A Robust Image Steganography Method Resistant to Scaling and Detection

Yue Zhang[1,3], Xiangyang Luo[1,3], Jinwei Wang[2], Chunfang Yang[1,3], Fenlin Liu[1,3]

[1] State Key Laboratory of Mathematical Engineering and Advanced Computing, China
[2] School of Computer and Software, Nanjing University of Information Science and Technology, China
[3] Zhengzhou Science and Technology Institute, China
yue_zhang95@126.com, luoxy_ieu@sina.com, wjwei_2004@163.com,
chunfangyang@126.com, liufenlin@vip.sina.com

Abstract

The current image steganography algorithms mainly focus on the anti-detectability rather than the robustness to scaling attacks. Therefore, it is difficult to extract the secret messages correctly after stego images subject to scaling attacks. To this end, an image steganography method for the nearest-neighbor interpolation method in image scaling is proposed, which can resist both scaling attack and statistical detection. First, the principle of nearest-neighbor interpolation method is analyzed and summarized, which is using the resized pixel coordinates to find the original adjacent pixels, and obtaining the weights of the adjacent original pixels by the distance between resized pixel and the original adjacent pixels, finally calculating the resized pixel value. Second, the scaling invariant pixels are extracted using the principle of nearest-neighbor interpolation method to generate a new cover image. Then the distortion functions in WOW, S-UNIWARD and MiPOD are used to calculate the new cover's distortion to minimize the distortion embedding using STCs coding. Finally, resize the stego image to the original size. The steganalysis experiments based on BossBase-1.01 image library and SPAM, maxSRM features demonstrate that the proposed method has good resistance of scaling attack and Statistical detection under various scaling factors and payloads.

Keywords: Image steganography, Scaling attack resistant, Statistical detection resistant, Nearest-neighbor interpolation method, Scaling invariant pixels

1 Introduction

Information steganography technology achieves covert communication by hiding the secret messages in the multimedia file. At present, the main image-based steganography algorithms achieve a high resistance of detection by minimizing the embedded distortion. However, these algorithms usually take no account of image processing attacks such as image compression, scaling, and noise suppression when the stego images are transmitted over the open channel. As we know, the widespread use of intelligent mobile terminals such as mobile phones, tablet PCs makes the multimedia file collection and transmission more and more convenient and covert communication based on the multimedia file more and more common. However, the challenges also are brought [1]. In order to save bandwidth, improve storage and transmission efficiency, intelligent mobile terminals and network service providers tend to file compression, scaling and other processing operations, which results in information loss. If the current steganography algorithms are applied directly to the intelligent device to achieve information steganography, it is often difficult to extract the embedded secret messages completely from the stego images. Therefore, the steganography technology based on intelligent terminal has to ensure not only its resistance of statistical detection, but also its robustness to image processing operations. This article focuses on such steganography method that can resist both scaling attack and statistical detection simultaneously.

In terms of anti-detection, the current steganography algorithms design the distortion function to calculate the pixel distortion caused by change, and then use the STCs (Syndrome-Trellis Codes) [2] to select the position with small distortion to embed the messages, so as to achieve higher resistance of statistical detection. In recent years, with the rapid development of adaptive steganography, the designs of distortion function are also varied. A typical spatial domain steganography algorithm such as HUGO (Highly-Undetectable Stego) [3] is proposed to improve the resistance of statistical detection by keeping the high-dimensional statistical model of cover images. WOW (Wavelet Obtained Weights) [4] algorithm uses the image wavelet decomposition coefficient to calculate the pixel embedding distortion, which can resist the detection of rich model effectively. S-UNIWARD

*Corresponding Author: Xiangyang Luo; E-mail: luoxy_ieu@sina.com
DOI: 10.3966/160792642018031902029

(Spatial Universal Wavelet Relative Distortion) [5] algorithm is improved on the basis of WOW, and the resistance of statistical detection is further enhanced. There are also HILL (High-pass, Low-pass, and Low-pass) [6], MiPOD (Minimizing the Power of Optimal Detector) [7] and so on. Adaptive steganography algorithm in JPEG domain such as UED (Uniform Embedding Distortion) [8] as well as J-UNIWARD (JPEG Universal Wavelet Relative Distortion) [5], etc. These steganographic algorithms have been greatly improve the detection resistant. However, the experimental results show that the algorithms result in plenty of extraction errors after the stego images subject to scaling attack.

Scaling attack is focused on the image watermarking field to improve the robustness of watermarking messages. Common watermarking algorithms resistant to scaling attack are based on geometric invariants [9-10], time-frequency transforms [11-12], image feature points [13-14], quantization index modulation [15-16] and so on. For example, Kim B. S [9] proposed a watermarking algorithm by using logarithmic polar coordinates in spatial domain to provide scaling invariance, which is robust to RST (Rotation, Scaling, Translation) attacks. Literature [12] pointed out that the image scaling processing was similar to discrete wavelet transform. Embedding the watermark message in the approximate coefficient of the wavelet transform can make the algorithm more robust to the scaling attack. In literature [14], the feature points were extracted by the Harris detector and the watermark message was embedded by the image time-frequency transform. When the watermarking image suffered 0.8 times scaling attack, the correct extraction rate was still 93.75%. Zareian and Tohidypour [16] combined image transformation and quantization modulation, making the watermark message still be correctly extract under the 0.5 times scaling attack. All the algorithms above embed the massages into the domain which is insensitive to scaling, and adopt the embedding algorithm of scaling resistant, which improve the robustness of the algorithm greatly to various image processing attacks such as scaling. However, if the algorithms are applied directly to the steganography field, only a few algorithms can ensure to extract the embedded massage correctly after scaling attack. In the other hand, most of watermarking algorithms improve the robustness by modifying the main contents of cover image, which often results in relatively large distortion, so the resistance of statistical detection is poor. Besides the image watermarking field, scaling attacks has also been studied in the field of image recognition and detection [17-21] and image representation [22-23], mainly used to improve the accuracy of identification and detect illegal copying of images.

In addition to the above methods, it has not be seen the steganographic method that resisted both scaling attack and statistical detection in the existing literature. In view of the effect of image processing attacks on steganography algorithm, our group has proposed image steganography algorithm which can resist both JPEG-compression attack and statistical detection [24-25]. The main idea is to improve the robustness of stego image to JPEG-compression attack while ensuring the detection resistant. However, the methods still can't resist scaling attacks.

Therefore, this paper proposes an image steganography method that can resist both scaling attack and statistical detection. The most common interpolation method, nearest-neighbor interpolation method, is used to find the adjacent original pixels by resized pixel coordinates in this paper, and obtain the weights of the resized pixels by the distance between resized pixel and the adjacent original pixels. Then extract the scaling invariant pixels according to the different scaling factors, and combine the WOW, S-UNIWARD and MiPOD distortion function and STCs encoding to minimize the embedding distortion. It can achieve not only the resistance of scaling attack, but also the resistance of statistical detection.

The remainder of this paper is organized as follows. The second section describes the principle of image scaling and its effect on steganography briefly. The third section elaborates the principle frame and the main steps of the proposed method. The fourth section gives the experimental results and this paper ends in fifth section.

2 Analysis of Scaling Principle and Effect on Steganography

This section mainly introduces the scaling principle of the nearest-neighbor interpolation method applied in this paper, and the effect of image scaling processing on steganography. By analyzing the principle of the nearest- neighbor interpolation method, the adaptive image steganography method is proposed to extract the scaling invariant pixels and realize the scaling resistant.

2.1 Analysis of Scaling Principle

Scaling is one way of image processing, the vast majority of editing software has image scaling function. For the spatial image, the scaling changes the image size by changing the number of pixels. In this section, traditional interpolation method are analyzed, and the principle of the methods are summed up as shown in Figure 1.

