IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON RECENT ADVANCES IN VIDEO CODING AND SECURITY

Received January 21, 2019, accepted February 6, 2019, date of publication February 20, 2019, date of current version March 7, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2900286

Zernike Moment-Based Spatial Image Steganography Resisting Scaling Attack and Statistic Detection

YUE ZHANG[1], XIANGYANG LUO[1], YANQING GUO[2], CHUAN QIN[3], AND FENLIN LIU[1]

[1]State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450000, China
[2]School of Information and Communication Engineering, Dalian University of Technology, Dalian 116024, China
[3]School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China

Corresponding author: Xiangyang Luo (xiangyangluo@126.com)

This work was supported in part by the National Natural Science Foundation of China under Grant U1636219, Grant U1736119, Grant 61772549, Grant U1736214, and Grant U1804263, in part by the National Key R&D Program of China under Grant 2016YFB0801303 and Grant 2016QY01W0105, and in part by the Plan for Scientific Innovation Talent of Henan Province under Grant 2018JR0018.

ABSTRACT The mainstream adaptive steganography algorithm is difficult to resist scaling attack, and the anti-detection performance of the algorithm based on quantization index modulation is not high enough. To solve the above problems, this paper proposes a spatial image adaptive steganography algorithm based on Zernike moment to resist scaling attack and statistic detection. First, the Zernike moment of the normalized cover image is extracted and the new cover is obtained by the dither modulation algorithm. Second, the minimized distortion embedding is realized by Spatial UNIversal WAvelet Relative Distortion (S-UNIWARD) and syndrome-trellis codes coded. And finally, the stego image is generated by changing the original Zernike moment according to the modified amplitude of the new cover. The experimental results show that the proposed algorithm is robust to the three common scaling attacks, and the message extraction error rate is significantly lower than the S-UNIWARD steganography after the scaling attacks; moreover, compared with the steganography algorithm based on quantization index modulation, the proposed algorithm has higher detection resistance.

INDEX TERMS Steganography algorithm, scaling attack, statistic detection, zernike moment.

I. INTRODUCTION

The steganography technology embeds the secret messages into the cover image through a specific algorithm to realize covert communication. Most of the current adaptive steganography algorithms embed the secret messages into the image texture complex area through distortion function design and the STCs (syndrome-trellis codes) code [1] to enhance the detection. However, the adaptive steganography usually can't extract the secret messages exactly and correctly when the stego image suffer from image processing attacks, such as compression, scaling, and so on. Similar situations exist in other multimedia fields such as video [2], [3]. In practice, most digital images are obtained and transmitted through electronic devices such as mobile phones and tablets, while others are computer generated images [4]. Due to the restriction of network bandwidth and software processing ability, images are often processed by scaling and so on during transmission. The adaptive steganography algorithms can no longer meet the demand of anti-scaling attack. Therefore, it is necessary to study a new image steganography algorithm which can resist both scaling attack and statistic detection.

For anti-detection performance, the current mainstream adaptive steganography algorithms have a high anti-detection performance by the design distortion function. With the further study of adaptive steganography, the types of distortion function are various, and their resistance to statistic detection becomes higher and higher [5]. Typical spatial adaptive steganography algorithms such as HUGO (Highly Undetectable steGOnography) [6], [7], uses the weighted sum of the SPAM feature [8] difference of the cover and stego as a measure of the distortion. The algorithm guarantees the high dimensional statistical model of the embedded image. WOW (Wavelet Obtained Weights) [9] uses the wavelet filter group to filter the cover image in multiple directions. Compared with HUGO steganography, and has a higher resistance

The associate editor coordinating the review of this manuscript and approving it for publication was Zhaoqing Pan.

to detection. S-UNIWARD (Spatial UNIversal WAvelet Relative Distortion) [10] uses the relative change rate of the decomposition coefficient of its directional filter as a measure of distortion to further improve the anti-detection performance. At the same time, J-UNIWARD (JPEG Universal Wavelet Relative Distortion) steganography algorithm is proposed in [11] for frequency domain. With further research, the anti-detection performance of image adaptive steganography algorithms has been greatly improved. However, most steganography algorithms often have a high message extraction error rate after scaling attack [12].

