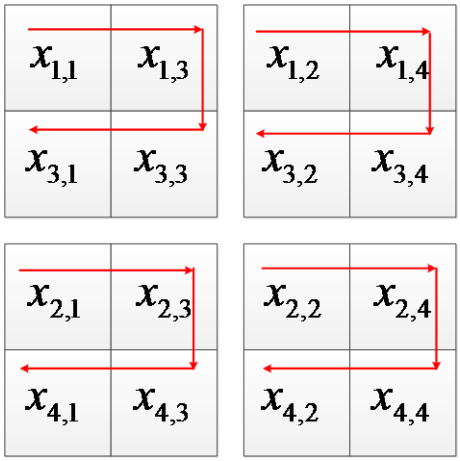


Fig. 7. An example of the embedding order

we denote the embedding sub-blocks by $S_t, t \in \{1,2,...,L_1 \times L_2\}$.

Part 2: Initial the embedding costs

Step 6: Set the initial conditions. Start with $t=1, Y=X, D=Y-X$ .Determine the initial distortion function. For example, choose ternary UED[8] as the initial distortion function as follows.

$$\rho_{ij}^{n_1 \times n_2} = \sum_{p_{ia} \in P_{ia}} \left(|c_{ij}| + |p_{ia}| + \alpha_{ia}\right)^{-1} + \sum_{p_{ir} \in P_{ir}} \left(|c_{ij}| + |p_{ir}| + \alpha_{ir}\right)^{-1} \tag{13}$$

where $P_{ia} = \{c_{i+1,j}, c_{i-1,j}, c_{i,j+1}, c_{i,j-1}\}$ and $P_{ir} = \{c_{i+8,j}, c_{i-8,j}, c_{i,j+8}, c_{i,j-8}\}$ denote the inter- and intra-four-neighborhood DCT coefficients of c_{ij} ,respectively. α_{ia} and α_{ir} are scaling factor determined by experiment.

Step 7: Embed the first part of the secret message into the first embedding sub-block of cover image according to the initial embedding costs.

Part 3: Embed the remaining data

Step 8: Update the embedding costs using DUS and embed the remaining data according to the scan sequence which is specified in advance using STC codes. Considering the boundary DCT coefficients without four-neighborhood, we pad the DCT coefficients of cover image before costs updating.

Step 9: Repeat this embedded operating until $t = L_1 \times L_2$, then output the stego image Y.

4.2 Secret Messages Extraction

The detailed steps of secret messages extraction are as follows.

Step 1: For a stego JPEG image, the quantized DCT coefficients are applied to generate the quantized DCT coefficients.

Step 2: Generate embedding sub-blocks S_t based on sub-images, $t \in \{1,2,...,L_1 \times L_2\}$.

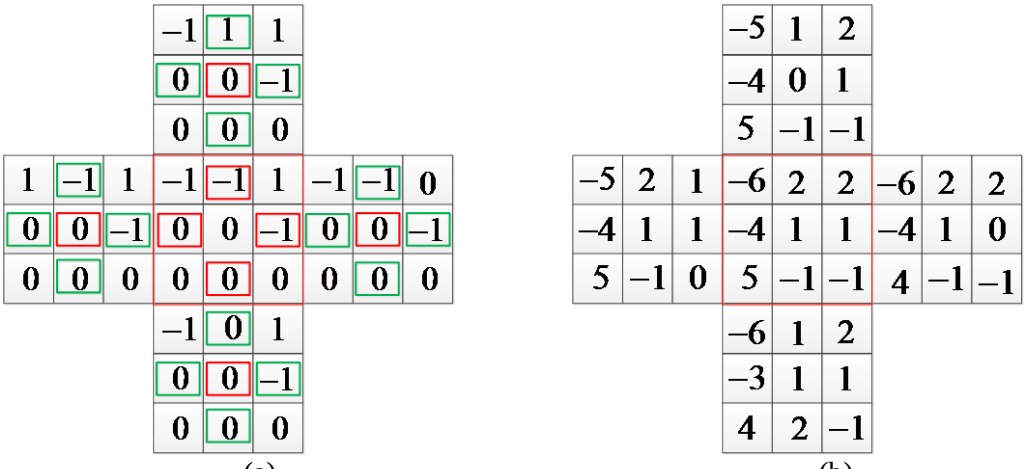
Step 3: For each embedding sub-blocks, using $m_t = HS_t^T$ to extract the secret messages until all the secret messages are extracted.