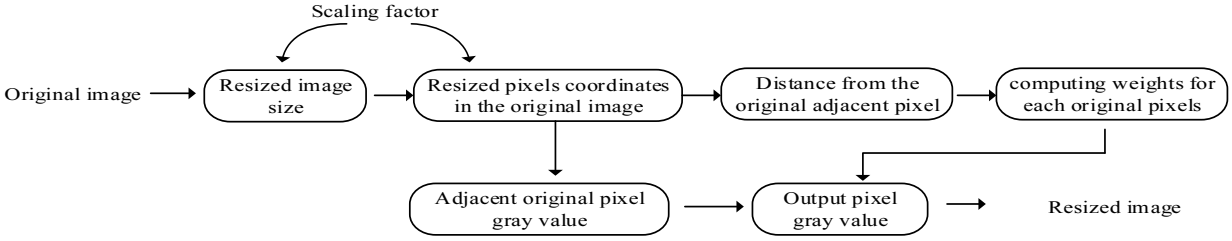

Figure 1. Interpolation algorithm schematic

Hypothesis the original image is $\mathbf{X}$, whose size is $m \times n$. The scaling factor is s. The resized image is $\mathbf{X}_s$, whose size $m_s \times n_s$ is first obtained by the original image size $m \times n$ and the scaling factor s, where m_s and n_s are the width and height of the resized image. $p_{(i,j)}^{(s)}$ represents the pixel of resized image, whose coordinate is (i, j) and the scaling factor is s, where $i=1,2,...,m_s$, $j=1,2,...,n_s$. Then the coordinate $\left(x_i^{(s)}, y_j^{(s)}\right)$ of each resized pixel in the original image pixel coordinate system is shown in the following formula.

$$\left(x_i^{(s)}, y_j^{(s)}\right)=\left(\frac{s+(2i-1)}{2s}, \frac{s+(2j-1)}{2s}\right) \quad \textbf{(1)}$$

According to each resized pixel coordinate in formula(1), the four adjacent original pixels p_k, where $k=\left(\left\lfloor x_i^{(s)}\right\rfloor, \left\lfloor y_j^{(s)}\right\rfloor\right)$, $\left(\left\lfloor x_i^{(s)}\right\rfloor, \left\lceil y_j^{(s)}\right\rceil\right)$, $\left(\left\lceil x_i^{(s)}\right\rceil, \left\lfloor y_j^{(s)}\right\rfloor\right)$, $\left(\left\lceil x_i^{(s)}\right\rceil, \left\lceil y_j^{(s)}\right\rceil\right)$, are found. Finally, calculate the weights $w(p_k)$ of each adjacent pixel through the distance $d\left(p_{(i,j)}^{(s)}, p_k\right)$ between the resized pixel and original adjacent pixels. The resized pixel value is the linear combination of the weight and original adjacent pixels value, then the resized image $\mathbf{X}_s$ is obtained.

2.2 The Effect of Image Scaling on Steganography

At present, the adaptive steganography algorithms improve the detection resistant by minimizing the embedding effect. However, the algorithms do not consider the effect of scaling attack on images, which will lead to the loss of information if the stego images are subject to the scaling attack, resulting in the incorrect extraction.

$\mathbf{Y}=\left(p_{(i,j)}\right)_{m\times n}$ represents the stego image generated by the current image adaptive steganography algorithm, whose column vector of the least significant bit is $\mathbf{y}$. $\mathbf{Y}'=\left(p_{(i,j)}^{(s)}\right)_{m_s\times n_s}$ represents the stego image subject to scaling attack, whose column vector of the least significant bit is $\mathbf{y}'$. Then there are the following formulas in the extraction process.

$$\mathbf{m}=\mathbf{H}\mathbf{y} \quad \textbf{(2)}$$

$$\mathbf{m}'=\mathbf{H}\mathbf{y}' \quad \textbf{(3)}$$

Where $\mathbf{m}$ represents the secret messages extracted in the original stego image, and $\mathbf{m}'$ represents the secret messages extracted in the stego image after scaling. $\mathbf{H}$ is a linear parity-check matrix. For example, when the payload is 0.5, the parity check matrix $\mathbf{H}$ consists of a sub-parity matrix with the width of 2 in order of the diagonal direction. If the sub-parity matrix is $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$, the parity check matrix $\mathbf{H}$ is shown in (4).

$$\begin{bmatrix}
1 & 1 & & & & & & & \\
0 & 1 & 1 & 1 & & & & & \\
 & & 0 & 1 & & & & & \\
 & & & & \ddots & & & & \\
 & & & & & 1 & 1 & & \\
 & & & & & 0 & 1 & 1 & 1
\end{bmatrix} \quad \textbf{(4)}$$

According to the formulas (2) and (3), we can deduce the formula (5).

$$\mathbf{m}-\mathbf{m}'=\mathbf{H}(\mathbf{y}-\mathbf{y}') \quad \textbf{(5)}$$

Where $\mathbf{y}-\mathbf{y}'=\left(y_{(1,1)}-y'_{(1,1)}, y_{(2,1)}-y'_{(2,1)}, \cdots, y_{(m,n)}-y'_{(m,n)}\right)'$.

In the case that the nearest-neighbor interpolation method is used to reduce and enlarge the image size, there are constant pixels $y_{(i,j)}$ before and after the image scaling attack, which means $y_{(i,j)}-y'_{(i,j)}=0$. Remove the value of 0 in $(\mathbf{y}-\mathbf{y}')$, while removing the corresponding columns in $\mathbf{H}$, which has no effect on the value of $\mathbf{m}-\mathbf{m}'$. After scaling attack, the column vector $(\mathbf{y}-\mathbf{y}')$ is randomly valued at 0 or 1. The probability that the value in $\mathbf{m}-\mathbf{m}'$ takes 0 and 1 are 50%, respectively, under the condition that the probability of a full row of 0 in $\mathbf{H}$ is almost zero. In summary, the scaling attack has a serious impact on the performance of the steganography algorithm, and the

existing image adaptive steganography algorithm is difficult to resist the scaling attack.

3 The Steganography Method Based on Scaling Invariant Pixels

Based on the above analysis and summary of the principle of the nearest-neighbor interpolation algorithm, this paper proposes a steganography method resistant to scaling attack and statistical detection based on the scaling invariant pixels. Find adjacent primitive pixels by resized pixel, calculate the resized pixel value by the distance between the resized pixel and adjacent primitive pixels. Then extract the invariant pixels of the original image. Combine with distortion functions in WOW, S-UNIWARD, MiPOD and STCs coding to embed the secret messages in the invariant pixels, so as to achieve both scaling attack resistant and detection resistant. Finally, resize the stego image to the original size. The basic principle of the method framework is shown in Figure 2.

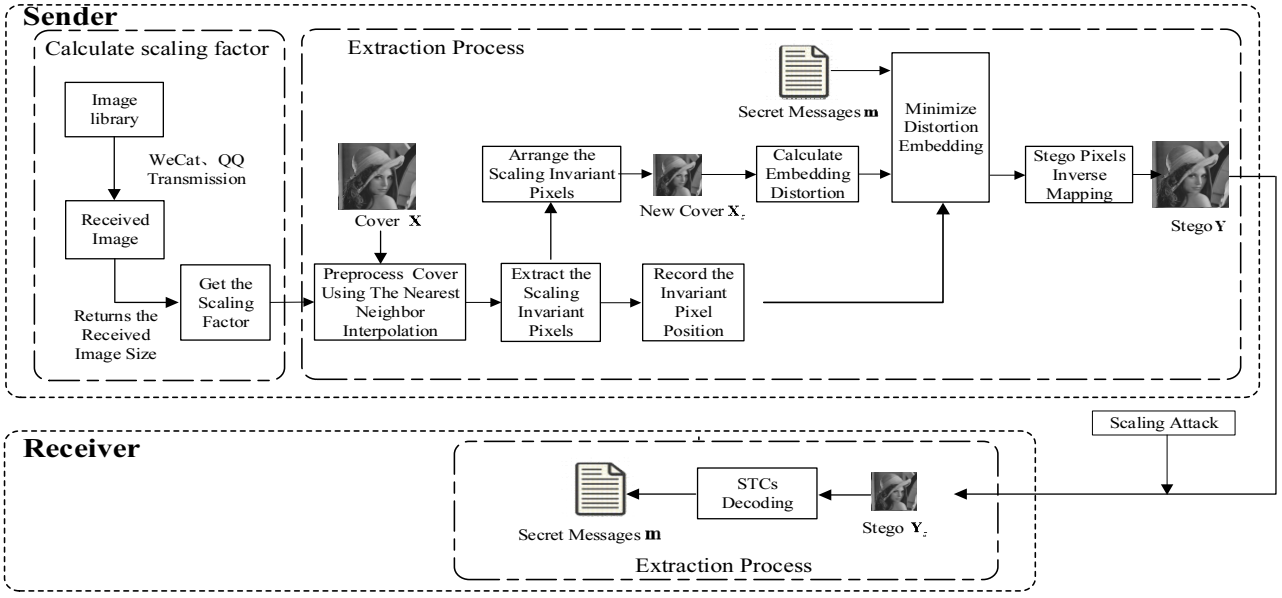

Figure 2. Framework diagram of the proposed method

The embedding process of the proposed method mainly includes the following six steps.