For anti-scaling attack performance, some common watermarking algorithms against geometric attacks have studied extensively. Kim *et al.* [13] used the logarithmic polar plot in the spatial domain by improving the Fourie-Mellin transform, using the image centroid as the origin of the LPM (Log-Polar Map), and then performing the DFT (Discrete Fourier Transform) on the LPM image and extracting its amplitude to obtain the RST (Rotation, Scaling, Translation) invariant domain. In [14], a method based on feature point and image transform is proposed to embed watermark massages into DCT (Discrete Cosine Transform) coefficients. When the watermark image is scaled 0.8 times, the correct rate is 93.75%. In [15], the cover signal is subjected to DWT, and then the watermark messages are embedded by quantifying the ratio of p-norm of the LL domain coefficients. Experimental results show that when the scaling factor is 0.5, the watermark messages can still be extracted completely. In [16], the Zernike moments of normalized image are used as watermark embedding cover to achieve robustness to scaling attacks. The algorithm in [17] calculates the amplitude of the image Zernike moments, embeds the messages through the dither modulation algorithm, and finally extracts the messages from the amplitude of the watermark image Zernike moments through the Euclidean distance. Most of these watermarking algorithms embed the secret messages in the region insensitive to scaling attacks, and use an embedding algorithm resisting scaling attacks, which greatly improves the robustness of the algorithms to various image processing attacks such as scaling. However, only a few algorithms can ensure the secret messages completely extracted after scaling attacks, and most of these watermarking algorithms modify the main content of the cover image to improve the robustness, often resulting in relatively large image distortion. Therefore, its anti-detection performance is poor.

For the influence of image processing attacks on steganography algorithms, Zhang [18]–[20] has researched and proposed image steganography algorithms which can resist both JPEG compression and statistic detection, and we also proposed image steganography algorithm which can resist both scaling attack and statistic detection in [12]. However, the method in [12] is only effective for the nearest neighbor interpolation scaling processing, and the anti-detection performance in [21] needs to be improved.

Based on the above research, the paper analyzes the scaling invariance of the Zernike moment, and proposes a spatial image adaptive steganography algorithm based on Zernike moment to resist scaling attack and statistic detection. The amplitude of Zernike moment after image normalization is extracted, and the new embedded cover and embedding algorithm are obtained by dither modulation algorithm to increase its scaling resistance. Based on the S-UNIWARD steganography, the distortion function of the new cover is designed, and the STCs encoding is used to minimize the distortion embedding.

The remainder of this paper is organized as follows. In the second section, the principle of Zernike moment and its invariance are briefly described. The third section expounds the principle frame of the algorithm proposed and the implementation of the concrete steps. The fourth section tests the algorithm from two aspects of anti-scaling and anti-detection; and the fifth section is the conclusion.

II. ZERNIKE MOMENTS AND INVARIANCE ANALYSIS

As a powerful feature descriptor, Zernike moment has been used in the field of pattern recognition, image processing and robust watermarking algorithms. This section explains how to implement RST invariance, especially scaling invariance, by simply describing the Zernike moment. The m-th n-order Zernike moment is defined as follows.

$$A_{nm} = \frac{n+1}{\pi} \iint_{x^2+y^2 \le 1} f(x,y) V^*_{nm}(x,y) dxdy \tag{1}$$

where n is a non-negative integer, $n - |m|$ is an even number and satisfies $n \ge |m|$. The complex value function $V_{nm}(x, y)$ is Zernike polynomial. $V^*_{nm}(x, y)$ is the conjugate of $V_{nm}(x, y)$. $V_{nm}(x, y)$ is defined as follows.

$$V_{nm}(x,y) = V_{nm}(\rho,\theta) = R_{nm}(\rho) e^{jm\theta} \tag{2}$$

where ρ and θ are the polar coordinates of the unit circle, $\rho = \sqrt{x^2+y^2}$ represents the vector length from the origin to the pixel(x, y), and $\theta = \tan^{-1}(y/x)$ is the angle between counter-clockwise vector ρ and the x-axis. $R_{nm}(\rho)$ is a real-valued radial polynomial whose formula is as follows.

$$R_{nm}(\rho) = \sum_{s=0}^{(n-|m|)/2} (-1)^s \frac{[(n-s)!]}{s!(\frac{n+|m|}{2}-s)!(\frac{n-|m|}{2}-s)!} \rho^{n-2s} \tag{3}$$

For a given digital image, equation (1) is replaced by summation, and the equation (4) is calculated.

$$A_{nm} = \frac{n+1}{\pi} \sum_x \sum_y f(x,y) V^*_{nm}(\rho,\theta), \quad x^2+y^2 \le 1 \tag{4}$$

The Zernike moment of the image only has rotational invariance [22]. In order to achieve the scaling invariance, the image must be normalized firstly, which means the center of mass of the image is coincident with the center of the unit circle, and the image into a standard size. For the image $f(x, y)$, the normalized image $g(x, y)$ is calculated as follows.

