Journal of Network Intelligence
Taiwan Ubiquitous Information

©2020 ISSN 2414-8105 (Online)
Volume **5**, Number **2**, May **2020**

A Robust Digital Image Watermarking Scheme for Content Protection

Xu-Shi Mei and Huan-Tong Chen

School of Information Engineering
Jinhua Polytechnic
Jinhua 321000, P. R. China
meixushi@163.com

Hang-Yu Fan and Zhe-Ming Lu*

School of Aeronautics and Astronautics
Zhejiang University
Hangzhou 310027, P.R. China
*Correponding Author: zheminglu@zju.edu.cn

Jyh-haw Yeh

Department of Computer Science
Boise State University
Idaho, USA
jhyeh@boisestate.edu

Received April 2019;Revised January 2020;
(Communicated by Zhe-Ming Lu)

Abstract. *In this paper, a blind image watermarking scheme is proposed for resist the attacks such as collages, cutouts, etc. Traditional image watermarking technology cannot resist such attacks, because the synchronization information is broken. We use the noise template as the watermark, and the watermark can be detected with a high accuracy from part of the watermarked image. We also propose an improved weight template, which can enhance the imperceptibility of the watermark. In the watermark detection process, the autocorrelation of the high frequency component is necessary. Because of the existence of the attack, the first autocorrelation contains much disturbing peak points. In order to enhance the feature and suppress the interference, we propose the second autocorrelation on the result of the first autocorrelation. Next, a simple and effective method is proposed for detection and decision. In addition, some tricks are proposed to get a higher detection accuracy. Experimental results demonstrate that our scheme outperforms traditional schemes in resisting collage, cutout and image synthesis, and our scheme has a high accuracy, and the proposed watermarking scheme has a strong robustness to common image processing operations.*

Keywords: Image watermarking, Noise template, Robust watermarking, Copyright Protection.

1. **Introduction.** With the development of the Internet, the application of multimedia has become extremely extensive. As an important kind of multimedia, digital images are ubiquitous, but attacks against images such as collages and cutouts are becoming more and more common. Digital image watermarking [1-8] has been widely used for copyright protection. In 2015, Zong et al.[1] proposed a robust histogram shape-based method for image watermarking. In 2016, Wang et al.[2] proposed a geometrically invariant image

watermarking method based on fast radial harmonic Fourier moments. In 2017, Liu et al. [3] presented a digital image watermarking method based on DCT and fractal encoding. In 2018, Liu et al.[4] propose an optimal blind watermarking method for color images based on the U matrix of quaternion singular value decomposition, Xu et al. [5] presented a color image watermarking method based on the tensor domain, which takes efficient account of the overall characteristics of color images and spreads the watermark information into three channels of color images based on tensor decomposition. In 2019, Sadreazami and Amini [6] proposed a robust image watermarking scheme using local statistical distribution in the contourlet domain, Wang and Du [7] proposed a method of processing color image watermarking based on the Haar wavelet. In 2020, Fan et al. proposed a low-frequency construction watermarking scheme based on histogram[8].

In e-commerce websites, the authorized product images are often illegally copied and used by some merchants who sell fakes, and they know the images on websites have been watermarked. In order to wreck the watermarks in these illegally copied images, these merchants usually make some changes, such as collages and cutouts, on the images as shown in Fig. 1. These attacks are simple and common and are highly destructive to traditional image watermarking schemes. Traditional digital image watermarking schemes [1-8] often require the watermarked image should be complete during watermark detection, even if they are robust to rotation, scaling and translation operations[2] or other attacks such as cropping and random bending[1], which cannot effectively deal with the attacks mentioned above. These attacks can destroy not only the synchronization information but also the statistical characteristics of the image. Therefore, we need to design a new watermarking scheme which can resist these attacks for image content protection.

