 CMC, vol.56, no.1, pp.151-167, 2018

An Image Steganography Algorithm Based on Quantization Index Modulation Resisting Scaling Attacks and Statistical Detection

Yue Zhang[1], Dengpan Ye[2], Junjun Gan[1], Zhenyu Li[3] and Qingfeng Cheng[1,*]

Abstract: In view of the fact that the current adaptive steganography algorithms are difficult to resist scaling attacks and that a method resisting scaling attack is only for the nearest neighbor interpolation method, this paper proposes an image steganography algorithm based on quantization index modulation resisting both scaling attacks and statistical detection. For the spatial image, this paper uses the watermarking algorithm based on quantization index modulation to extract the embedded domain. Then construct the embedding distortion function of the new embedded domain based on S-UNIWARD steganography, and use the minimum distortion coding to realize the embedding of the secret messages. Finally, according to the embedding modification amplitude of secret messages in the new embedded domain, the quantization index modulation algorithm is applied to realize the final embedding of secret messages in the original embedded domain. The experimental results show that the algorithm proposed is robust to the three common interpolation attacks including the nearest neighbor interpolation, the bilinear interpolation and the bicubic interpolation. And the average correct extraction rate of embedded messages increases from 50% to over 93% after 0.5 times-fold scaling attack using the bicubic interpolation method, compared with the classical steganography algorithm S-UNIWARD. Also the algorithm proposed has higher detection resistance than the original watermarking algorithm based on quantization index modulation.

Keywords: Image steganography, anti-scaling attack, anti-statistical detection, quantization index modulation.

1 Introduction

The steganography technology embeds secret messages into the cover file by certain modification way, so as to achieve the covert communications through broadband and Wi-Fi. As one branch of the steganography technology, digital image steganography has been widely used in the modern era of digital media and network development resisting detection of rich model [Ma, Luo, Li et al. (2018)]. However, with the development of electronic equipment, the digital image sharpness is getting higher, and the memory space occupied is also increasing, which makes the digital image suffer compression, scaling and

[1] State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China.

[2] Computer School of Wuhan University, Wuhan 430072, China.

[3] Department of Computer Science, University of York, York YO10 5GH, UK.

[*] Corresponding Author: Qingfeng Cheng. Email: qingfengc2008@sina.com.

other processing operations during transmission, resulting in the decline of digital image quality and information loss. If the existing highly-resistant adaptive image steganography is applied directly to digital images of electronic devices to realize information covert communication, it is difficult to extract the secret completely and correctly from the received stego image. Therefore, in order to realize the steganography technology based on electronic devices, the robustness of embedded message to image processing operation should be considered while the stego image is highly resistant to statistical detection. This paper focuses on image scaling processing, and studies an image steganography algorithm which can resist both scaling attack and statistical detection.

In the aspect of anti-statistic detection, the existing adaptive steganography algorithms have realized the high anti-detection. Most of these algorithms calculate the distortion caused by the change of the cover pixel, and then apply the STCs coding [Tomas, Judas and Fridrich (2011)] to select the location with small distortion to realize the embedding of the secret messages. In recent years, with the rapid development of adaptive steganography, the design of distortion function is also various. Typical spatial adaptive steganography such as Hugo (Highly-undetectable Stego) [Pevný, Filler and Bas (2010); Luo, Song, Li et al. (2016)] steganography algorithm, WOW (Wavelet obtained Weights) [Holub and Fridrich (2012)] steganography algorithm, S-UNIWARD (Spatial Universal Wavelet relative Distortion) [Holub and Fridrich (2013)] steganography algorithm. In addition, there are Hill (High-pass, Low-pass, and Low-pass) [Li, Wang, Huang et al. (2014)], MiPOD (Minimizing the Power of Optimal Detor) algorithm [Sedighi, Cogranne and Fridrich (2016)], and so on, which have higher resistance to detection. Typical frequency-domain adaptive steganography algorithms such as UED (uniform embedding distortion) [Guo, Ni and Shi (2012)] Steganography and J-UNIWARD (JPEG Universal Wavelet Relative Distortion) [Holub and Fridrich (2013)] steganography algorithm. With the further research, the anti-detection performance of steganography algorithms has been greatly improved. However, a large number of experiments show that such steganography algorithms often have a high error rate in extracting secret message after suffering scaling attack. For example, a typical steganography S-UNIWARD, after a 0.5x the nearest neighbor interpolation scaling attack, whose correct rate of secret message extracted is only 50%.

The main research of anti-scaling attack performance is focused on the field of digital watermarking, and most of the existing robust watermarking algorithms are robust to scaling attacks. The common watermarking algorithms resisting scaling attacks are based on geometric invariants, time-frequency transform, image features, quantization index modulation and so on. Kim et al. [Kim, Choi, Park et al. (2003)] use logarithmic polar graph to obtain geometric invariants in the spatial domain, this scheme has strong robustness to RST (Rotation, Scaling, Translation) attacks. In the paper of Naderahmadian et al. [Naderahmadian and Beheshti (2015)], the message is embedded in the image wavelet domain in order to obtain stronger scaling attack performance. The Literature [Lin, Niu and Jiang (2015)] uses the Harris detector to extract the feature points and embed the watermark message. Zareian et al. [Zareian and Tohidypour (2014)] combined with image time-frequency transformation and quantization index modulation, watermark message can be extracted completely and correctly when watermark image suffers 0.5 times scaling attack. Most of these algorithms embed secret message into the region which is insensitive to scaling attack, and use the embedding algorithm of anti-

scaling attack, which greatly improves the robustness of the algorithm to the scaling and other image processing attacks. However, if applied directly to the steganography field, only a few algorithms can ensure that the secret message is extracted correctly after the scaling attack. On the other hand, most of these watermarking algorithms modify the main content of the cover image to improve the robustness, so the image distortion is relatively large, so their performance of anti-detection is poor.

In view of the effect of image processing on the performance of steganography, the papers [Zhang, Luo, Yang et al. (2015, 2016); Zhang, Qin, Zhang et al. (2018)] put forward the solution, which can resist JPEG compression processing and statistical detection. The main idea is to improve the robustness of the stego image to the compression attack by combining the robust watermarking algorithm against JPEG compression while guaranteeing the anti-detection of the stego image. However, such methods only consider compression attacks and do not consider scaling attacks during image transmission. Based on these researches, this paper studies the method of image steganography which can resist both scaling attack and statistic detection.