$$g(x,y) = f(\frac{x}{m_{00}} - \bar{x}, \frac{y}{m_{00}} - \bar{y}) \tag{5}$$

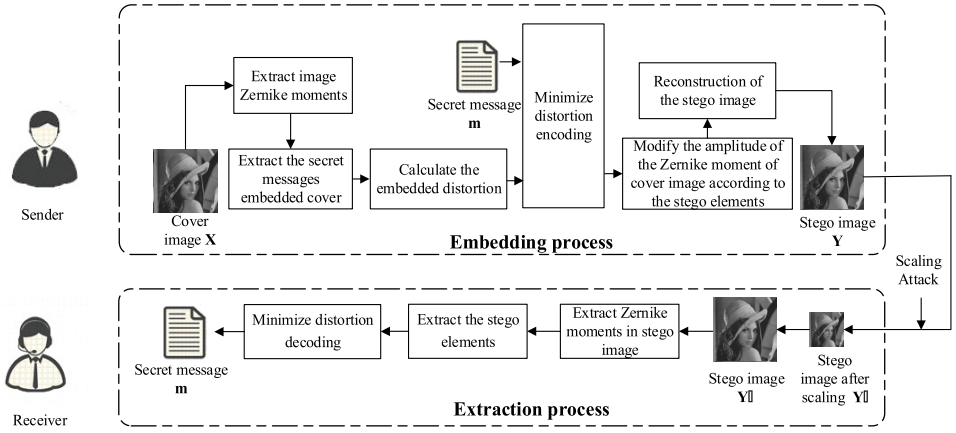

FIGURE 1. The diagram of the proposed algorithm.

where $(\bar{x}, \bar{y})$ is the centroid of the image $f(x, y)$. m_{00} is the zero-order standard moment of the image. Finally, the Zernike moment of the normalized image $g(x, y)$ has RST invariance.

Because of the orthogonality of Zernike moment, the image $f(x, y)$ can be reconstructed by Zernike moment.

$$f(x, y) = \sum_{n=0}^{\infty} \sum_{m} A_{nm} V_{nm}(\rho, \theta) \tag{6}$$

III. THE PROPOSED ALGORITHM

In order to further enhance the anti-scaling of steganography algorithm and improve anti-detection performance, we propose a spatial image steganography algorithm based on Zernike moment resisting scaling attack and statistic detection. The algorithm combines Zernike moment and dither modulation algorithm to obtain a new messages embedding cover and embedding algorithm, which guarantees the robustness for scaling attack. At the same time, the distortion function of the new cover is constructed using the S-UNIWARD algorithm to ensure the anti-detection performance. The principle frame of the proposed algorithm and the main steps of the algorithm embedding and extracting are introduced in the following section.

A. ALGORITHM PRINCIPLE ARCHITECTURE

Figure 1 is a schematic diagram of the adaptive steganography algorithm based on Zernike moment resisting scaling attack and statistic detection. The embedding process and the extraction process are described as figure 1.

1) EMBEDDING PROCESS

Step 1 (Extract the Secret Messages Embedded Cover): Based on Zernike moment and dither modulation extraction algorithm, the new cover of secret messages is extracted, and the preference of messages embedding is obtained, which facilitates the design of distortion function and the realization of STCs coding.

Step 2 (Calculate the Embedded Distortion): Using the dither modulation embedding algorithm to embed 0 and 1 in new cover, the new distortion function is constructed by the modified amplitude of original image using spatial S-UNIWARD distortion function.

Step 3 (Minimize Distortion Encoding): Use the minimum distortion coding STCs to embed secret messages in the new cover elements to generate the stego elements. The message embedding can minimize the change of new cover elements so as to achieve anti-detection.

Step 4 (Modify the Amplitude of the Zernike Moment of Cover Image According to the Stego Elements): According to the modified amplitude of the new cover elements by secret messages, the stego elements coded by STCs is embedded in the amplitude of the Zernike moment of the original cover image using the dither modulation algorithm.

Step 5 (Reconstruction of the Stego Image): The stego Zernike moment is used to reconstruct the image and generate the stego image.

2) EXTRACTION PROCESS

Step 1 (Stego Image Processing): Once again, the stego image subjected to the scaling attack is scaled to obtain the stego image with the same size as the original stego image.

Step 2 (Extract the Stego Elements): The robust extraction algorithm based on Zernike moment and dither 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 messages embedded in the stego elements in the step 2 is extracted by STCs decoding.

The algorithm uses the scaling invariance of the Zernike moment, the distortion function design and the STCs encoding to embed the secret messages into the amplitude of the Zernike moment of the cover image, which not only keeps the robustness to the scaling attack, at the same time, the method combining the distortion function design with the STCs coding can also ensure the anti-detection performance.

The following describes the main steps in the embedding and extraction process, the message embedding and extraction algorithm based on Zernike moments and dither modulation, and the distortion function design method based on the amplitude of the cover image.

B. THE ALGORITHM BASED ON ZERNIKE MOMENTS AND DITHER MODULATION

Using the algorithm based on Zernike moment and dither modulation, the new cover elements are extracted from the amplitude of Zernike moment of the original cover image, and the preference of message embedding is obtained so as to facilitate the design of distortion function and the realization of STCs coding, and to improve its anti-detectability. Further using the algorithm to realize the final embedding of STCs encoded secret messages is helpful to enhance the robustness to scaling attack. The algorithm as shown in Figure 2.

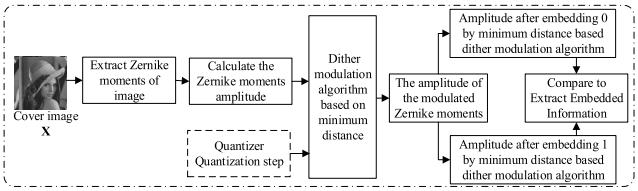

FIGURE 2. The algorithm diagram based on Zernike moments and dither modulation.