Step 4: Put the secret messages together and obtain the original secret messages m.

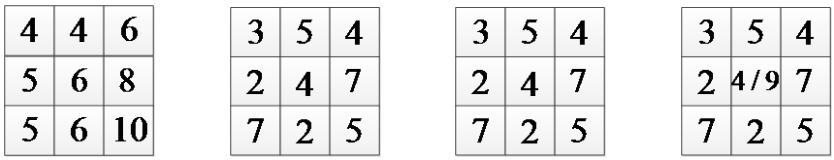
4.3 An Example of Updating Costs

As an example, **Fig. 8** gives a detailed explanation about how to embed the secret message bits using DUS strategy. In practical, we choose $L_1 = L_2 = 8$ as the size of the sub-image because the size of JPEG's sub-block is 8×8. However, for simplicity, we suppose $L_1 = L_2 = 3$ in this example, we also suppose the size of quantization table is 3×3.

According to the zig-zag order, suppose the DCT coefficients in S_1, S_2, S_3 and S_4 have already been embedded, and it is S_5's turn. **Fig.8(a)** and **(b)** shows the difference matrix D and the value of quantized DCT coefficients to be modified, respectively. **Fig.8(c)** and **(d)** shows the QS and the initial costs F. According to the formula of DUS in Eq.(9) and(10), we obtains the calculation result in Eq.(14). Suppose $\alpha = 9$. It can be seen that the result is negative, therefore, the $\rho_{2,2}^-$ will be replaced by $\rho_{2,2}^- / 9$. **Fig.8(e)** and **(f)** shows the ρ^+ and ρ^- after the initial cost $f_{2,2}$ is updated.



(a) (b)



(c) (d) (e) (f)

Fig. 8. An example of updating costs. (a) and (b) are the difference matrix D and the value of quantized DCT coefficients to be modified. (c) and (d) are the QS and the initial costs F. (e) and (f) are the ρ^{+} and ρ^{-} after the initial cost $f_{2,2}$ is updated.

$$\begin{aligned}
&\sum_{d_{ia}\in N_{ia}}\left(\frac{d_{ia}\times|V_{ia}|}{q_{ia}}+\frac{d'_{ir}\times|V_{ir}|}{q_{ir}}\right)\\
&=\frac{-1\times 2}{4}+\frac{-1\times 1}{8}+\frac{0\times|-1|}{6}+\frac{0\times|-4|}{5}+\frac{\frac{1}{4}(1-1+0+0)\times 0}{6}+\\
&\frac{\frac{1}{4}(-1-1+0+0)\times 1}{6}+\frac{\frac{1}{4}(0-1+0+0)\times 1}{6}+\frac{\frac{1}{4}(-1-1+0+0)\times 1}{6}\\
&=-\frac{5}{6}<0
\end{aligned} \tag{14}$$

5 Experiment Results And Analysis

In this section, firstly, we determined the optimal scaling factor through experiments. Then experimental results and analysis are presented to demonstrate the feasibility of the proposed JPEG steganographic scheme.

5.1 Experiment Setup

A set of 10000 uncompressed gray images of size 512×512 pixels from BOSSbase[15] database is used in our experiments. Then the images are JPEG compressed by quality factors 75, 85 and 95. The content of the image is varied, including landscapes, people, animals and plants. We test the steganographic scheme for different payloads (0.05 to 0.5 bpac). Secret message bits is randomly generated.

We compare our steganographic scheme with several well-known steganographic schemes, such as nsF5 [16], ternary UED[8], J-UNIWARD[5]. And the powerful steganalyzer CC-JRM[13] developed by Kodovský and Fridrich is used for experiments, which includes 22510 both integral and DCT-mode specific features. Besides, DCTR-8000[14] is employed to demonstrate the security performances of the proposed JPEG steganographic schemes. The ensemble classifier[17] is incorporated in our experiments, since it enables fast and automatic training in high-dimensional feature spaces. The P_E (the minimum error probability under equal priors) is calculated as follows.

$$P_E=\min_{P_{FA}}\frac{1}{2}(P_{FA}+P_{MD}(P_{FA})) \tag{15}$$

where P_{FA} and P_{MD} represent the probabilities of false alarms and missed detection, respectively.