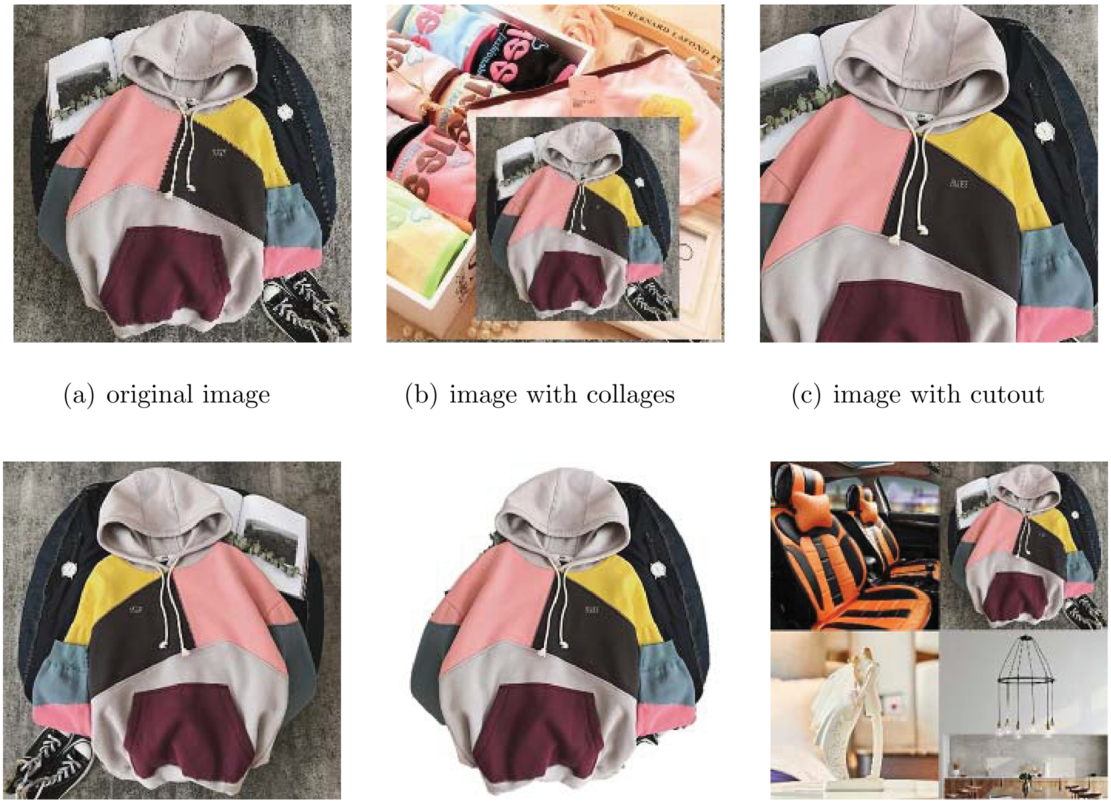
Review the problem, we want a robust watermarking scheme, and the watermark can be detected in the attacked images for recognizing the authority. So, we think that it is necessary to detect the watermark, but the capacity of the watermark scheme is not important. For a watermarking scheme, the robustness, imperceptibility and capacity cannot be excellent at the same time. Thus we decide to design a watermarking scheme which has high robustness, high imperceptibility and the minimal capacity. The watermark information is 1, which represents the image is watermarked. The custom watermark information can be embedded by other algorithm in the joint scheme. Therefore, unlike the traditional ways, we focus on the watermark detection process in the proposed watermarking scheme. Based on consulting literature material, we find the watermarking scheme based on noise template [4]. This scheme is usually used to estimate the rotation and scaling of the image [5,6]. Although these schemes cannot directly solve our problem, it gives us a lot of inspirations. Based on this, we propose a blind watermarking scheme. If the content of the image exists, the watermark should be detected.

Our scheme contains two parts, i.e., embedding and detection. The flow charts are given in Fig. 2. In the embedding process, we propose an improved weight template, which can enhance the imperceptibility of the watermark. In the detection process, we creatively use double autocorrelation, which can reinforce the features effectively. We have also proposed the method of classification, making the detection process simple with high accuracy.