According to the scaling invariance of normalized Zernike moment, the amplitude normalized Zernike moment can be used as the embedded domain to achieve the resistance of scaling attack. Then, the amplitude of the stego Zernike moment is obtained by embedding the messages using dither modulation algorithm, which can improve the robustness to scaling attack. In the extraction process, the difference between the amplitude of the Zernike moment of the stego image and the new amplitude of embedding 0 and 1 is calculated respectively to extract the embedded message.

The amplitude of the Zernike moment of normalized cover image is A. The amplitude of the Zernike moment after embedding is A'. Quantization step is Δ. Quantizer is $d = [d, d + \Delta/2]$. The secret message to embed is w, where $w \in \{0, 1\}$. In order to enhance the robustness of the algorithm, the message embedding algorithm in the amplitude of the Zernike moment is as follows.

$$A_i' = \begin{cases} [(A_i - d)/\Delta] * \Delta + d, & w_i = 0 \\ \left[(A_i - \dfrac{d+\Delta}{2})/\Delta\right] * \Delta + \dfrac{d+\Delta}{2}, & w_i = 1 \end{cases} \tag{7}$$

The above formula indicates, according to the different bits of message to be embedded, the amplitude of the Zernike moment is modulated into different locations to achieve the embedding of information. In the message extraction phase, the amplitude of the normalized Zernike moment of the stego image is first obtained, and then the message is extracted by the following formula.

$$\begin{aligned} A_i^0 &= \left|A_i'' - \left[(A_i'' - d)/\Delta\right] * \Delta - d\right| \\ A_i^1 &= \left|A_i'' - \left[(A_i'' - \frac{d+\Delta}{2})/\Delta\right] * \Delta - \frac{d+\Delta}{2}\right| \end{aligned} \tag{8}$$

where A_i'' represents the amplitude of the Zernike moment extracted from the stego image. A_i^0 represents the difference between A_i'' and the amplitude change when embedding 0 into A_i'', and A_i^1 represents the difference between A_i'' and the amplitude change when embedding 1 into A_i''. The embedded secret message bit can be extracted according to the following formula.

$$w_i' = \begin{cases} 0, & A_i^0 < A_i^1 \\ 1, & A_i^0 > A_i^1 \end{cases} \tag{9}$$

C. THE DISTORTION FUNCTION DESIGN BASED ON THE COVER MODIFICATION AMPLITUDE

Combining the modification amplitude of the original cover image after embedding 0 and 1 using the dither modulation algorithm, the embedding distortion of the new cover elements is constructed by S-UNIWARD steganography algorithm. Then the minimum distortion embedding is realized by STCs encoding, which can reduce the influence of the secret message embedding on the cover image. The design principle of the distortion function is shown in the following figure.

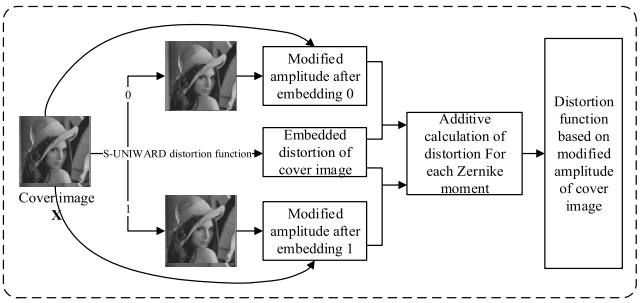

FIGURE 3. The design of distortion function based on the cover modification amplitude.

First, ±1, ±2 and ±3 distortion of cover image are calculated by S-UNIWARD according to the following formula.

$$\mathrm{D}(\mathbf{X}, \mathbf{Y}) = \sum_{k=1}^{3} \sum_{u=1}^{n_1} \sum_{v=1}^{n_2} \frac{\left|\mathrm{W}_{uv}^{(k)}(\mathbf{X}) - \mathrm{W}_{uv}^{(k)}(\mathbf{Y})\right|}{\sigma + \left|\mathrm{W}_{uv}^{(k)}(\mathbf{X})\right|} \tag{10}$$

where X and 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. $\sigma > 0$ is a constant used to stabilize numerical computations.