In view of anti-scaling attack of steganography algorithm, we have proposed a steganography method based on scaling invariant pixels for anti-scaling attack and statistical detection. This method extracts the invariant pixels from the cover image suffering the nearest neighbor scaling attack, and generates a new embedded cover, and then uses the spatial distortion function S-UNIWARD to compute the distortion of the new cover, and finally embeds the secret message by STCs coding. This steganography ensures high resistance to detection and scaling attack, and also high embedding capacity. However, this method is only valid for the nearest neighbor interpolation scaling attack, and not resistant to other scaling methods.

In this paper, combining the watermarking algorithm with strong robustness to scaling attack, an image adaptive steganography algorithm based on quantization modulation resisting scaling attack and statistical detection is proposed, drawing on the research scheme in reference Zhang et al. [Zhang, Luo, Yang et al. (2015)]. For the spatial domain image, the algorithm firstly uses the watermarking algorithm based on quantization index modulation to extract the embedded domain of secret message, then uses the spatial distortion function S-UNIWARD to construct the embedded distortion of the new embedded domain, and uses the minimization distortion coding to embed secret message. Finally, according to the modified amplitude of the new embedded domain, the algorithm based on quantization index modulation is applied to realize the final embedding of secret message in the original embedded domain. The algorithm is robust to three kinds of common interpolation scaling attacks [Han (2013)], and also has resistance to detection.

The remainder of this manuscript is organized as follows. In the second section, the original quantization index modulation watermarking algorithm and the principle of S-UNIWARD distortion function and STCs coding are described. The third section elaborates the principle frame and the concrete steps of the proposed algorithm. The fourth section performs performance analysis from two aspects of algorithm anti-scaling and anti-detection. The fifth section gives the experimental results, and the sixth section is the conclusion.

2 Related work

2.1 Quantization index modulation watermarking algorithm

The embedded algorithm of quantization index modulation (QIM) modulates the cover vector into different intervals to form the stego vector according to the different embedded message. If the stego vector is still fluctuating in this interval after scaling attack, it shows that it has better anti-scaling attack performance. In the paper Chen et al. [Chen and Wornell (2001)], a watermarking algorithm based on quantization index modulation is proposed, in which the distortion between cover vector and stego vector is minimized, and the robustness to image processing attack is considered. The basic principle of quantization index modulation algorithm and its contribution to the design of steganography algorithm against scaling attack and statistical detection are described below.

The basic QIM algorithm uses two uniform quantizers $Q_0(.)$ and $Q_1(.)$, their centroids are given by the shift lattice $\Lambda_m = \Delta\mathbf{Z} - m\frac{\Delta}{2}, m = 0,1$, where $\mathbf{Z}$ is the integer set, Δ is the quantization step. Assuming that the cover vector is $\mathbf{u}$, $m \in \{0,1\}$ is the message bit to be embedded. When the message is embedded, the following formula is applied to modulate the cover vector to the corresponding interval.

$$\mathbf{u}' = Q_m(\mathbf{u}) = \Delta round(\frac{\mathbf{u} + m\Delta/2}{\Delta}) - m\frac{\Delta}{2} \tag{1}$$

where $\mathbf{u}'$ is the stego vector. The extraction operation is accomplished by minimizing the Euclidean Distance between $\mathbf{u}'$ and $Q_m(\mathbf{u})$.

$$\hat{m} = \arg\min_{m\in\{0,1\}} |\mathbf{u}' - Q_m(\mathbf{u}')| \tag{2}$$

The watermarking algorithm based on quantization index modulation achieves its anti-scaling capability by modulating the cover vector into different intervals according to the secret massage bit and quantization step. When the stego vector is attacked, the secret message can still be extracted exactly if its value is still fluctuating within the interval. For image scaling processing, the more accurate the algorithm is, the smaller the numerical change is, the higher the resistance.

2.2 S-UNIWARD steganography algorithm

S-UNIWARD steganography is a common steganography algorithm for spatial images. The distortion is calculated as the sum of the relative changes of the decomposition coefficients of the directional filter group of the cover image, and the detection resistance is improved by embedding the secret message into the region with complex texture. The calculation formula is as follows.

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

where X and Y represent the cover and stego images in the spatial domain,

and $W_{uv}^{(k)}(\mathbf{X})$, $W_{uv}^{(k)}(\mathbf{Y})$, $k=1,2,3, u=\{1,\cdots,n_1\}, v=\{1,\cdots,n_2\}$ are their corresponding uv-th wavelet coefficient in the *k*-th subband of the first decomposition level. $\sigma>0$ is a constant used to stabilize numerical computations.

STCs code is the encoding method commonly used in adaptive steganography, which can make the message embedding minimize the modification of the cover pixel. The process of embedding and extracting secret information using STCS encoding are shown in formulas (4) and (5).

$$\mathbf{y}=\mathrm{Emb}(\mathbf{x},\mathbf{m})=\arg\min_{\mathbf{y}\in C(\mathbf{m})}\mathrm{D}(\mathbf{x},\mathbf{y}) \tag{4}$$

$$\mathbf{m}=\mathrm{Ext}(\mathbf{y})=\mathbf{H}\mathbf{y} \tag{5}$$

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

3 Image steganography algorithm based on quantization index modulation

In order to enhance the robustness of the algorithm to a variety of scaling attacks, the adaptive steganography algorithm based on quantization index modulation against scaling attack and statistical detection is proposed in this paper. The quantization index modulation watermarking algorithm is used to extract the robust embedded domain and embedding mode, which guarantees the robustness of the algorithm to common scaling attacks. At the same time, the new distortion function is designed according to the original cover image modification after message embedding, so that the algorithm has resistance to detection. The principle frame and the main steps of the proposed algorithm during embedding and extracting are introduced in following.

3.1 Algorithm principle architecture

The schematic diagram of the image steganography algorithm based on quantization index modulation resisting scaling attack and statistical detection is shown in Fig. 1. Its embedding process and extraction process are described as follows.