Step 1: Calculate the scaling factor by image pre-transmission. In the actual transmission process of image, we can calculate the scaling factor by the image pre-transmission. The sender transmits the original images through the transmission software such as WeChat, QQ and obtains the size of the received image from the receiver. Then the scaling factor s is obtained by calculating the ratio of the received image size and the original image size.

Step 2: Preprocess the cover image using the nearest-neighbor interpolation. The cover image $\mathbf{X}$ is pre-scaled by the nearest-neighbor interpolation method with the scaling factor s so as to extract scaling invariant pixels.

Step 3: Extract scaling invariant pixels and record invariant pixel position. Extract the scaling invariant pixels from the pre-scale cover image according to the principle of the nearest-neighbor interpolation algorithm. The corresponding position information of the scaling invariant pixels in the original image is preserved in table $\mathbf{T}$.

Step 4: Arrange the scaling invariant pixels to obtain new cover image. The scaling invariant pixels preserved are sorted in the order in which they are fetched, and then a new cover image $\mathbf{X}_s$ is generated.

Step 5: Calculate distortion to minimize distortion embedding. Combine with the spatial distortion functions in WOW, S-UNIWARD and MiPOD to calculate the distortion caused by the new cover image pixel change and embed message using STCs coding, so that the embedding effect to the cover image is minimized, and the detection resistant of the algorithm is improved.

Step 6: Stego pixels inverse mapping to generate new stego image. The corresponding scaling invariant pixels in the original cover image are replaced by the stego image pixels obtained in step 5 according to the position information of the scaling invariant pixels stored in the table $\mathbf{T}$. And the other pixels in the original image remain unchanged. Thereby, the new stego image $\mathbf{Y}$ is obtained which has the same size as the original cover image.

The extraction process is relatively simple and the STCs decoding is applied directly to extract the secret messages in the stego image subject to the public channel scaling attack.

The following describes all the embedding process in order.

3.1 Calculate the Scaling Factor by Image Pre-transmission

The sender transmits the original image of different sizes through the open channel such as WeChat, QQ, etc. used for transmitting the stego image, and obtains the scaling factor according to the ratio of the received image size and the original image size. Hypothesize the original image $\mathbf{X}$ size is $m \times n$, the receiver image $\mathbf{X}'$ size is $m' \times n'$. Usually, the image in the intelligent terminal transmission is transmitted in proportion, so the scaling factor s can be calculated as follow.

$$s = \frac{m'}{m} = \frac{n'}{n} \tag{6}$$

3.2 Preprocess the Cover Image using the Nearest-Neighbor Interpolation

According to the scaling factor s obtained in 3.1, the size of the resized image $\mathbf{X}_s$ is obtained by scaling cover image $\mathbf{X}$ using the nearest-neighbor interpolation method. The process is shown in Figure 3.

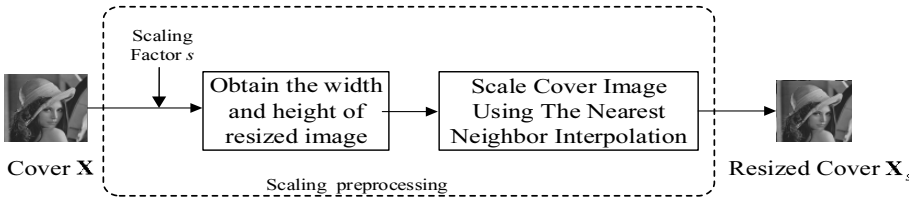

Figure 3. Scaling preprocessing

3.3 Extract Scaling Invariant Pixels and Record Invariant Pixel Position

In general, the starting pixel coordinate of the resized image $\mathbf{X}_s$ in the original image pixel coordinate system is defined in equation (7).

$$\left(x_1^{(s)}, y_1^{(s)}\right) = \left(\frac{s+1}{2s}, \frac{s+1}{2s}\right) \tag{7}$$

Where s is the scaling factor, $x_1^{(s)}$ and $y_1^{(s)}$ represent the first row and first column coordinates of resized pixels in the original pixel coordinate. Then, all resized pixels in the original pixel coordinate system are shown in equation (8).

$$\mathbf{X}_s\left(x_i^{(s)}, y_j^{(s)}\right) = \mathbf{X}_s\left(\frac{s+(2i-1)}{2s}, \frac{s+(2j-1)}{2s}\right) \tag{8}$$

Where $\mathbf{X}_s(i, j)$ is the resized pixels in the row i and column j corresponds to the position $\left(x_i^{(s)}, y_j^{(s)}\right)$, $i=1,2,...,m_s$, $j=1,2,...,n_s$. m_s and n_s are the width and height of the resized image $\mathbf{X}_s$. The coordinates of resized image pixels are shown as follow.

$$\begin{bmatrix} \mathbf{X}_s(1,1) & \cdots & \mathbf{X}_s(1,n_s) \\ \vdots & \ddots & \vdots \\ \mathbf{X}_s(m_s,1) & \cdots & \mathbf{X}_s(m_s,n_s) \end{bmatrix} = \begin{bmatrix} \mathbf{X}_s(x_1^{(s)}, y_1^{(s)}) & \cdots & \mathbf{X}_s(x_1^{(s)}, y_{n_s}^{(s)}) \\ \vdots & \ddots & \vdots \\ \mathbf{X}_s(x_{m_s}^{(s)}, y_1^{(s)}) & \cdots & \mathbf{X}_s(x_{m_s}^{(s)}, y_{n_s}^{(s)}) \end{bmatrix} \tag{9}$$

Where $\mathbf{X}_s(i, j)$ represents the resized pixel value of the coordinate (i, j) .

According to the coordinates of each resized pixel in equation (9), four adjacent primitive pixels can be found for each resized pixel. The values are then weighted for the four original pixels based on the distance between the resized pixel and the four original pixels. Principle is shown in Figure 4.