Then the algorithm based on Zernike moment and dither modulation introduced in Section 3.2 is applied to embed 0 and 1 respectively in the Zernike moment amplitude of the

original cover image, and to generate the spatial stego images $\mathbf{Y}_0$ and $\mathbf{Y}_1$. The cover modification amplitude is calculated by the following formula.

$$\mathbf{Dif}^{w}(\mathbf{X}, \mathbf{Y}_w) = p_{\mathbf{X}(i,j)} - p_{\mathbf{Y}_w(i,j)}, \quad w \in \{0, 1\} \tag{11}$$

where $\mathbf{Y}_w \in \{\mathbf{Y}_0, \mathbf{Y}_1\}$, $p_{\mathbf{X}(i,j)}$ is the pixel value of cover image in each pixel. $p_{\mathbf{Y}_w(i,j)}$ is the pixel value of $\mathbf{Y}_0$ and $\mathbf{Y}_1$ in each pixel. $\mathbf{Dif}^{w}(\mathbf{X}, \mathbf{Y}_w)$ is the difference between cover image X and stego images $\mathbf{Y}_0$ and $\mathbf{Y}_1$, which means the modification amplitude. If $\mathbf{Dif}^{w}(\mathbf{X}, \mathbf{Y}_w) \notin \{\pm1, \pm2, \pm3\}$, the distortion in corresponding position is $wet \cos t = 10^{13}$.

Finally, according to the original cover modification amplitude after embedding 0 and 1 in each new cover pixels, calculate the distortion using the linear combination of $\mathbf{Dif}^{w}(\mathbf{X}, \mathbf{Y}_w)$ and the distortion obtained by S-UNIWARD.

$$\mathbf{D}_w = \sum_{i=x}^{M} \sum_{j=y}^{N} \mathbf{D}_{\mathbf{Dif}^{w}(\mathbf{X}, \mathbf{Y}_w)}(i, j)$$
$$i = \{x, x+1, \ldots, M\}, \quad j = \{y, y+1, \ldots, N\} \tag{12}$$

where $\mathbf{D}_{\mathbf{Dif}^{w}(\mathbf{X}, \mathbf{Y}_w)}$ is the corresponding distortion in formula (10) according to the value of $\mathbf{Dif}^{w}(\mathbf{X}, \mathbf{Y}_w)$. $i = \{x, x+1, \ldots, M\}, j = \{y, y+1, \ldots, N\}$ is the affected position in original cover after embedding $w \in \{0, 1\}$ in new cover pixels. $\mathbf{D}_w$ is the final distortion we need.

After getting the distortion for each new cover pixels, we can embed secret messages in the new cover pixels using STCs code by formula (13) and (14).

$$\mathbf{y} = \mathrm{Emb}(\mathbf{x}, \mathbf{m}) = \arg \min_{\mathbf{y} \in C(\mathbf{m})} \mathrm{D}(\mathbf{x}, \mathbf{y}) \tag{13}$$

$$\mathbf{m} = \mathrm{Ext}(\mathbf{y}) = \mathbf{H}\mathbf{y} \tag{14}$$

where $\mathbf{x} = \{0, 1\}^n$ is the new cover sequences and $\mathbf{y} = \{0, 1\}^n$ is the new stego sequences. $\mathbf{H} \in \{0, 1\}^{m \times n}$ is a parity-check matrix and $C(\mathbf{m})$ is the coset corresponding to syndrome m, $\mathrm{D}(\mathbf{x}, \mathbf{y})$ is the distortion function calculated by formula (10).

IV. EXPERIMENTAL RESULTS AND ANALYSIS

In this section, the experimental parameter settings of the proposed algorithm are given, the anti-scaling performance and anti-detection performance of the proposed algorithm are verified experimentally, and the experimental results are given.

A. EXPERIMENTAL PARAMETER SETTINGS

In order to verify the resistance of the proposed algorithm to scaling attack and statistic detection, the steganography algorithm based on quantization index modulation [21], the proposed algorithm in this paper and S-UNIWARD adaptive steganography algorithm [10] are used to realize the embedding and extracting of messages. The SPAM features [8] and maxSRM [23] features are extracted respectively in the cover image and the stego image to test performance against statistic detection. 2000 images in BossBase-1.01 library are randomly selected as cover images, and the size is 512×512. The message to be embedded is 0 and 1 sequence generated randomly.

The relevant parameters of this algorithm are set as Table 1: The length of the new cover is 183, so the length of the embedded message is fixed to 128 bit. The scaling factor is from 0.25 to 2 with interval 0.25. The nearest neighbor interpolation, the bilinear interpolation and the bicubic interpolation method are used to the stego image. The embedding distortion in this position which is unsuitable to change in the cover image is constant $wet \cos t = 10^{13}$. Quantization step $\Delta = 30000$, and quantizer $d = [0, 15000]$. The order of the Zernike moment is equal to 30.

TABLE 1. Experimental parameter settings.

Cover	Embedding Process			
	Scaling factor	Interpolation Method	payload	parameter
BossBase-1.01 512×512 2000	0.25 0.5 0.75 1 1.25 1.5 1.75 2	The nearest neighbor interpolation, The bilinear interpolation, The bicubic interpolation	128bit	wetcost=10^{13} △=30000 d=[0,15000] $N_{Zernike}$=30

B. SCALING ATTACK RESISTANT EXPERIMENT

This section verifies the robustness of the proposed algorithm for three interpolation scaling attacks and the scaling performance compared with the classic S-UNIWARD steganography algorithm and the steganography algorithm based on quantization index modulation. By scaling attacks on the generated 2000 stego images, the extraction error rate and the correct extraction rate of the secret messages in the stego images after the attack are calculated. The extraction error rate is shown as $R_{error} = \frac{n_{error}}{n}$, where n_{error} is the number of message bits extracted mistakenly, and n is the total number of embedded message. The correct extraction rate of the secret messages is $R_{right} = \frac{N_{right}}{N}$, where N_{right} is the number of the stego images that can be extract the secret message completely and correctly, and N is the total number of the stego images.