5.2 Impact of the Scaling Factor

In order to obtain the optimal scaling factor, we vary the value of the scaling factor α under the condition of $L_1 = L_2 = 8$ for UED-DUS and J-UNI-DUS. The steganalyzers used in the experiment are CC-JRM and DCTR, respectively. The results of the classification error are shown in **Fig. 9** and **Fig. 10**. It can be noted that the scaling factor which performs the best does not varies significantly for different initial distortion function and different steganalyzers. We can observed that in the range of $\alpha = 3 \sim 15$, there is a peak value of classification error at the position of $\alpha = 9$. So the optimal scaling factor α is obtained when $\alpha = 9$

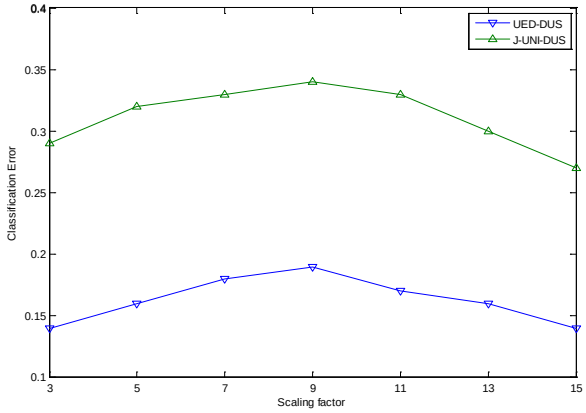


Fig. 9. Classification error(CC-JRM) for UED-DUS and J-UNI-DUS with different scaling factors (Payload=0.3bpac,QF=75) .

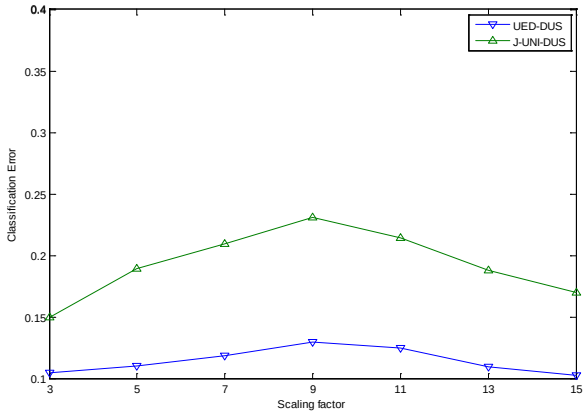
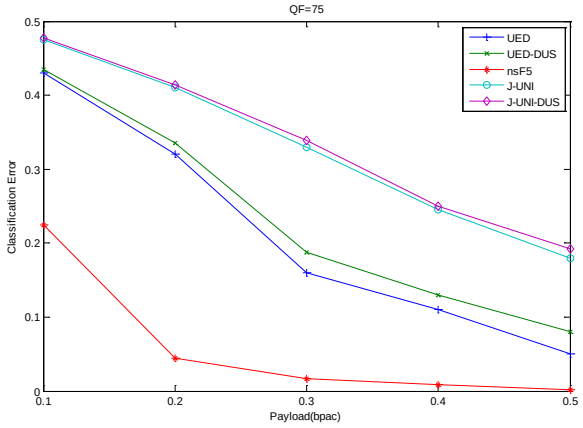


Fig. 10. Classification error(DCTR) for UED-DUS and J-UNI-DUS with different scaling factors(Payload=0.3bpac,QF=75).