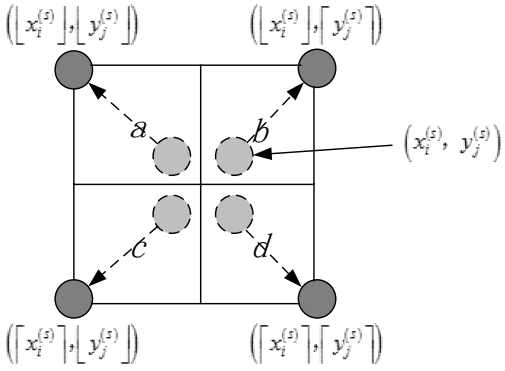

Figure 4. Schematic diagram of the nearest-neighbor interpolation method

$\left(x_i^{(s)}, y_j^{(s)}\right)$ represents the coordinate of the resized pixel in the original image pixel coordinate system after the scaling and $\left(\lfloor x_i^{(s)} \rfloor, \lfloor y_j^{(s)} \rfloor\right)$, $\left(\lfloor x_i^{(s)} \rfloor, \lceil y_j^{(s)} \rceil\right)$, $\left(\lceil x_i^{(s)} \rceil, \lfloor y_j^{(s)} \rfloor\right)$, $\left(\lceil x_i^{(s)} \rceil, \lceil y_j^{(s)} \rceil\right)$ are four adjacent original pixels coordinates. Hypothesize $u = x_i^{(s)} - \lfloor x_i^{(s)} \rfloor$, $v = y_j^{(s)} - \lfloor y_j^{(s)} \rfloor$ and $u, v \in [0,1)$. w represents the weight of the original pixel. If $u < 0.5$ and $v < 0.5$, the resized pixel falls in the area a, $w\left(\lfloor x_i^{(s)} \rfloor, \lfloor y_j^{(s)} \rfloor\right) = 1$, so $\mathbf{X}_s\left(x_i^{(s)}, y_j^{(s)}\right) = \mathbf{X}\left(\lfloor x_i^{(s)} \rfloor, \lfloor y_j^{(s)} \rfloor\right)$.

Similarly, the resized pixel falls in the area b, $w\left(\left\lfloor x_i^{(s)}\right\rfloor,\left\lceil y_j^{(s)}\right\rceil\right)=1$ and $\mathbf{X}_s\left(x_i^{(s)},y_j^{(s)}\right)=\mathbf{X}\left(\left\lfloor x_i^{(s)}\right\rfloor,\left\lceil y_j^{(s)}\right\rceil\right)$. If the resized pixel falls in the area c, $\mathbf{X}_s\left(x_i^{(s)},y_j^{(s)}\right)=\mathbf{X}\left(\left\lceil x_i^{(s)}\right\rceil,\left\lfloor y_j^{(s)}\right\rfloor\right)$. If $u\geq 0.5$ and $v\geq 0.5$, then $w\left(\left\lceil x_i^{(s)}\right\rceil,\left\lceil y_j^{(s)}\right\rceil\right)=1$ and $\mathbf{X}_s\left(x_i^{(s)},y_j^{(s)}\right)=\mathbf{X}\left(\left\lceil x_i^{(s)}\right\rceil,\left\lceil y_j^{(s)}\right\rceil\right)$.

Then the original pixel value with the weight value of 1 is assigned to the resized pixel as the scaling invariant pixel.

Assume $u\geq 0.5$ and $v\geq 0.5$ for all resized pixels coordinates, the process of extracting the scaling invariant pixel values after scaling is shown in Figure 5.

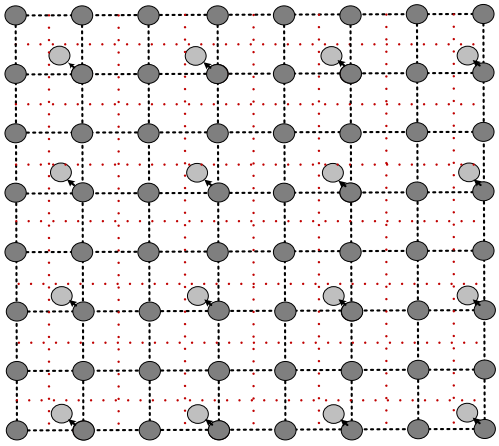

Figure 5. extracting the scaling invariant pixel

The resized image pixels value are shown in equation (10).

$$\mathbf{X}_s=\begin{bmatrix}\mathbf{X}\left(\left\lceil x_1^{(s)}\right\rceil,\left\lceil y_1^{(s)}\right\rceil\right) & \cdots & \mathbf{X}\left(\left\lceil x_1^{(s)}\right\rceil,\left\lceil y_{n_s}^{(s)}\right\rceil\right)\\ \vdots & \ddots & \vdots\\ \mathbf{X}\left(\left\lceil x_{m_s}^{(s)}\right\rceil,\left\lceil y_1^{(s)}\right\rceil\right) & \cdots & \mathbf{X}\left(\left\lceil x_{m_s}^{(s)}\right\rceil,\left\lceil y_{n_s}^{(s)}\right\rceil\right)\end{bmatrix} \quad \textbf{(10)}$$

The coordinates of the pixels in the original pixel coordinate system are recorded while the scaling invariant pixels are found, which is useful for the resized stego image. According to the coordinates, the stego can be restored as the original image size. The coordinates of the scaling invariant pixels in the original image pixels coordinate system are shown in (11).

$$\begin{bmatrix}\left(\left\lceil x_1^{(s)}\right\rceil,\left\lceil y_1^{(s)}\right\rceil\right) & \cdots & \left(\left\lceil x_1^{(s)}\right\rceil,\left\lceil y_{n_s}^{(s)}\right\rceil\right)\\ \vdots & \ddots & \vdots\\ \left(\left\lceil x_{m_s}^{(s)}\right\rceil,\left\lceil y_1^{(s)}\right\rceil\right) & \cdots & \left(\left\lceil x_{m_s}^{(s)}\right\rceil,\left\lceil y_{n_s}^{(s)}\right\rceil\right)\end{bmatrix} \quad \textbf{(11)}$$

3.4 Arrange the Scaling Invariant Pixels to Obtain New Cover Image

From the above analysis, it can be seen that each resized pixel value is corresponding original image pixel value after the nearest-neighbor interpolation method. So extracting the corresponding original image pixel value in equation (10) to generate a new cover image $\mathbf{X}_s$ in order, and regarding the new image $\mathbf{X}_s$ as cover image to embed the message can guarantee the robustness of the method for scaling attack.

3.5 Calculate Distortion to Minimize Distortion Embedding

Use the distortion functions in WOW, S-UNIWARD and MiPOD to calculate the distortion of new cover image pixels generated in 3.3, and then use the STCs encoding to minimize distortion embedding respectively.

In [4], WOW steganography is proposed to calculate the pixel embedding distortion by using the image wavelet decomposition coefficient. The method embeds the secret messages in the complex region of the texture, and its distortion function is defined as follow.

$$\rho_{ij}^{(p)}=\left(\sum_{k=1}^{n}\left|\xi_{ij}^{(k)}\right|^{p}\right)^{-\frac{1}{p}} \quad \textbf{(12)}$$

Where $\xi_{ij}^{(k)}=\left|\mathbf{R}^{(k)}\right|*\left|\mathbf{R}^{(k)}-\mathbf{R}_{[ij]}^{(k)}\right|^{\swarrow}\overset{(a)}{=}\left|\mathbf{R}^{(k)}\right|*\left|\mathbf{K}^{(k)}\right|^{\swarrow}$, $\mathbf{R}^{(k)}=\mathbf{K}^{(k)}*\mathbf{X}$, $k=1,\cdots,n$ is the residuals computed by filters $\mathbf{K}^{(k)}$ and image $\mathbf{X}$, and $p=-1$.

In [5], the definition of embedding distortion function based on image wavelet decomposition coefficient is further studied, and S-UNIWARD is proposed and the performance of anti-detection is better than WOW. The distortion function of the S-UNIWARD steganography algorithm is defined as follow.

$$\mathrm{D}(\mathbf{X},\mathbf{Y})=\sum_{k=1}^{3}\sum_{u=1}^{n_1}\sum_{v=1}^{n_2}\frac{\left|\mathrm{W}_{uv}^{(k)}(\mathbf{X})-\mathrm{W}_{uv}^{(k)}(\mathbf{Y})\right|}{\sigma+\left|\mathrm{W}_{uv}^{(k)}(\mathbf{X})\right|} \quad \textbf{(13)}$$

Where $\mathbf{X},\mathbf{Y}$ represent the cover and stego images in the spatial domain, and $\mathrm{W}_{uv}^{(k)}(\mathbf{X}),\mathrm{W}_{uv}^{(k)}(\mathbf{Y})$, $k=1,2,3$, $u=\{1,\cdots,n_1\},v=\{1,\cdots,n_2\}$ are their corresponding uv th wavelet coefficient in the k th subband of the first decomposition level.