2. **Watermark Embedding and Detection.**

2.1. **Watermark Embedding.**

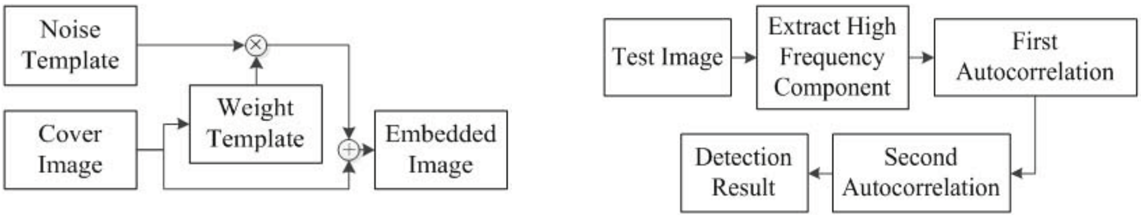
Weight template, which is also called adaptive gain, is generally required in the method which uses noise templates. The features at different area in the cover image are different. Some areas are smoother and some areas are brighter. If the noise template is added on the cover image directly, the imperceptibility will be



(a) original image (b) image with collages (c) image with cutout

(d) image flip (e) remove the background (f) multiple image synthesis

FIGURE 1. The original image and the attacked images.



(a) The embedding process (b) The detection process

FIGURE 2. The flow charts of the proposed scheme.

seriously affected. Thus, we use weight template to enhance the imperceptibility of the watermark. The improved weight template is shown in Eqs. (1-4).

$$\texttt{weight}(x,y) = [w_1 M_1(x,y) + w_2 M_2(x,y)] HCM(x,y) \tag{1}$$

$$M_1(x,y) = \frac{1}{8}\sum_{r=0}^{8} \texttt{abs}(p(x,y) - p(r)) \tag{2}$$

$$M_2(x,y) = \texttt{abs}(p(x,y) - \frac{255}{2}) \tag{3}$$

$$HCM(x,y) = \begin{cases} 1 & M_1(x,y) \geq MaskThresh \\ 0 & M_1(x,y) < MaskThresh \end{cases} \tag{4}$$

Where M_1 denotes the local gradient, M_2 denotes the absolute brightness, w_1 and w_2 denote the weights of M_1 and M_2, HCM denotes the high contrast mask. In Eq. (2), $p(x, y)$ denotes the pixel value in the image, and $p(r)$ means one adjacent pixel of $p(x, y)$. $MaskThresh$ is a threshold, which can be usually set between 0 and 5.

The noise template is constructed by repeating a small-sized basic noise template in a non-overlapping fashion, as shown in the Fig. 3. The small-sized basic noise template is typically square. Before the embedding, if the cover image contains a few noise components, denoising can be performed by using a low-pass filter to improve the embedding effect. The embedding of the watermark can be shown in Eq. 5, where nt denotes noise template.