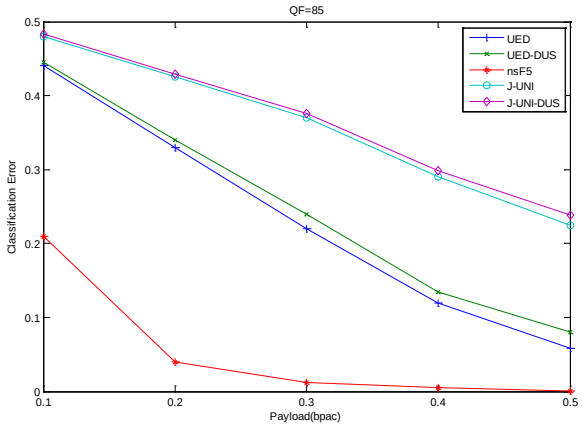
5.3 Comparison to State-of-the-Art Steganographic Methods

In this subsection, we compare our steganographic schemes UED-DUS and J-UNI-DUS with the non-adaptive steganographic schemes nsF5 and adaptive steganographic schemes ternary UED and J-UNIWARD. The security performances of the proposed schemes against the

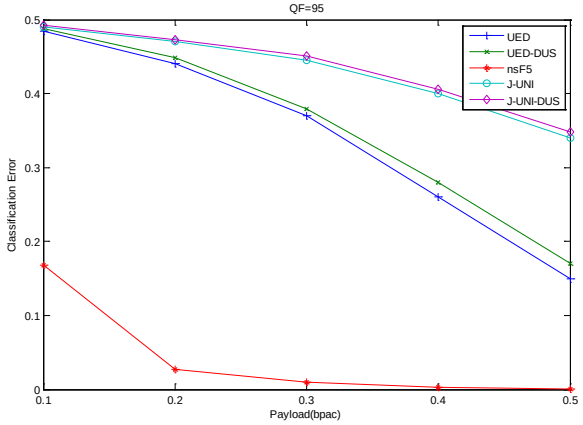
CC-JRM and DCTR, for JPEG quality factors 75, 85 and 95, are illustrated in **Fig. 11** and **Fig. 12**. We can see from the figures that for all cases, J-UNI-DUS has the best security performance which gives a slightly better performance than J-UNIWARD by a sizeable margin across all three quality factors. And these two methods obviously outperform the rest of the steganographic methods. We can conclude that the proposed strategy DUS can indeed improve the security performance of the original distortion function. J-UNIWARD performs well may because it can embed secret messages in all DCT coefficients, including DC and zero AC coefficients, so it is difficult for conventional steganalyzers to extract features. It is also noted that UED-DUS has a higher level of statistical undetectability than UED especially for large data payload ($\geq$0.4 bpac). The reason may be that with the increase of data payload, our proposed strategy can better keep the correlation of JPEG images, therefore lead to better security performance. In addition, for nsF5, the detection accuracy of CC-JRM is almost at the same level as DCTR, and the classification error of these two steganalyzers for nsF5 is the lowest because nsF5 is a non-adaptive method.



(a)

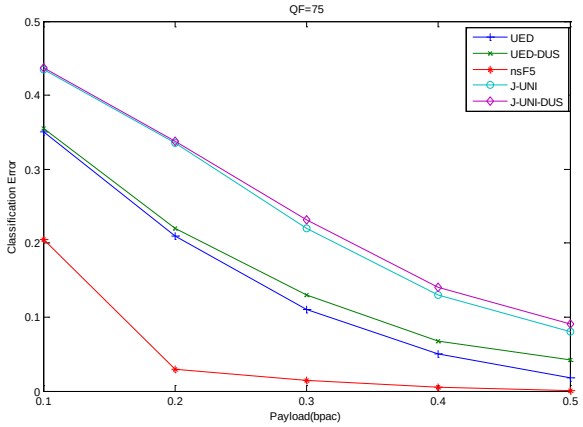


(b)

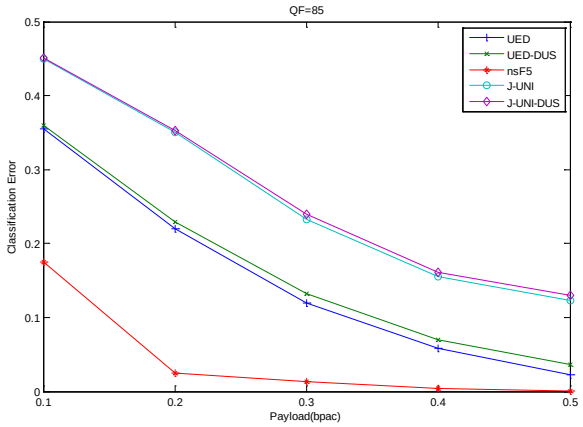


(c)