1) ANTI-SCALING PERFORMANCE TEST EXPERIMENT

The nearest neighbor interpolation method, the bilinear interpolation method and the bicubic interpolation method are applied to the stego images generated by this proposed algorithm. The scaling factor is 0.25 to 2 in sequence, interval 0.25. Then the scaled stego images are rescaled by the same interpolation method and the reciprocal of scaling factor to be stored in original size to finish the extraction of message. The average extraction error rate and the correct extraction rate are obtained, as shown in Figure 4 (a) and (b) respectively.

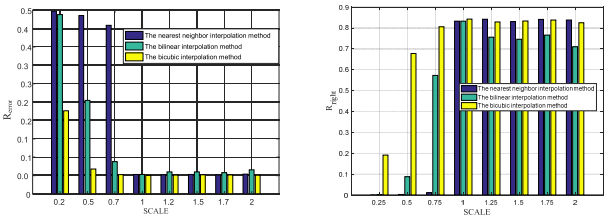

FIGURE 4. The scaling attack resistant test of the proposed algorithm under different scaling factors. (a) The extraction error rate. (b) The correct extraction rate.

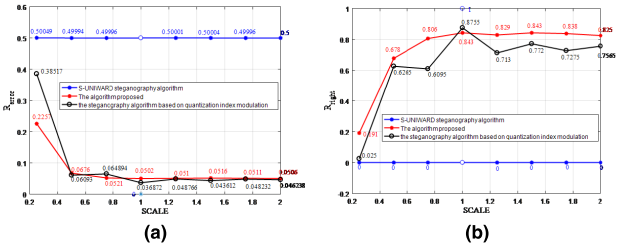

FIGURE 5. The scaling attack resistant comparison under different steganography algorithm. (a) The extraction error rate. (b) The correct extraction rate.

From Figure 4, we can see that when the scaling factor is less than 1, the average extraction error rate of the secret message of the proposed algorithm decreases gradually with the increase of the scaling factor, and the correct extraction rate becomes larger and larger. The robustness of the algorithm to the bicubic interpolation scaling attack is strongest. For example, when the scaling factor is 0.5, the extraction error rate of message extraction is 0.0676, and the correct extraction rate is 0.6780. When the scaling factor is greater than 1, the average extraction error rate and the correct extraction rate of the proposed algorithm tend to be stable. In this case, the algorithm has the best robustness to the nearest neighbor interpolation and bicubic interpolation scaling attacks. When the scaling factor is 1.25, the average extraction error rate of the message in the stego images after applying the nearest neighbor interpolation attack is 0.0516, and the correct extraction rate is 0.8420. Experimental results show that under certain conditions, the proposed algorithm is robust to three kinds of interpolation scaling attacks. In practical applications, the cover image can be selected according to the need to ensure that the secret message can be extracted correctly after scaling attacks.

2) ANTI-SCALING COMPARISON EXPERIMENT

Using the S-UNIWARD adaptive steganography algorithm, the algorithm in this paper and the steganography algorithm based on quantization index modulation embeds the secret messages in 2000 cover images, and then extract the secret messages after the bicubic interpolation attacks. Figure 5 are the extraction error rate and the correct extraction rate of the secret messages under the attack of different scaling factors.

Figure 5 (a) shows that when the scaling factor of S-UNIWARD steganography algorithm is not 1, the message extraction error rate is about 50%. After the scaling factor is higher than 0.5, the message extraction error rate of the proposed algorithm and the steganography algorithm based on quantization index modulation is obviously decreased to about 5%. When the scaling factor is 0.25, the message extraction error rate of the proposed algorithm is 22.57%, and the extraction error rate of the steganography algorithm based on quantization index modulation is 38.52%, which shows that the algorithm has better scaling performance even in the case of low scaling factor.

Figure 5 (b) shows that the message extracted in the stego image generated by S-UNIWARD algorithm can't be fully and correctly extracted as long as it is subject to scaling attack. The message correct extraction rate of stego images generated by the algorithm proposed is higher than the algorithm based on quantization index modulation. This is because the scaling attack resistance of the algorithm based on the Zernike scaling invariant moment is higher than the quantization index modulation based message embedding and extraction algorithm.

C. STATISTICAL DETECTION RESISTANT EXPERIMENT

Extract the classical SPAM [8] features and maxSRM [23] features of cover images and stego images generated by the proposed algorithm and the steganography algorithm based on the quantization index modulation. Then the cover features and the stego features are input into the integrated classifier for discrimination. The detection error rate is shown in Figure 6.