In [7], the embedding distortion of the cover image element is determined by minimizing the power of optimal detector. The distortion formula is shown in equation (14).

$$\mathrm{D}(\mathbf{X},\mathbf{Y})=\sum_{n=1}^{N}\rho_n\ [x_n\neq y_n] \quad \textbf{(14)}$$

Where $\rho_n = \ln(1/\beta_n - 2)$, $n = 1,...,N$ are the pixel costs, β_n is the change rates of cover pixels and $\beta_n \sigma_n^{-4} = \frac{1}{2\lambda} \ln \frac{1-2\beta_n}{\beta_n}$, $n = 1,...,N$, σ_n^2 is the variance of each pixel, $\lambda > 0$ is the Lagrange multiplier.

Calculate the embedded distortion of cover image according to the above three ways, and then combine with STCs coding to minimize the distortion embedding and extract the embedded secret messages. The process of embedding and extracting secret messages using STCscoding is shown in equations (15) and (16).

$$\mathbf{y} = \mathrm{Emb}(\mathbf{x}, \mathbf{m}) = \arg \min_{\mathbf{y} \in C(\mathbf{m})} \mathrm{D}(\mathbf{x}, \mathbf{y}) \tag{15}$$

$$\mathbf{m} = \mathrm{Ext}(\mathbf{y}) = \mathbf{H}\mathbf{y} \tag{16}$$

Where $\mathbf{x} = \{0,1\}^n, \mathbf{y} = \{0,1\}^n$ are the cover and stego sequences respectively. $\mathbf{H} = \{0,1\}^{m \times n}$ is a parity-check matrix and $\mathrm{C}(\mathbf{m}) = \left\{ \mathbf{z} \in \{0,1\}^n \middle| \mathbf{H}\mathbf{z} = \mathbf{m} \right\}$ is the coset corresponding to syndrome $\mathbf{m}$.

3.6 Stego Pixels Inverse Mapping to Generate New Stego Image

In order to prevent the stego image from being subjected to the scaling attack when transmitted in the open channel, the resized image is used to realize the coordinate inverse mapping. The pixels of the original image with weight equal to 1 are replaced by the corresponding resized image pixels, and then restore the image to the original size.

In the transmission process after the same scaling attack, the proposed method can also ensure that the secret messages are extracted completely correctly, thereby achieving the robustness against the scaling attack. As can be seen from Equation (10), the new cover image generated are expressed as follow.

$$\mathbf{X}_s = \begin{bmatrix} \mathbf{X}_s(1,1) & \cdots & \mathbf{X}_s(1,n_s) \\ \vdots & \ddots & \vdots \\ \mathbf{X}_s(m_s,1) & \cdots & \mathbf{X}_s(m_s,n_s) \end{bmatrix} = \begin{bmatrix} \mathbf{X}\left(\left\lceil x_1^{(s)} \right\rceil, \left\lceil y_1^{(s)} \right\rceil\right) & \cdots & \mathbf{X}\left(\left\lceil x_1^{(s)} \right\rceil, \left\lceil y_{n_s}^{(s)} \right\rceil\right) \\ \vdots & \ddots & \vdots \\ \mathbf{X}\left(\left\lceil x_{m_s}^{(s)} \right\rceil, \left\lceil y_1^{(s)} \right\rceil\right) & \cdots & \mathbf{X}\left(\left\lceil x_{m_s}^{(s)} \right\rceil, \left\lceil y_{n_s}^{(s)} \right\rceil\right) \end{bmatrix} \tag{17}$$

When the secret messages are embedded, a stego image $\mathbf{Y}_s$ is generated.

$$\mathbf{Y}_s = \begin{bmatrix} \mathbf{Y}_s\left(\left\lceil x_1^{(s)} \right\rceil, \left\lceil y_1^{(s)} \right\rceil\right) & \cdots & \mathbf{Y}_s\left(\left\lceil x_1^{(s)} \right\rceil, \left\lceil y_{n_s}^{(s)} \right\rceil\right) \\ \vdots & \ddots & \vdots \\ \mathbf{Y}_s\left(\left\lceil x_{m_s}^{(s)} \right\rceil, \left\lceil y_1^{(s)} \right\rceil\right) & \cdots & \mathbf{Y}_s\left(\left\lceil x_{m_s}^{(s)} \right\rceil, \left\lceil y_{n_s}^{(s)} \right\rceil\right) \end{bmatrix} \tag{18}$$

Then, $\mathbf{Y}_s\left(\left\lceil x_i^{(s)} \right\rceil, \left\lceil y_j^{(s)} \right\rceil\right)$ is used to replace $\mathbf{X}\left(\left\lceil x_i^{(s)} \right\rceil, \left\lceil y_j^{(s)} \right\rceil\right)$ in original cover image to generate a stego image $\mathbf{Y}$ with the same size as the original image.

Figure 6 shows the example of the pixel block scaling inverse mapping in the case of scaling factor of 0.5. First, use the nearest-neighbor interpolation method to scale the original pixel block. Then Embed the secret message $\mathbf{m}$ into the pixel block after scaling. Finally, use the stego pixel block replace the original pixel block Correspondingly. The red pixels indicate the new pixel acquired after the scaling, and after the embedding of the secret message, they will be replaced by the light gray pixels value. And the remaining pixel values remain unchanged to obtain the same size stego image as the original cover image.

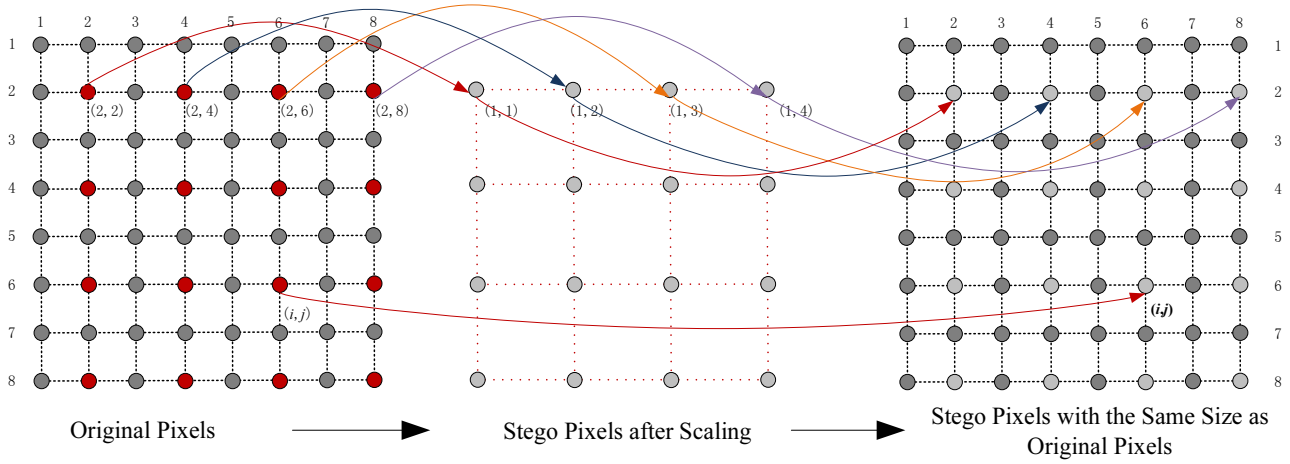

Figure 6. Stego pixels inverse mapping

4 Experimental Results and Analysis

In order to verify the scaling attack resistant and detection resistant performance of the proposed method, the WOW [4], S-UNIWARD [5] and MiPOD [7] algorithms and the proposed method are simulated in the MatlabR2015a, and the stego images generated in both schemes are scaled and the secret messages are extracted in the stego images after scaling. The steganalysis experiment is realized by extracting SPAM feature and maxSRM feature. Select 2000 images randomly in the BossBase-1.01 image library as the original cover images, and the original image size are 512×512. Randomly generate binary sequence as the secret messages sequence to be embedded. The payload is from 0.1 to 0.5, and he scaling factor includes 0.25, 0.5, 0.75 and 1 respectively. In the case where the scaling factor is 1, the scaling image is not scaled. The parameter settings are shown in Table 1.