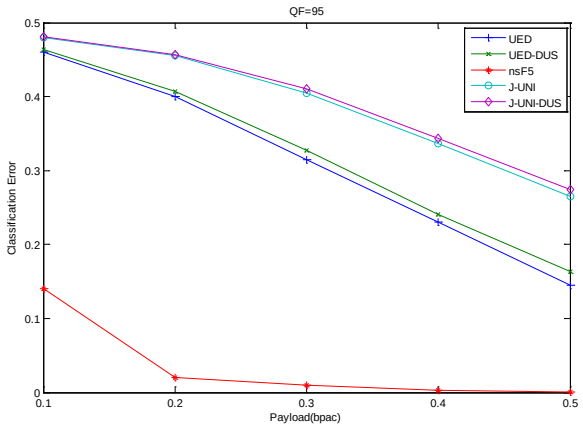
Fig. 11. Classification error for UED-DUS, J-UNI-DUS, nsF5, UED, and J-UNI with CC-JRM and ensemble classifier for (a) QF = 75, (b) QF = 85 and (c) QF = 95. (ternary STC coded)



(a)



(b)



(c)

Fig. 12. Classification error for UED-DUS, J-UNI-DUS, nsF5, UED, and J-UNI with DCTR and ensemble classifier for (a) QF = 75, (b) QF = 85 and (c) QF = 95. (ternary STC coded)

6. Conclusion

In this paper, we put forward a distortion update strategy(DUS) for JPEG, which takes mutual impacts during embedding in consideration. Then we implement an adaptive steganography method combined with the strategy. Firstly, the DCT coefficients of the cover image are divided into several sub-images, then the embedding sub-blocks is obtained based on sub-images. Secondly, The first segment of the secret messages is embedded into the first part of the cover image according to the initial additive steganographic method such as UED and J-UNIWARD. Then, the embedding costs of the DCT coefficients in other embedding sub-blocks are updated according to the sub-blocks that have already been embedded. Thirdly, the remaining message secret messages are sequentially embedded into the remaining parts of the cover image with the updated costs in sequence.

Experiments show that the proposed method can obviously improve the security performance of the well-known additive schemes for JPEG. It can effectively keep the correlation of DCT coefficients and has a higher level of statistical undetectability in the fight against the current state-of-the-art steganalyzers with high-dimensional features. In future work, we are going to research embedding schemes with larger magnitudes such as pentary embedding and consider more factors that affect embedding fluctuations among JPEG coefficients.

References

[1] Sedighi V, Cogranne R and Fridrich J, “Content-Adaptive Steganography by Minimizing Statistical Detectability,” *IEEE Transactions on Information Forensics and Security*, vol.11, no.2, pp. 221-234, 2016. Article (CrossRef Link)

[2] Song X, Liu F, Yang C, et al, "Steganalysis of adaptive JPEG steganography by selecting DCT coefficients according to embedding distortion," *KSII Transactions on Internet And Information Systems*, vol.9, no.12, pp. 5209-5228, 2015. Article (CrossRef Link)

[3] Filler T, Judas J, and Fridrich J, "Minimizing additive distortion in steganography using syndrome-trellis codes," *IEEE Transactions on Information Forensics and Security*, vol.6, no.3, pp. 920- 935, 2011. Article (CrossRef Link)

[4] Holub V and Fridrich J, "Designing steganographic distortion using directional filters," in *Proc. of the IEEE Workshop on Information Forensic and Security*, Tenerife, Spain, pp.234–239, 2012.Article (CrossRef Link)

[5] Holub V and Fridrich J, "Digital image steganography using universal distortion," in *Proc. of 1st ACM Workshop on Information Hiding and Multimedia Security*, Montpellier, France, pp.59–68, 2013. Article (CrossRef Link)