$$p_w(x, y) = p(x, y) + \texttt{weight}(x, y)nt(x, y) \tag{5}$$

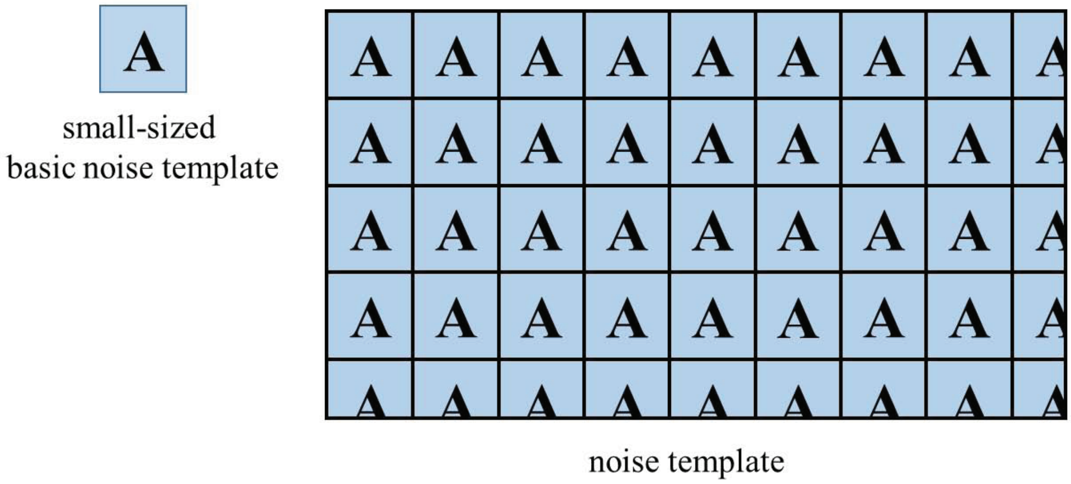
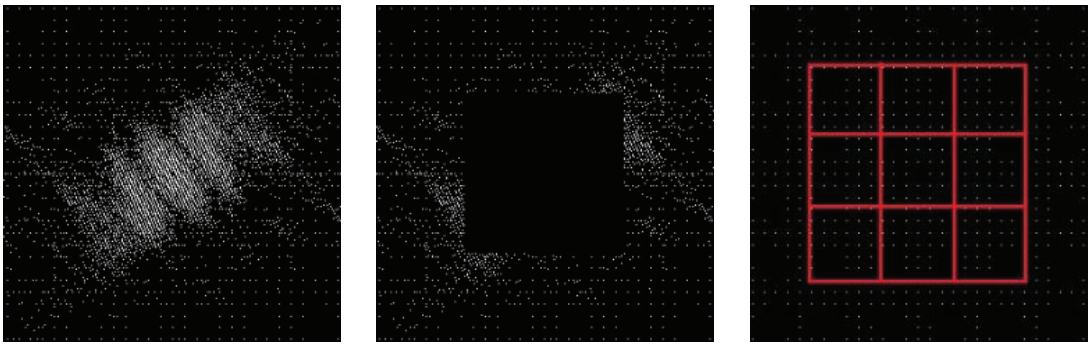


Figure 3. The display of the small-sized basic noise template and the noise template.

2.2. **Watermark Detection.** The watermark detection process is essentially the process of feature extraction and classification. We hope to be able to detect the watermark from the image which contains part of the watermarked image. First, the test image need to be filtered by Wiener high-pass filter, and the high-frequency component can be named as H_0. Then, an autocorrelation is performed on H_0 to obtain an autocorrelation result AC_1. The way of calculating the autocorrelation of I can be seen in Eq. (6), where X and Y are the sizes of I.