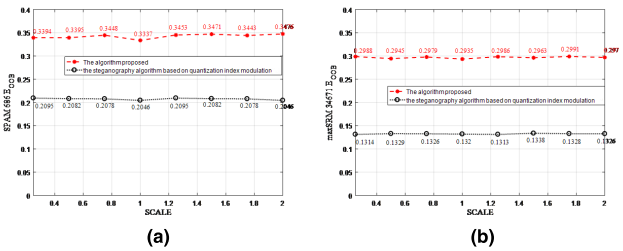

FIGURE 6. The detection resistant comparison under different steganography algorithm. (a) The detection error rate of SPAM. (b) The detection error rate of maxSRM.

The detection resistance of the proposed algorithm based on Zernike moment is significantly higher than that algorithm based on quantization index modulation. In the SPAM feature detection, the detection error rate of the proposed algorithm is about 34%, while the detection error rate in [21] is about 20.8%. Under the maxSRM feature detection, the detection error rate of the algorithm in this paper is close to 30%, which is obviously higher than the algorithm in [21]. Because the algorithm based on quantization index modulation in [21] is equivalent to embedding message in the whole image, and the modified amplitude of the image is larger. But the algorithm proposed only embeds the message in

the image scaling invariants, and improves the anti-detection performance in some extent.

V. CONCLUSIONS AND FUTURE WORK

Because of the poor scaling attack resistance of the existing adaptive steganography algorithm and the low detection resistance of the algorithm based on quantization index modulation, we propose a new adaptive steganography algorithm based on Zernike moment. This algorithm generates the new cover and embedding algorithm using the normalized Zernike moment and dither modulation algorithm, calculates distortion of the new cover by modified S-UNIWARD, and uses STCs encoding to embed the secret messages to ensure anti-scaling attack performance and anti-detection performance. The experimental results show that the message average extraction error rate is reduced significantly compared with the S-UNIWARD algorithm after scaling attack, and the anti-detection performance is higher than the steganography algorithm based on quantization index modulation. But in practical applications, the algorithm proposed has a problem of low embedding rate.

REFERENCES

[1] T. Filler, J. Judas, J. Fridrich, "Minimizing embedding impact in steganography using trellis-coded quantization," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 1, pp. 920–935, 2011.

[2] Z. Pan, J. Lei, Y. Zhang, and F. L. Wang, "Adaptive fractional-pixel motion estimation skipped algorithm for efficient HEVC motion estimation," *ACM Trans. Multimedia Comput., Commun. Appl.*, vol. 14, no. 1, pp. 12–19, 2018.

[3] Z. Pan, X. Yi, and L. Chen, "Motion and disparity vectors early determination for texture video in 3D-HEVC," *Multimedia Tools Appl.*, pp. 1–18, Nov. 2018. doi: 10.1007/s11042-018-6830-7.

[4] J. Wang, T. Li, X. Luo, Y. Shi, and S. K. Jha, "Identifying computer generated images based on quaternion central moments in color quaternion wavelet domain," *IEEE Trans. Circuits Syst. Video Technol.*, 2018. doi: 10.1109/ TCSVT.2018.2867786.

[5] Y. Ma, X. Luo, X. Li, Z. Bao, and Y. Zhang, "Selection of rich model steganalysis features based on decision rough set α-positive region reduction," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 29, no. 2, pp. 336–350, Feb. 2019. doi: 10.1109/TCSVT.2018.2799243.

[6] T. Pevný, T. Filler, and P. Bas, "Using high-dimensional image models to perform highly undetectable steganography," in *Proc. 12th Int. Workshop Inf. Hiding*, 2010, pp. 161–177.

[7] X. Luo *et al.*, "Steganalysis of HUGO steganography based on parameter recognition of syndrome-trellis-codes," *Multimedia Tools Appl.*, vol. 75, no. 21, pp. 13557–13583, 2016.

[8] T. Pevný, P. Bas, and J. Fridrich, "Steganalysis by subtractive pixel adjacency matrix," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 2, pp. 215–224, Jun. 2010.

[9] V. Holub and J. Fridrich, "Designing steganographic distortion using directional filters," in *Proc. IEEE Workshop Inf. Forensics Secur.*, Dec. 2012, pp. 234–239.

[10] V. Holub and J. Fridrich, "Digital image steganography using universal distortion," in *Proc. ACM Workshop Inf. Hiding Multimedia Secur.*, 2013, pp. 59–68.

[11] V. Holub, J. Fridrich, and T. Denemark, "Universal distortion function for steganography in an arbitrary domain," *EURASIP J. Inf. Secur.*, vol. 2014, no. 1, p. 1, 2014.

[12] Y. Zhang, X. Luo, J. Wang, C. Yang, and F. Liu, "A robust image steganography method resistant to scaling and detection," *J. Internet Technol.*, vol. 19, no. 2, pp. 607–618, 2018.