Table 1. Experimental parameters table

Cover		Embedding Process			Features
		Scaling factor	Payloads	Distortion Function	
Source	BossBase-1.01	0.25	0.1 0.2 0.3 0.4 0.5	WOW [4] S-UNIWARD [5] MiPOD [7]	SPAM [26] maxSRM [27]

4.1 Scaling Attack Resistant Experiment

The original WOW, S-UNIWARD, MiPOD and the proposed method calculating distortion by the above three algorithms are used to embed the secret messages, and the stego images generated are scaled with the scaling factors of 0.25, 0.5, 0.75 and 1 respectively, then extract the secret messages in the stego images after scaling. The extraction error rate of the secret messages in the four embedded schemes are R_{error}, as shown in equation (19).

$$R_{error} = \frac{n_{error}}{n} \tag{19}$$

Where n_{error} is the number of message bits extracted mistakenly, and n is the total number of embedded messages.

Figure 7 show the average extraction error rate of WOW, S-UNIWARD, MiPOD algorithms and the proposed method under different payloads after the stego images subjected to scaling attack. It can be seen from the figures that when the scaling factor is 0.25, 0.5 and 0.75, the average extraction error rate of WOW, S-UNIWARD and MiPOD algorithms are close to 50%, equivalent to random guess. This is because the scaling attack makes the stego image pixel values change randomly, resulting in the secret massages loss and extraction errors. And the extraction error rate of the proposed method is 0. Because the proposed method in this paper constructs a new cover image to ensure that the stego is not changed before and after scaling, so as to ensure the correct extraction of the secret messages. When the scaling factor is 1, which means no scaling attack to stego images, the average extraction error rate of WOW, S-UNIWARD and MiPOD algorithms and the proposed method are all zero.

4.2 Statistical Detection Resistant Experiment

The steganalysis experiment is carried out by scaling the original cover images with the same scaling factor and the 686 dimension feature SPAM [26] and 34671 dimension feature maxSRM [27] are extracted. At the same time, these two kinds of features of the stego images after the scaling attack are extracted, and ensemble classifier is used for training and testing, The average detection error rates are shown in the following four figures.

Figure 8 show the detection error rates of low-dimensional feature SPAM and high-dimensional feature maxSRM under the different payloads when the scaling factor is 0.25. The three curves are the proposed method applying three different distortion calculation methods respectively. Figure 9, Figure 10 and Figure 11 show the detection error rates when scaling factor are 0.5, 0.75, and 1. The experimental results show that the detection error rates of the proposed method are still high under the premise that the secret messages can be completely correctly extracted. For example, under the payload of 0.5, when the scaling factor is 0. 25, the detection error rates based on the maxSRM feature are 0.4054, 0.4229 and 0.4589. When the scaling factor is 0.5, the detection error rates are 0.3655, 0.3749 and 0.4275. When the scaling factor is 0.75, the detection error rates are still up to 0.3615, 0.2889 and 0.2888 respectively by three different distortion function calculation methods of WOW, S-UNIWARD and MiPOD. when the scaling factor is 1, which means that the cover image is not scaled, the detection error rates of the proposed methods using WOW, S-UNIWARD and MiPOD is close to the original steganography algorithms.

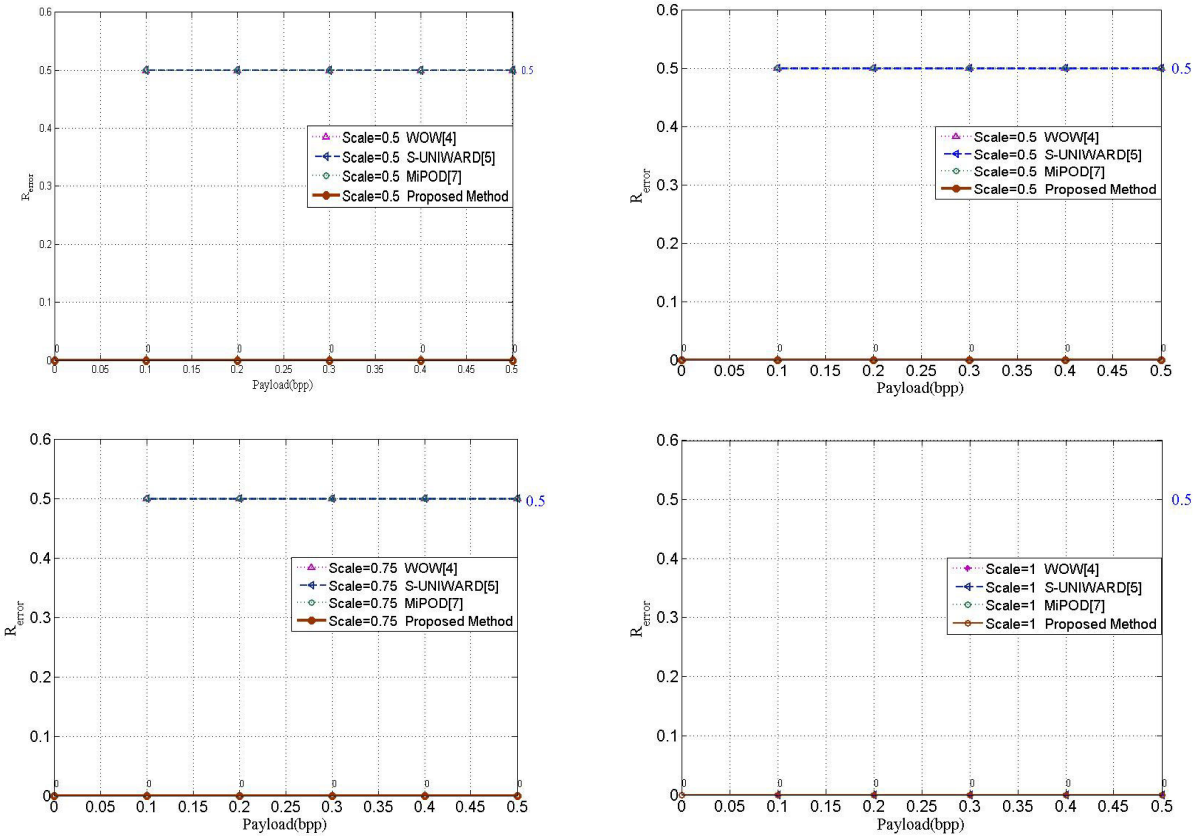

Figure 7. Extraction error rate under different payloads

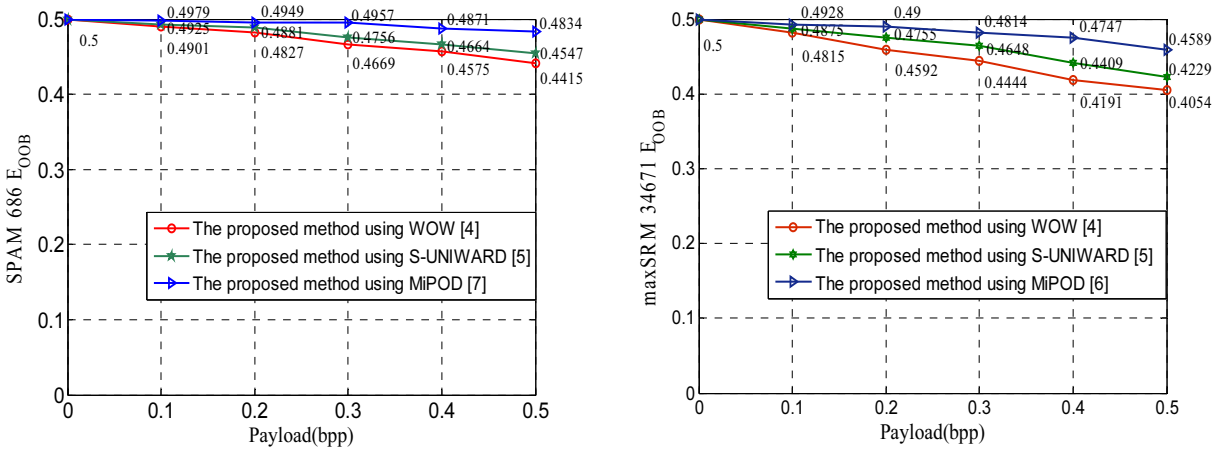

Figure 8. Detection error rate under the scaling factor 0.25. SPAM feature (left), maxSRM feature (right)