[6] B. Li, M. Wang, J. Huang, and X. Li, "A new cost function for spatial image steganography," in *Proc. of the IEEE International Conference on Image Processing*, Pairs, France, pp.4206–4210, 2014. Article (CrossRef Link)

[7] Sedighi V, Fridrich J and Cogranne R, "Content-adaptive pentary steganography using the multivariate generalized Gaussian cover model," in *Proc. of IS&T/SPIE Electronic Imaging. International Society for Optics and Photonics*, pp.94090H-94090H, March, 2015.
Article (CrossRef Link)

[8] Guo L, Ni J and Shi Y Q, "Uniform embedding for efficient JPEG steganography," *IEEE Transactions on Information Forensics and Security*, vol.9, no.5, pp. 814- 825, 2014.
Article (CrossRef Link)

[9] Guo L, Ni J, Su W, et al, "Using Statistical Image Model for JPEG Steganography: Uniform Embedding Revisited," *IEEE Transactions on Information Forensics and Security*, vol.10, no.12, pp. 2669-2680, 2015. Article (CrossRef Link)

[10] Filler T and Fridrich J, "Gibbs construction in steganography," *IEEE Transactions on Information Forensics and Security*, vol.5, no.4, pp. 705-720, 2010. Article (CrossRef Link)

[11] B. Li, M. Wang, J. Huang, and X. Li, "A Strategy of Clustering Modification Directions in Spatial Image Steganography," *IEEE Transactions on Information Forensics and Security*, vol.10, no.9, pp. 1905-1917, 2015.Article (CrossRef Link)

[12] Tang W, Li B, Luo W, et al, "Clustering Steganographic Modification Directions for Color Components," *IEEE Signal Processing Letters*, vol.23, no.2, pp. 197-201, 2016.
Article (CrossRef Link)

[13] Kodovský J and Fridrich J, "Steganalysis of JPEG images using rich models," *IS&T/SPIE Electronic Imaging*, I*nternational Society for Optics and Photonics*, pp.83030A-83030A, February, 2012. Article (CrossRef Link)

[14] Holub V and Fridrich J, "Low-complexity features for JPEG steganalysis using undecimated DCT," *IEEE Transactions on Information Forensics and Security*, vol.10, no.2, pp. 219-228, 2015. Article (CrossRef Link)

[15] Bas P, Filler T and Pevný T, "Break Our Steganographic System: The Ins and Outs of Organizing BOSS," in *Proc. of International Workshop on Information Hiding*, Springer Berlin Heidelberg, pp.59-70, May, 2011.Article (CrossRef Link)

[16] Fridrich J, Pevný T and Kodovský J, "Statistically undetectable jpeg steganography: dead ends challenges, and opportunities," in *Proc. of the 9th workshop on Multimedia & security*, *ACM*, pp.3-14, September, 2007.Article (CrossRef Link)

[17] Kodovsky J, Fridrich J, and Holub V, "Ensemble classifiers for steganalysis of digital media," *IEEE Transactions on Information Forensics and Security*, vol.7, no.2, pp. 432-444, 2012. Article (CrossRef Link)

Yi Sun received the B.S. degree in electronic science and technology from Zhengzhou information science and technology institute, Henan, China, in 2015. She is pursuing the M.S. degree in information security at Zhengzhou information science and technology institute. Her research interests include information hiding and information security.

Guangming Tang received the B.S., M.S. and Ph.D degrees in information security from Zhengzhou information science and technology institute, Henan, China, in 1983, 1990, and 2008, respectively. She is now a professor at the Department of Information Security, Zhengzhou information science and technology institute. Her research interests include information hiding, watermarking and software reliability. She has published 60 research articles and 3 books in these areas.

Yuan Bian received the B.S. degree in electronic science and technology from Zhengzhou information science and technology institute, Henan, China, in 2014. She is pursuing the M.S. degree in information security at Zhengzhou information science and technology institute. Her research interests including information hiding and information security.

Xiaoyu Xu received the B.S. degree in electronic science and technology from Zhengzhou information science and technology institute, Henan, China, in 2015. He is pursuing the M.S. degree in information security at Zhengzhou information science and technology institute. His research interests include deep learning and steganalysis.