[13] B.-S. Kim, J.-G. Choi, and K.-H. Park, "RST-resistant image watermarking using invariant centroid and reordered Fourier-Mellin transform," in *Proc. Int. Workshop Digit. Watermarking*, 2003, pp. 370–381.

[14] Z. Lin, L. Niu, and X. Jiang, "A method on digital watermarking image against geometric distortion," in *Proc. Int. Congr. Image Signal Process.*, Oct. 2015, pp. 130–134.

[15] M. Zareian and H. R. Tohidypour, "A novel gain invariant quantization-based watermarking approach," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 11, pp. 1804–1813, Nov. 2014.

[16] H. S. Kim and H.-K. Lee, "Invariant image watermark using Zernike moments," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 766–775, Aug. 2003.

[17] Y. Xin, S. Liao, and M. Pawlak, "A multibit geometrically robust image watermark based on Zernike moments," in *Proc. 17th Int. Conf. Pattern Recognit.*, Aug. 2004, pp. 861–864.

[18] Y. Zhang, X. Luo, C. Yang, D. Ye, and F. Liu, "A JPEG-compression resistant adaptive steganography based on relative relationship between DCT coefficients," in *Proc. Int. Conf. Availability Rel. Secur.*, Aug. 2015, pp. 461–466.

[19] Y. Zhang, X. Luo, C. Yang, and F. Liu, "Joint JPEG compression and detection resistant performance enhancement for adaptive steganography using feature regions selection," *Multimedia Tools Appl.*, vol. 76, no. 3, pp. 3649–3668, 2017.

[20] Y. Zhang, C. Qin, W. Zhang, F. Liu, and X. Luo, "On the fault-tolerant performance for a class of robust image steganography," *Signal Process.*, vol. 146, pp. 99–111, May 2018.

[21] Y. Zhang, D. Ye, J. Gan, Z. Li, and Q. Cheng, "An image steganography algorithm based on quantization index modulation resisting scaling attacks and statistical detection," *Comput. Mater. Continua*, vol. 56, no. 1, pp. 151–167, 2018.

[22] A. Khotanzad and Y. H. Hong, "Invariant image recognition by Zernike moments," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 12, no. 5, pp. 489–497, May 1990.

[23] T. Denemark, V. Sedighi, V. Holub, R. Cogranne, and J. Fridrich, "Selection-channel-aware rich model for steganalysis of digital images," in *Proc. IEEE Int. Workshop Inf. Forensics Secur.*, Dec. 2014, pp. 48–53.

YUE ZHANG received the M.S. degree from the Zhengzhou Science and Technology Institute, in 2018.

She has been with the State Key Laboratory of Mathematical Engineering and Advanced Computing, since 2015. Her research interest includes multimedia Steganography/Steganalysis. She has obtained the support of the National Natural Science Foundation of China and the Basic and Frontier Technology Research Program of Henan Province.

XIANGYANG LUO received the B.S., M.S., and Ph.D. degrees from the State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou, China, in 2001, 2004, and 2010, respectively.

He has been with the State Key Laboratory of Mathematical Engineering and Advanced Computing, since 2004. From 2006 to 2007, he was a Visiting Scholar with the Department of Computer Science and Technology, Tsinghua University. Since 2011, he held a Postdoctoral position with the Institute of China Electronic System Equipment Engineering Co., Ltd. He has authored or co-authored over 100 refereed international journal and conference papers. His research interests include multimedia steganography/steganalysis, and network and information security. He has obtained the support of the National Natural Science Foundation of China, the National Key R&D Program of China, and the Basic and Frontier Technology Research Program of Henan Province.

YANQING GUO received the B.S. and Ph.D. degrees in electronic engineering from the Dalian University of Technology, China, in 2002 and 2009, respectively.

He is currently a Professor with the Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology. His research interests include multimedia security and forensics, digital image processing, and machine learning.

CHUAN QIN received the B.S. degree in electronic engineering, and the M.S. degree in signal and information processing from the Hefei University of Technology, Anhui, China, in 2002 and 2005, respectively; and the Ph.D. degree in signal and information processing from Shanghai University, Shanghai, China, in 2008.

Since 2008, he has been with the faculty of the School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, where he is currently a Professor. From 2010 to 2012, he was with Feng Chia University, Taiwan, as a Postdoctoral Researcher. His research interests include image processing and multimedia security. He has published over 110 papers in these research areas.

FENLIN LIU received the B.S. degree from the Zhengzhou Science and Technology Institute, in 1986, the M.S. degree from the Harbin Institute of Technology, in 1992, and the Ph.D. degree from the Northeast University, in 1998.

He is currently a Professor with the Zhengzhou Science and Technology Institute. His research interests include network topology and network geolocation. He has authored or co-authored more than 90 refereed international journal and conference papers. He has obtained the support of the National Natural Science Foundation of China, and the Found of Innovation Scientists and Technicians Outstanding Talents of Henan Province of China.