Embedding process:

Step 1: Extract new cover elements. For the original spatial cover image, the robust watermark extraction algorithm based on quantization index modulation is used to extract new cover elements. It is convenient to use STCs code to find the embedded location with less distortion.

Step 2: Design distortion function. Combined with the modified amplitude of the original cover image after embedding 0 and 1 by watermarking algorithm, the embedded distortion of new cover elements is constructed using S-UNIWARD of the spatial distortion function.

Step 3: Minimize distortion embedding. Using the minimum distortion coding STCs to embed secret message in the new cover elements, the message embedding can minimize

the change of new cover elements so as to achieve anti-detection.

Step 4: Modify the original cover image according to the stego elements. According to the modifying of the cover elements by secret message, the watermarking algorithm based on quantization index modulation is used to embed the stego elements containing the secret message into the original cover image and to generate stego image.

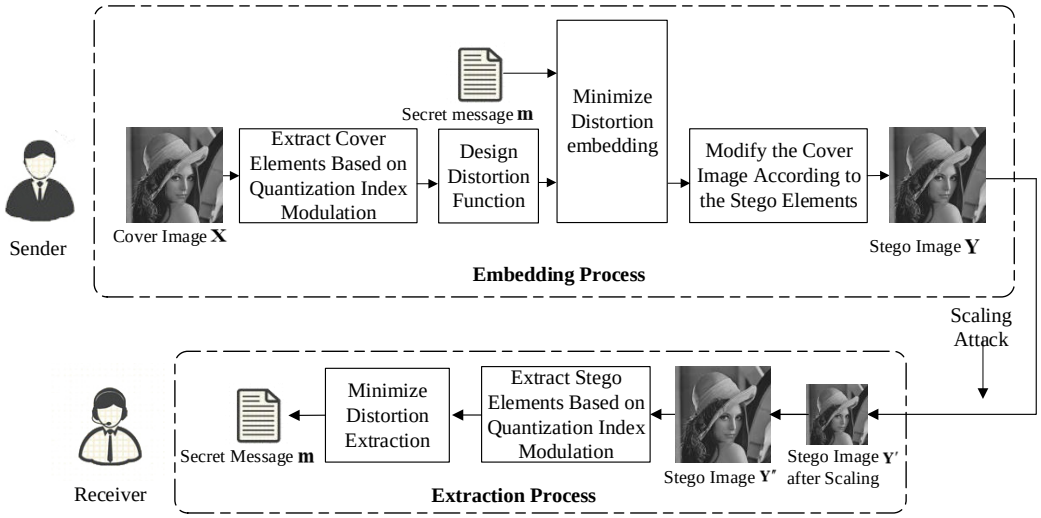


Figure 1: The diagram of the proposed algorithm

Extraction process:

Step 1: Stego image processing. Once again, the stego image $\mathbf{Y}'$ subjected to the scaling attack is scaled to obtain the stego image $\mathbf{Y}''$ with the same size as the original stego image.

Step 2: Extract the stego elements. The robust watermark extraction algorithm based on quantization index modulation is applied to extract the stego elements encoded by STCs in preparation for further extracting the secret message.

Step 3: Minimize distortion decoding. The secret message embedded in the stego elements in the Step 2 is extracted by STCs decoding.

The algorithm proposed uses the robust watermark algorithm based on quantization index modulation to extract the embedded domain and the embedding modification amplitude of the secret message, and combines the distortion function design and STCs coding to embed the secret message into the cover image, which not only maintains the robustness of the algorithm to scaling attack, but also guarantees the anti-detection of the algorithm to a certain extent.

The main steps in the process of embedding and extracting are introduced respectively, including the secret message embedding and extracting algorithm based on quantization index modulation and the design of distortion function based on modification amplitude of cover image.

3.2 Watermarking algorithm based on quantization index modulation

Based on the quantization index modulation algorithm, the new cover elements are extracted from the original cover image, which is convenient to design distortion function and improve the anti-detection performance of the algorithm. And the algorithm is further used to realize the final embedding of stego elements encoded by STCs to enhance its robustness against scaling attacks. The embedding and extraction algorithms are shown in Fig. 2 and Fig. 3, respectively.

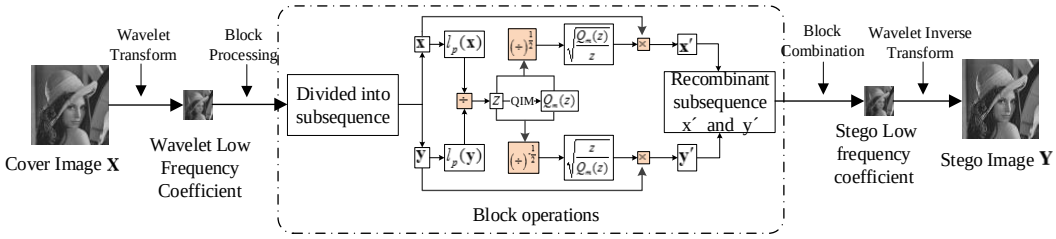


Figure 2: Secret message embedding algorithm based on quantization index modulation

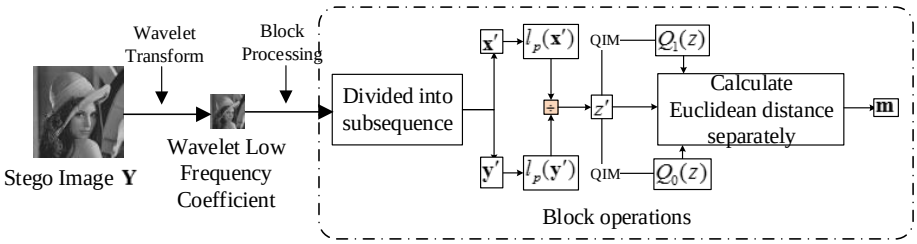


Figure 3: Secret message extraction algorithm based on quantization index modulation

In the embedding process of the algorithm, the cover image is first transformed by wavelet transform, because embedding secret message in the wavelet domain can improve the robustness of the algorithm to the scaling attack. Then the wavelet low frequency coefficients are divided into blocks, the blocks are rearrange into vectors, and for each low frequency coefficient vector, $\mathbf{u}=\{u_1,u_2,...,u_N\}$, it is divided into odd vector $\mathbf{x}$ and even vector $\mathbf{y}$, and $x_i=u_{2i}, y_i=u_{2i-1}$, $i=1,2,...,\frac{2}{N}$, where N is the length of cover vectors. Then calculate the norm of vector $\mathbf{x}$ and $\mathbf{y}$ respectively, the formula is as follows.