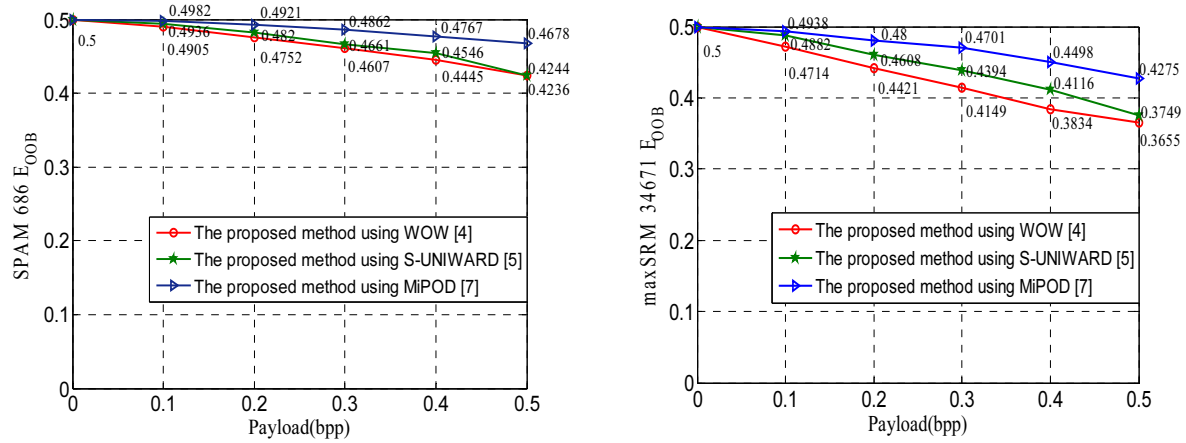

Figure 9. Detection error rate under the scaling factor 0. 5. SPAM feature(left), maxSRM feature (right)

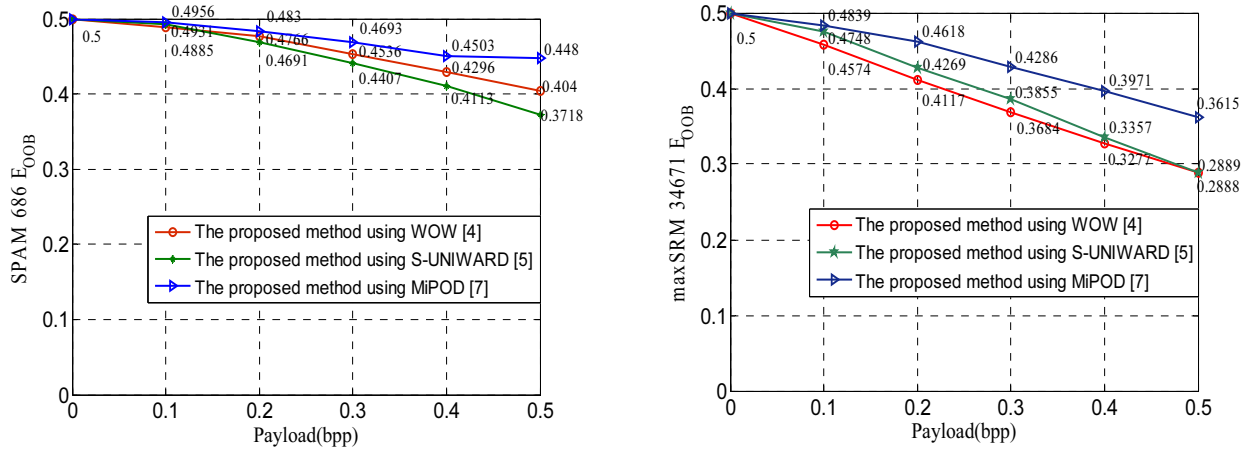

Figure 10. Detection error rate under the scaling factor 0.75. SPAM feature (left), maxSRM feature (right)

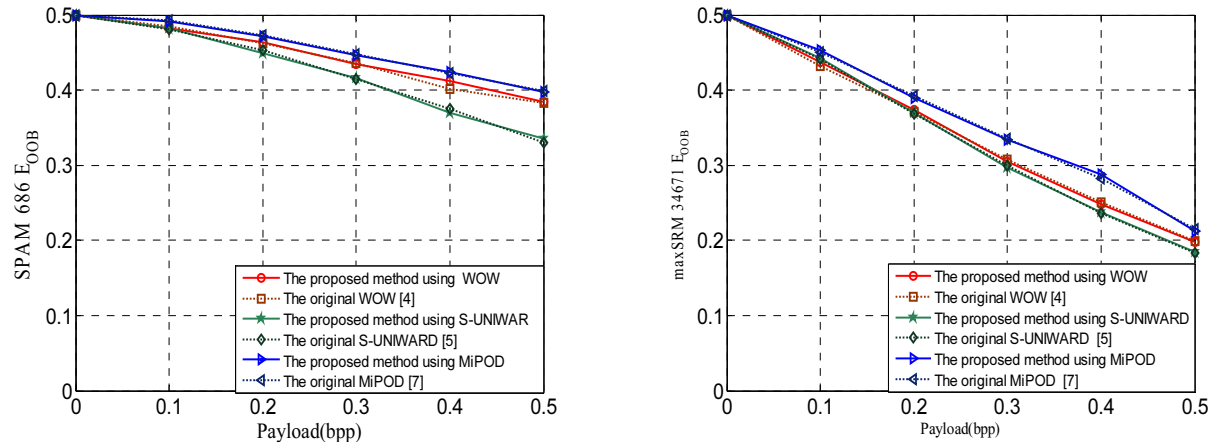

Figure 11. Detection error rate under the scaling factor 1. SPAM feature (left), maxSRM feature (right)

At the same time the smaller the scaling factor is, the higher detection error rate is in both features. This is because the decrease of scaling factor leads to the increase of spatial distance between adjacent pixels of the resized image, at the same time the increase of spatial distance between pixels results in weaker dependence between adjacent pixels, which makes the detection method based on the feature extraction more difficult. So, with the decrease of scaling factor, the detection error rate becomes higher and higher.

5 Conclusion

This paper proposes a scaling attack and detection resistant method based on the scaling variable pixels to solve the problem of information loss when the stego image is subjected to scaling attack. By analyzing the principle of the nearest-neighbor interpolation method, the scaling invariant pixels before and after scaling are extracted and reconstructed into a new cover image. Distortion function in WOW, S-UNIWARD and MiPOD and STCs coding are used to embed and extract the messages on the cover image. The experimental results show that the proposed method demonstrates good scaling attack resistant and detection resistant performance under different scaling factors and payloads. However, this paper is only a preliminary attempt for the steganography algorithm that resists to scaling attack, and can only resists the scaling attack of the nearest-neighbor interpolation method. It's ineffective on the other scaling processing, such as bilinear interpolation, bicubic interpolation and so on.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (No. 61379151, 61401512, 61572052, U1636219), the National Key Research and Development Program of China (No. 2016YFB0801303, 2016QY01W0105), and the Key Technologies Research and Development Program of Henan Provinces (No.162102210032). Part of the manuscript has been published in the ICCCS 2017 conference.

References

[1] Z. Pan, J. Lei, Y. Zhang, X. Sun, S. Kwong, Fast Motion

Estimation Based on Content Property for Low-complexity H.265/HEVC Encoder, *IEEE Transactions on Broadcasting*, Vol. 62, No. 3, pp. 675-684, September, 2016.