$$l_x=(\frac{2}{N}\sum_{i=1}^{N/2}|x_i|^p)^{\frac{1}{p}}, l_y=(\frac{2}{N}\sum_{i=1}^{N/2}|y_i|^p)^{\frac{1}{p}} \tag{6}$$

Then the relative relationship between the two vectors $\mathbf{x}$ and $\mathbf{y}$ is obtained by calculating the ratio of the norm l_p of vectors $\mathbf{x}$ and $\mathbf{y}$, $z=\frac{l_x}{l_y}$. Then the method of quantization index modulation is applied to ratio z to get z_q, and its calculation formula

is as follows.

$$z_q = Q_m(z) = \Delta round(\frac{z + m\Delta/2}{\Delta}) - m\frac{\Delta}{2}, m \in \{0,1\} \tag{7}$$

where Δ is the quantization step, determining the intensity of the modification of the vector. Finally, the values of sub-vectors x and y are modulated according to the ratio between z and z_q to get $\mathbf{x}'$ and $\mathbf{y}'$, and then rearrange $\mathbf{x}'$ and $\mathbf{y}'$ to get $\mathbf{u}'$. Through block combination, wavelet inverse transform, the stego image is finally obtained. The calculation formula of $\mathbf{x}'$ and $\mathbf{y}'$ are as follows.

$$x_i' = \sqrt{\frac{z_q}{z}} x_i = \sqrt{\frac{z_q}{z}} u_{2i}, y_i' = \sqrt{\frac{z}{z_q}} y_i = \sqrt{\frac{z_q}{z}} u_{2i-1} \tag{8}$$

The extraction process of the algorithm is similar to the embedding process. After wavelet transform, the low frequency stego coefficients are divided into blocks. For each block, rearranged into vectors, and each vector $\mathbf{u}'$ is divided into odd vector $\mathbf{x}'$ and even vector $\mathbf{y}'$, calculating the norm l_p' of $\mathbf{x}'$ and $\mathbf{y}'$ respectively, getting the ratio z'. Then $Q_0(z')$ and $Q_1(z')$ modulated z' by quantized modulation after embedding 0 and 1 are calculated respectively, and then calculate Euclidean distance between z' and $Q_0(z')$, $Q_1(z')$. The secret message can be extracted according to the following formula.

$$\hat{m} = \arg\min_{m \in \{0,1\}} | z' - Q_m(z') | \tag{9}$$

The extraction process of this algorithm is relatively simple, as long as knowing the quantization step Δ using when embedding. In the above embedding process, the ratio of the two norms is used to guarantees the relative numerical relationship between scaling sub-vectors. Therefore, the algorithm is robust to scaling attacks and the secret message can be extracted after stego image suffering scaling attacks.

3.3 Design of distortion function based on modification amplitude of cover image

Combining the modified amplitude of the original cover image after embedding 0 and 1 and the definition of the spatial distortion function S-UNIWARD, the embedded distortion of new cover elements are constructed, and the minimum distortion embedding is realized by STCs coding, which can reduce the influence of embedding of secret message to cover image and improve the detection performance. The design schematic diagram of the distortion function is shown below.

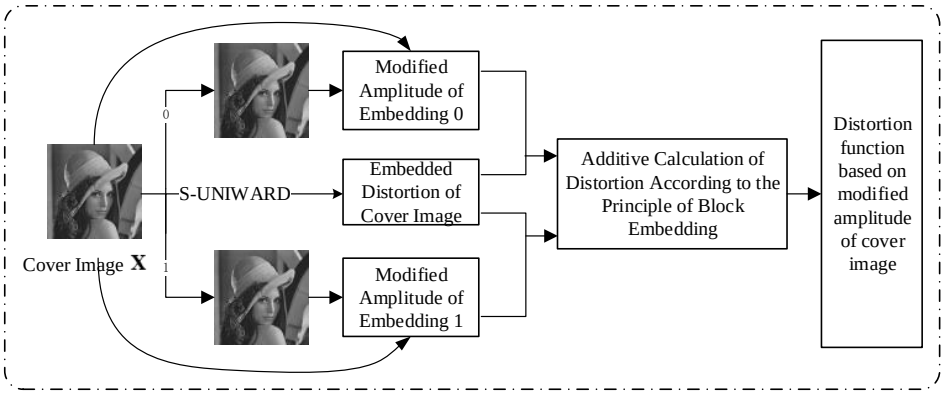


Figure 4: Design schematic diagram of distortion function based on the modification amplitude of cover image

Firstly, the $\pm 1, \pm 2$ and ± 3 distortion of cover image are calculated by S-UNIWARD according to the formula (3).

Then, the secret message embedding algorithm based on quantization index modulation in 3.2 is used to embed 0 and 1 in the original cover image, to generate the stego image $\mathbf{Y}_0$ and $\mathbf{Y}_1$. The modified amplitude of pixel value after embedding 0 and 1 of original cover image is calculated respectively, and the formula is as follows.

$$\mathbf{Def}^m(\mathbf{X}, \mathbf{Y}_m) = p_{\mathbf{X}(i,j)} - p_{\mathbf{Y}_m(i,j)}, m \in \{0,1\} \tag{10}$$

where $p_{\mathbf{X}(i,j)}$ is the pixel value of cover image, and $p_{\mathbf{Y}_m(i,j)}$ is the pixel value after embedding *m*.

The embedding algorithm based on quantization index modulation is to embed 1 bit message in each vector, so the distortion function after embedding 0 and 1 is defined as the sum of the distortion value of all pixel values in each vector.

$$\mathbf{D}_u^m = \sum_{i=1}^{N}\sum_{j=1}^{N} \mathbf{D}^{(k)}(i,j), (i,j = \{1,2,...,N\}) \tag{11}$$

where $\mathbf{D}_u^m$ is the total distortion value in block $\mathbf{u}$ when embedding *m*, $m \in \{0,1\}$. $\mathbf{D}^{(k)}(i,j)$ is the distortion value of pixel (i,j) when $\pm k$, $k = \mathbf{Def}^m(i,j)$ is the modified amplitude when embedded *m*.

By means of the above distortion calculation, we can get the distortion value of the new cover element embedding 0 and 1. In addition, when we pre-embed 0 and 1, the distortion in the vector $\mathbf{u}$ where the extraction error occurred is $wet\cos t$, which means this block is less resistant to scaling attacks and is not suitable for embedding.

4 Performance analysis

4.1 Anti-scaling performance analysis

Compared with S-UNIWARD steganography algorithm, the proposed steganography algorithm based on quantization index modulation improves the correct extraction rate of secret message after scaling attack. However, under the low scaling factor, compared with the robust algorithm based on quantization index modulation, the correct extraction rate of secret message is slightly lower. Because the algorithm proposed uses STCs code to embed and extract secret message, there is error diffusion in STCs decoding, that is, if the stego elements STCs encoded in extraction Step 2 has errors, using STCs decoding in Step 3 will result in a larger extraction error.

The principle of correct message extraction and error diffusion during STCs decoding is shown in formulas (12) and (13). Hypothesis sub-check matrix $\hat{\mathbf{H}}=\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}$, $h=2$ and $w=2$ are the height and width of $\hat{\mathbf{H}}$, respectively. $\mathbf{H}$ is a parity-check matrix. $\mathbf{y}=(y_1,y_2,...,y_n)'$ and $\mathbf{y}'=(y_1',y_2,...,y_n)'$ are the stego sequences before and after scaling, $\mathbf{m}$ and $\mathbf{m}'$ are the sequences of secret messages extracted before and after scaling. The secret messages can be extracted exactly and correctly in the stego sequence $\mathbf{y}$ before scaling. However, a 1-bit error in the stego sequence will result in a 2-bit error in the extracted secret message $\mathbf{m}'$ after scaling. The position of the red mark in $\mathbf{y}'$ indicates the position where the error occurred in the stego sequence after scaling, and the position of the red mark in $\mathbf{H}$ indicates the position associated with the error in $\mathbf{y}'$.

$$\mathbf{m}=\mathrm{Ext}(\mathbf{y})=\mathbf{H}\mathbf{y}=\begin{pmatrix}1 & 1 & & & & & & & & \\ 1 & 0 & 1 & 1 & & & & & & \\ & & 1 & 0 & 1 & 1 & & & & \\ & & & & 1 & 0 & & & & \\ & & & & & & \ddots & & & \\ & & & & & & & 1 & 1 & \\ & & & & & & & 1 & 0 & 1 & 1\end{pmatrix}\begin{pmatrix}y_1\\ y_2\\ y_3\\ \vdots\\ y_n\end{pmatrix}=\begin{pmatrix}y_1+y_2\\ y_1+y_3+y_4\\ y_3+y_5+y_6\\ y_5+y_7+y_8\\ \vdots\\ y_{n-5}+y_{n-3}+y_{n-2}\\ y_{n-3}+y_{n-1}+y_n\end{pmatrix} \tag{12}$$

$$\mathbf{m}'=\mathrm{Ext}(\mathbf{y}')=\mathbf{H}\mathbf{y}'=\begin{pmatrix}1 & 1 & & & & & & & & \\ 1 & 0 & 1 & 1 & & & & & & \\ & & 1 & 0 & 1 & 1 & & & & \\ & & & & 1 & 0 & & & & \\ & & & & & & \ddots & & & \\ & & & & & & & 1 & 1 & \\ & & & & & & & 1 & 0 & 1 & 1\end{pmatrix}\begin{pmatrix}y_1'\\ y_2\\ y_3\\ \vdots\\ y_n\end{pmatrix}=\begin{pmatrix}y_1'+y_2\\ y_1'+y_3+y_4\\ y_3+y_5+y_6\\ y_5+y_7+y_8\\ \vdots\\ y_{n-5}+y_{n-3}+y_{n-2}\\ y_{n-3}+y_{n-1}+y_n\end{pmatrix} \tag{13}$$

This is because there are at most h elements in any column of the check matrix $\mathbf{H}$ that are not zero. When $y_i' \in \mathbf{y}'$ goes wrong, it affects at most h bit in embedded message, that is, the upper limit of the error diffusion is h-fold of the error bit occurred in $\mathbf{y}'$.

4.2 Anti-detection performance analysis

Compared with the original watermarking algorithm, the image steganography algorithm proposed based on quantization index modulation improves the detection resistance, which is because the algorithm based on the original watermarking algorithm, combined with the distortion function design and the principle of minimizing distortion embedding, makes the message embedding minimize the modification to cover image, so as to improve the detection resistance.

Fig. 5 is the schematic diagram of the proposed algorithm for improving detection resistance. After embedding with distortion function and STC encoding, the amount of modifications generated in the stego elements relative to the cover elements are smaller than the original quantization index modulation algorithm. The stego elements with the red mark represent the modified elements after STCs encoding in embedding Step 3. For the stego elements not modified after embedding, the corresponding positions of the original cover image are not changed at the end of embedding in embedding Step 4, resulting in a smaller embedding distortion.

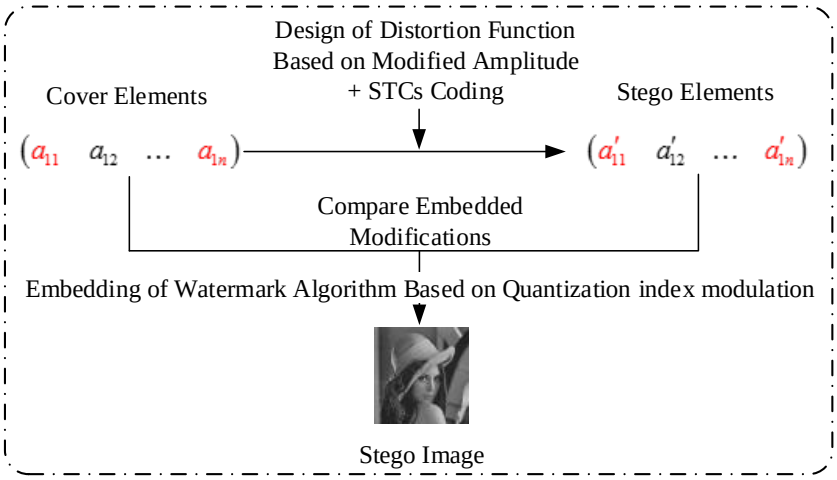


Figure 5: Schematic diagram of the proposed algorithm's resistance to detection

5 Experimental results and analysis

In order to verify the effectiveness of the proposed algorithm in this paper, we apply the robust watermarking algorithm in the document [Zareian and Tohidypour (2014)], the algorithm proposed and S-UNIWARD respectively in the MATLAB R2015a to realize the embedding and extracting of the message. The SPAM feature [Pevn, Bas and Fridrich (2010)] of the cover image and the stego image are extracted respectively to test the detection performance. The 2000 original images are randomly selected in BossBase-1.01