[2] T. Filler, J. Judas, J. Fridrich, Minimizing Additive Distortion in Steganography Using Syndrome-trellis Codes, *IEEE Transactions on Information Forensics and Security*, Vol. 6, No. 3, pp. 920-935, September, 2011.

[3] T. Pevný, T. Filler, P. Bas, Using High-dimensional Image Models to Perform Highly Undetectable Steganography, *International Conference on Information Hiding*, Calgary, AB, Canada, 2010, pp. 161-177.

[4] V. Holub, J. Fridrich, Designing Steganographic Distortion Using Directional Filters, *2012 IEEE International Workshop on Information Forensics and Security*, Tenerife, Spain, December, 2012, pp. 234-239.

[5] V. Holub, J. Fridrich, Digital Image Steganography Using Universal Distortion, *First ACM Workshop on Information Hiding and Multimedia Security*, Montpellier, France, 2013, pp. 59-68.

[6] B. Li, M. Wang, J. Huang, X. Li, A New Cost Function for Spatial Image Steganography, *International Conference on Image Processing*, Paris, France, 2014, pp. 4206-4210.

[7] V. Sedighi, R. Cogranne, J. Fridrich, Content-adaptive Steganography by Minimizing Statistical Detectability, *IEEE Transactions on Information Forensics and Security*, Vol. 11, No. 2, pp. 221-234, February, 2016.

[8] L. Guo, J. Ni, Y. Shi, An Efficient JPEG Steganographic Scheme Using Uniform Embedding, *2012 IEEE International Workshop on Information Forensics and Security*, Tenerife, Spain, December, 2012, pp. 169-174.

[9] B. S. Kim, J. G. Choi, C. H. Park, J. U. Won, D. M. Kwak, S. K. Oh, C. R. Koh, K. H. Park, Robust Digital Image Watermarking Method against Geometrical Attacks, *Real-Time Imaging*, Vol. 9, No. 2, pp. 139-149, April, 2003.

[10] D. Zheng, S. Wang, J. Zhao, Mathematical Modeling and Stochastic Analysis for RST Invariant Watermarking Algorithm, *5th International Conference on Visual Information Engineering*, Xi'an, China, July, 2008, pp. 130-135.

[11] A. H. Taherinia, M. Jamzad, A New Spread Spectrum Watermarking Method Using Two Levels DCT, *International Journal of Electronic Security and Digital Forensics*, Vol. 3, No.1, pp. 1-26, March, 2010.

[12] Y. Naderahmadian, S. Beheshti, Robustness of Wavelet Domain Watermarking against Scaling Attack, *Electrical and Computer Engineering*, Halifax, Canada, 2015, pp. 1218-1222.

[13] Y. Lin, C. Huang, G. Lee, Rotation, Scaling, and Translation Resilient Watermarking for Images, *IET Image Processing*, Vol. 5, No. 4, pp. 328-340, June, 2011.

[14] Z. Lin, L. Niu, X. Jiang, A Method on Digital Watermarking Image against Geometric Distortion, *2014 7th International Congress on Image and Signal Processing*, Dalian, China, 2014, pp. 130-134.

[15] Y. H. Lee, S. S. Yeo, K. Jin, Securing Digital Images over the Internet Using a Robust Watermarking Scheme, *Journal of Internet Technology*, Vol. 11, No. 3, pp. 315-322, May, 2010.

[16] M. Zareian, H. R. Tohidypour, A Novel Gain Invariant Quantization-based Watermarking Approach, *IEEE Transactions on Information Forensics and Security*, Vol. 9, No. 11, pp. 1804-1813, November, 2014.

[17] Z. Zhou, Y. Wang, Q. M. J. Wu, C. N. Yang, X. Sun, Effective and Efficient Global Context Verification for Image Copy Detection, *IEEE Transactions on Information Forensics and Security*, Vol. 12, No. 1, pp. 48-63, January, 2017.

[18] Z. Zhou, C. N. Yang, B. Chen, X. Sun, Q. Liu, Q. M. J. Wu, Effective and Efficient Image Copy Detection with Resistance to Arbitrary Rotation, *IEICE Transactions on Information and Systems*, Vol. E99.D, No. 6, pp. 1531-1540, 2016.

[19] B. Chen, H. Shu, G. Coatrieux, G. Chen, X. Sun, J. L. Coatrieux, Color Image Analysis by Quaternion-type Moments, *Journal of Mathematical Imaging and Vision*, Vol. 51, No. 1, pp. 124-144, January, 2015.

[20] I. Ullah, H. Aboalsamh, M. Hussain, G. Muhammad, G. Bebis, Gender Classification from Facial Images Using Texture Descriptors, *Journal of Internet Technology*, Vol. 15, No. 5 , pp. 801-811, September, 2014.

[21] J. Li, X. Li, B. Yang, X. Sun, Segmentation-based Image Copy-move Forgery Detection Scheme, *IEEE Transactions on Information Forensics and Security*, Vol. 10, No. 3, pp. 507-518, March, 2015.

[22] C. Qin, X. Zhang, Effective Reversible Data Hiding in Encrypted Image with Privacy Protection for Image Content, *Journal of Visual Communication and Image Representation*, Vol. 31, pp. 154-164, August, 2015.

[23] B. S. Saini, K. V. Krishna, Medical Image Up-sampling Using a Correlation-based Sparse Representation Model, *International Journal of Medical Engineering and Informatics*, Vol. 9, No. 1, pp. 73-86, December, 2017.

[24] Y. Zhang, X. Luo, C. Yang, D. Ye, F. Liu, A JPEG-Compression Resistant Adaptive Steganography Based on Relative Relationship between DCT Coefficients, *10th International Conference on Availability, Reliability and Security*, Toulouse, France, August, 2015, pp. 461-466.

[25] Y. Zhang, X. Luo, C. Yang, F. Liu, Joint JPEG Compression and Detection Resistant Performance Enhancement for Adaptive Steganography Using Feature Regions Selection, *Multimedia Tools and Applications*, Vol. 76, No. 3, pp. 3649-3668, February, 2017.

[26] T. Pevný, P. Bas, J. Fridrich, Steganalysis by Subtractive Pixel Adjacency Matrix, *IEEE Transactions on Information Forensics and Security*, Vol. 5, No. 2, pp. 215-224, June, 2010.

[27] T. Denemark, V. Sedighi, V. Holub, R. Cogranne, J. Fridrich, Selection-channel-aware Rich Model for Steganalysis of Digital Images, *the 6th IEEE International Workshop on Information Forensics and Security*, Atlanta, GA, 2014, pp. 48-53.

Biographies

Yue Zhang received the B.S. degree from the Dalian University of Technology, Dalian, China, in 2015. Currently, she is pursuing a M.S. degree in the State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou Science and Technology Institute, China. Her research interests include image steganography and steganalysis.

Xiangyang Luo received the M.S. degree and the Ph.D. degree from Zhengzhou Information Science and Technology Institute, Zhengzhou, China, in 2004 and 2010, respectively. He is currently an associate professor of State Key Laboratory of Mathematical Engineering and Advanced Computing, and Zhengzhou Information Science and Technology Institute.

Jinwei Wang works as a professor at Nanjing University of Information Science & Technology. His research interests include multimedia copyright protection, multimedia forensics, multimedia encryption and data authentication. He has published more than 40 papers, hosted and participated in more than 10 projects.

Chunfang Yang received the M.S. degree and Ph.D. degree from Zhengzhou Information Science and Technology Institute, Zhengzhou, China, in 2008 and 2012, respectively. Currently, he is a lecturer of Zhengzhou Information Science and Technology Institute. His research interest includes image steganography and steganalysis technique.

Fenlin Liu is currently a professor of State Key Laboratory of Mathematical Engineering and Advanced Computing, and Zhengzhou Information Science and Technology Institute. His research interests include information hiding and security theory. He is the author or co-author of more than 100 refereed international journal and conference papers.