Image Library with the size 512×512. The binary sequences are randomly generated as secret message sequences to be embedded.

The parameters of the algorithm are as follows: the bits of secret message are fixed at 96 bit; the scaling factor is varied from 0.25 to 2.0 in 0.25 increments; the three common interpolation method is used to scale the stego image; the distortion constant $wet\cos t = 10^{13}$; the norm $p = 2$, the length of a single segmented vector is 32.

5.1 Parameter Δ selection

Parameter Δ is the quantization step, it determines the extent to which the embedded message modifies the cover image. If it is too small, it is difficult to resist scaling attack, but if it is too large, the embedding will cause greater distortion to cover image, and the anti-detection performance is poor. Therefore, the purpose of this experiment is to find an optimal value for Δ making the algorithm proposed have maximum robustness along with maximum anti-detection.

In this paper, 2000 images are embedded and extracted using the algorithm proposed, and the quantization step Δ is varied from 0.02 to 0.1 in 0.02 increments. In this section, the bilinear interpolation method is used to scale the images, and the scaling factors are 0.25, 0.5, 0.75 and 1. The average extraction error rate and detection error rate in the 2000 images are obtained with the growth of Fig. 6 under different scaling factors.

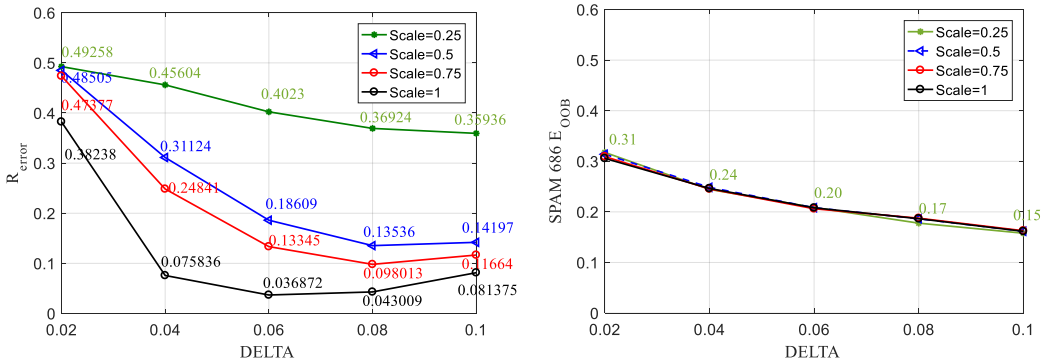


Figure 6: Extraction error rate of secret message under different quantization steps (left); Detection error rate of stego images under different quantization steps (right)

From the graph, when the parameter $\Delta < 0.06$, the change of the curve in the graph is larger, but when $\Delta > 0.06$, the change tends to smooth. In order to balance the anti-scaling performance and anti-detection performance of the algorithm, this paper chooses a compromise value to make the quantization step $\Delta = 0.06$, which not only can maintain the anti-detection, but also can guarantee the secret message to be extracted completely and correctly after scaling higher probability.

5.2 Scaling attack resistant experiment

This section tests the algorithm performance in two parts of anti-scaling performance test and anti-scaling comparison experiment. 2000 images are secret randomly in BossBase-

1.01 image library to embed the message and generate stego images. Then scale the stego images extract the secret message. The anti-scaling performance is evaluated through the average extraction bit error rate and exactly correct extraction rate of the secret message. The average extraction bit error rate $R_{error} = \frac{n_{error}}{n}$, Where n_{error} is the number of message bits extracted mistakenly, and *n* is the total number of embedded message. The extraction rate exactly correct $R_{right} = \frac{N_{right}}{N}$, N_{right} is the number of the stego images that can be extract the secret message completely and correctly, N is the total number of the stego images.

5.2.1 Anti-scaling performance test experiment

The nearest neighbor interpolation method, bilinear interpolation method and bicubic interpolation method are used to scale the 2000 stego images, the scaling factors are from 0.25 to 2, interval 0.25, and then the secret messages are extracted from the scaled stego images. The average bit error rate and the correct extraction rate of the secret message from the 2000 stego images are obtained as shown in Fig. 7.

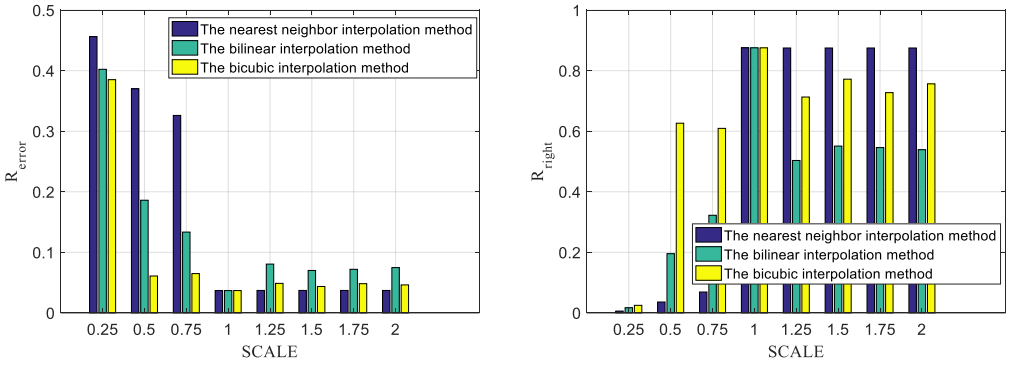


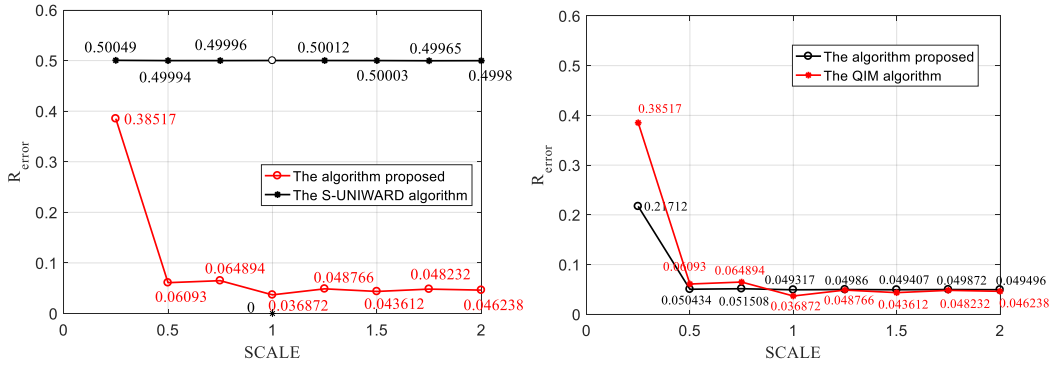
Figure 7: The average bit error rate of secret message under different scaling factors (left); the correct extraction rate of secret message under different scaling factors (right)

Fig. 7 shows that, with the scaling factor being less than 1, the average bit error rate of secret message decreases with the increase of the scaling factor, and the number of stego images that can extract the message completely and correctly increases. Because as the scaling factor increases, the loss of the secret message in the image decreases, the extraction error rate is reduced. At the same time, it can be seen that the algorithm is best for bicubic interpolation scaling attack. Using the bicubic interpolation method to scale the image, the scaled pixel is obtained by the weighted of the 16 pixels around it, so the computational complexity is the highest and the distortion of scaled image is the most accurate, so as to the bit error rate is lowest. Also, when the scaling factor is greater than 1, the bit error rate of massage in the stego images suffering the nearest neighbor interpolation method is lower than the other two interpolation methods. This is because when the nearest neighbor interpolation method is used to enlarge the image, the new

pixels to be inserted are the original pixels closest to the new pixels coordinate. When scaled to the original size, the pixels of the stego image change little, so the bit error rate is the lowest.

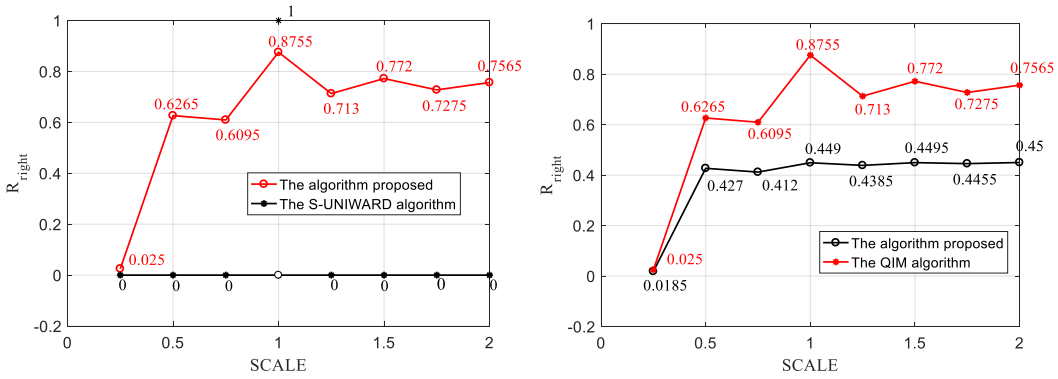
5.2.2 Anti-scaling comparison experiment

2000 spatial images are randomly selected, and S-UNIWARD adaptive steganography algorithm [Holub and Fridrich (2013)], the algorithm proposed in this paper and the robust watermarking algorithm in Zareian et al. [Zareian and Tohidypour (2014)] are used to embed the secret message and generate stego images. Bicubic interpolation is used to scale the stego images and then extract the secret message. Fig. 8 is the average bit error rate of secret message extracted for the stego images after scaling. Fig. 9 is the extraction rate exactly correct of secret message.



(a) (b)

Figure 8: Extraction error rate of secret message under different scaling factors



(a) (b)

Figure 9: Extraction rate exactly correct of secret message under different scaling factors

Fig. 8(a) shows that when the scaling factor is not 1, the extraction bit error rate of S-UNIWARD steganography algorithm is higher, which is about 50%, equivalent to random guessing. However, the correction rate of extracting message in 2000 stego images generated by the algorithm proposed is over 93% when the scaling factor is

greater than 0.5. Fig. 8(b) shows that the error rate of extracting message is flat with the original watermarking algorithm. When the scaling factor is 0.25, the algorithm proposed is higher, because the error diffusion of STCs coding, which leads to increase in error rate.

In order to further illustrate the resistance of the algorithm to scaling attack, we also make a further statistic on the extraction rate exactly correct of secret message under different scaling factors, as shown in Fig. 9. For 2000 testing images, the stego images obtained by S-UNIWARD steganography algorithm after scaling attacks cannot extract the secret message exactly and correctly. For the proposed algorithm, when the scaling factor is 0.5, the proportion of message extracted completely and correctly is 62.65%, which is 20% higher than the original watermark algorithm.

5.3 Statistical detection resistant experiment

The SPAM feature [Pevn, Bas and Fridrich (2010)] of the original cover image, the stego image generated by the robust watermarking algorithm in literature [Zareian and Tohidypour (2014)], the proposed algorithm in this paper are extracted respectively. The average detection error rate E_{OOB} is shown in Fig. 10 using the Ensemble Classifier for training and testing.

The experimental results show that under the SPAM feature, the robustness of the proposed algorithm is about 2% higher than the original robust watermarking algorithm. Under the premise of no scaling attack, the detection of this algorithm is much lower than S-UNIWARD adaptive steganography algorithm. This is because under the same embedding rate, taking the 'Lena' as an example, the S-UNIWARD steganography algorithm changes the image to about $13/262144$ ($4.959106e^{-5}$), however, in order to improve the anti-scaling performance of this algorithm, the change of the cover image is about $50/128$ (0.390625). In order to improve the anti-scaling attack performance of this algorithm, only sacrificing some resistance detection, this is the reason why the algorithm detection error rate is lower than S-UNIWARD steganography algorithm.

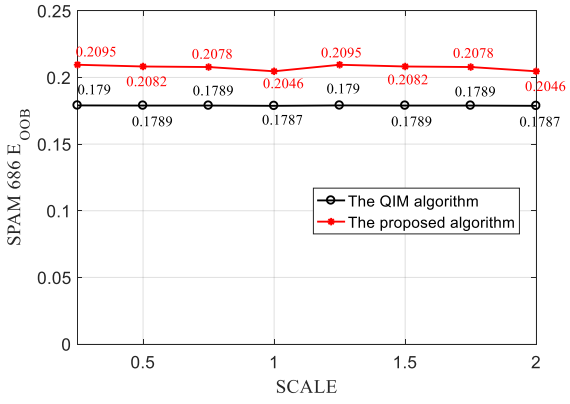


Figure 10: Detection error rate under different scaling factors

6 Conclusion

For the existing adaptive steganography algorithm is difficult to resist scaling attacks, and our earlier proposed algorithm resisting scaling attack and statistical detection only for the nearest neighbor interpolation scaling attack, this paper presents an image adaptive steganography algorithm based quantization index modulation of anti-scaling attacks and statistical detection. The algorithm first draws on the robust watermarking algorithm based on quantization index modulation to determine the embedded domain and embedding mode of secret message. Then, the spatial distortion function S-UNIWARD is used to construct the new embedding distortion, and the STCs code is used to embed the secret message, which improves the anti-detection performance of the algorithm while ensuring the robustness against scaling attack. The experimental results show that the average correct extraction rate of embedded messages increases from 50% to over 93% after 0.5 times scaling attack, compared with the classical steganography algorithm of S-UNIWARD, and the algorithm has higher detection resistance than the original watermarking algorithm based on quantization index modulation. But the algorithm proposed in this paper is implemented under low embedding rate, so next we will study how to improve the embedding rate of the algorithm.

Acknowledgement: 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).

References

Chen, B.; Wornell, G. W. (2001): Quantization index modulation: A class of provably good methods for digital watermarking and information embedding. *IEEE Transactions on Information Theory*, vol. 47, no. 4, pp. 1423-1443.

Guo, L.; Ni, J.; Shi, Y. Q. (2012): An efficient JPEG steganographic scheme using uniform embedding. *Proceedings of IEEE International Workshop on Information Forensics and Security*, pp. 169-174.

Holub, V.; Fridrich, J. (2012): Designing steganographic distortion using directional filters. *Proceedings of the 4th IEEE International Workshop on Information Forensics and Security*, vol. 2, no. 4, pp. 234-239.

Holub, V.; Fridrich, J. (2013): Digital image steganography using universal distortion. *Proceedings of ACM Workshop on Information Hiding and Multimedia Security*, pp. 59-68.

Han, D. (2013): Comparison of commonly used image interpolation methods. *ICCSEE-13.*

Kim, B. S.; Choi, J. G.; Park, C. H.; Won, J. U.; Kwak, D. M. (2003): Robust digital image watermarking method against geometrical attacks. *Real-Time Imaging*, vol. 9, no. 2, pp. 139-149.

Li, B.; Wang, M.; Huang, J.; Li, X. (2014): A new cost function for spatial image steganography. *Proceedings of International Conference on Image Processing*, pp. 4206-4210.

Luo, X. Y.; Song, X. F.; Li, X. L.; Zhang, W. M.; Lu, J. C. et al. (2016): Steganalysis of HUGO steganography based on parameter recognition of syndrome-trellis-codes. *Multimedia Tools and Applications*, vol. 75, no. 21, pp. 13557-13583.

Lin, Z.; Niu, L.; Jiang, X. (2015): A method on digital watermarking image against geometric distortion. *Proceedings of International Conference on Image Processing*, pp. 130-134.

Ma, Y. Y.; Luo, X. Y.; Li, X. L; Bao, Z. K.; Zhang, Y. (2018): Selection of rich model steganalysis features based on decision rough set α-positive region reduction. *IEEE Transactions on Circuits and Systems for Video Technology*.

Naderahmadian, Y.; Beheshti, S. (2015): Robustness of wavelet domain watermarking against scaling attack. *Electrical & Computer Engineering*, pp. 1218-1222.

Pevný, T.; Filler, T.; Bas, P. (2010): Using high-dimensional image models to perform highly undetectable steganography. *Lecture Notes in Computer Science*, vol. 6387, pp. 161-177.

Pevn, T.; Bas, P.; Fridrich, J. (2010): Steganalysis by subtractive pixel adjacency matrix. *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 215-224.

Sedighi, V.; Cogranne, R.; Fridrich, J. (2016): Content-adaptive steganography by minimizing statistical detectability. *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 2, pp. 221-234.

Tomas, F.; Judas, J.; Fridrich, J. (2011): Minimizing additive distortion in steganography using syndrome-trellis codes. *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 920-935.

Zareian, M.; Tohidypour, H. R. (2014): A novel gain invariant quantization-based watermarking approach. *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 11, pp. 1804-1813.

Zhang, Y.; Luo, X. Y.; Yang, C. F.; Ye, D. P.; Liu, F. L. (2015): A JPEG-Compression resistant adaptive steganography based on relative relationship between DCT coefficients. *Proceedings of International Conference on Availability, Reliability and Security*, pp. 461-466.

Zhang, Y.; Luo, X. Y.; Yang, C. F.; Liu, F. L. (2016): Joint JPEG compression and detection resistant performance enhancement for adaptive steganography using feature regions selection. *Multimedia Tools and Applications*, pp. 1-20.

Zhang, Y.; Qin, C., Zhang, W. M.; Liu, F. L.; Luo, X. Y. (2018): On the fault-tolerant performance for a class of robust image steganography. *Signal Processing*, vol. 146, pp. 99-111.