$$AC(m, n) = \sum_{x=0}^{X-1} \sum_{y=0}^{Y-1} I(m, n)I(m + x, n + x) \tag{6}$$

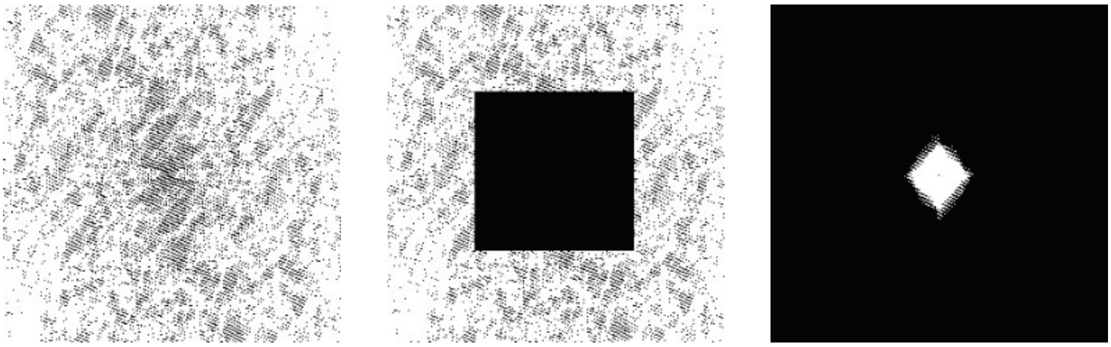
Then normalize the AC_1 and convert it to the binary one as AC_1_BIN. Due to the existence of the attack, there may be some disturbing peak points in the AC_1_BIN, as shown in Fig. 4(a). Through analysis, we find that if the test image does contain the watermark, the peak points in AC_1_BIN present a significant periodicity, and if the test image does not contain the watermark, the peak points in AC_1_BIN have no significant regularity, as shown in Fig. 5(a). Due to the existence of disturbing peak points, the classification directly on AC_1_BIN has a high error rate. In order to enhance the feature of periodicity and suppress the interference, once more autocorrelation is performed on AC_1_BIN to obtain AC_2. Then AC_2_BIN is obtained by normalizing and binarizing AC_2, as shown in Fig. 4(c). It can be found that if the test image contains the watermark, the periodic feature of the peak points is obviously enhanced, and the peak of the interference is effectively suppressed; if the test image does not contain the watermark, there is no such periodic feature, as shown in Fig. 5(c). The second autocorrelation brings great convenience to classification. Next, we set a square central detection area in AC_2_BIN, as shown in Fig. 4(c). The size of the detection area is set by us. Generally, it can be selected as 1/3 of the size of AC_2_BIN. Then, the central detection area is equally divided into $N \times N$ sub-areas, and generally N can be 3 or 4, as shown in Fig. 4(c). If every sub-area contains peak point, the next operation can be performed; otherwise, it can be considered that the test image does not contain the watermark. Next, the peak points density need to be calculated in the central detection area, which is the ratio of the number of peak points to the number of all elements in the central detection area. If the ratio in the range $[PDT\_LOW, PDT\_HIGH]$, a conclusion can be given that the test image contains the watermark, otherwise, the test image does not contain watermark. The values of PDT_LOW and PDT_HIGH can be specified according to the size of the small-sized basic noise template. Furthermore, if you want to obtain the scaling factor and rotation angle of the template, you can calculate the distance between the peak points in AC_2_BIN and the angle of the peak points connection.



(a) AC_1_BIN (b) Center masked AC_1_BIN (c) AC_2_BIN

FIGURE 4. The autocorrelation analysis about one attacked image which contains the watermark. Many interferences can be seen in the AC_1_BIN, and the square central detection area (red square area) can be seen in the AC_2_BIN.

3. **Some Tricks.** According to the above process, you can get good results, but if you want to improve the detection accuracy, we will give some tips and suggestions in this section. First, for the result of autocorrelation, such as AC_1 and AC_2, it is better to modify the element at the centre of the result to the mean of the result before normalizing and binarizing. This is because the element at the centre is extremely large, which can affect the result of normalization and binarization. In addition, there may be many annoying useless peaks at the centre of AC_1_BIN, as shown in Fig. 4(a). In order to enhance the periodic feature, we recommend performing a peak density test on the central area of AC_1_BIN before the second autocorrelation. If the peak density in the central area of AC_1_BIN is large, the element values of the central area of $AC1\_BIN$ can be set to zero, and then the second autocorrelation operation is performed, as shown in Fig. 4(b) and Fig. 5(b). After this, the interference peaks in the result of the second autocorrelation are effectively suppressed.



(a) AC_1_BIN (b) Center masked AC_1_BIN (c) AC_2_BIN

FIGURE 5. The autocorrelation analysis about one image which does not contain the watermark.There is no significant regularity in the AC_1_BIN.

4. Experiment and Discussion.

4.1. **Invisibility and Robustness to Common Image Processing.** In this experiment, we mainly discuss the robustness of our scheme under JPEG compression(QF=90 and 70), cropping(25%), rotation(0.5°), scaling(1.2 and 0.8), Gaussian noise(1%), and median blur(3×3). The PSNR displaying the imperceptibility of our scheme are given, and the detection judgement results (Yes or No) are given to evaluate the robustness. In this experiment, 10 standard test images with the size of 512×512 are chosen as the carrier images, as shown in Fig. 6. The PSNR values are shown in Table 1, and the detection results are shown in Table 2. From these results, we can see that our scheme has good invisibility and robustness to common attacks.

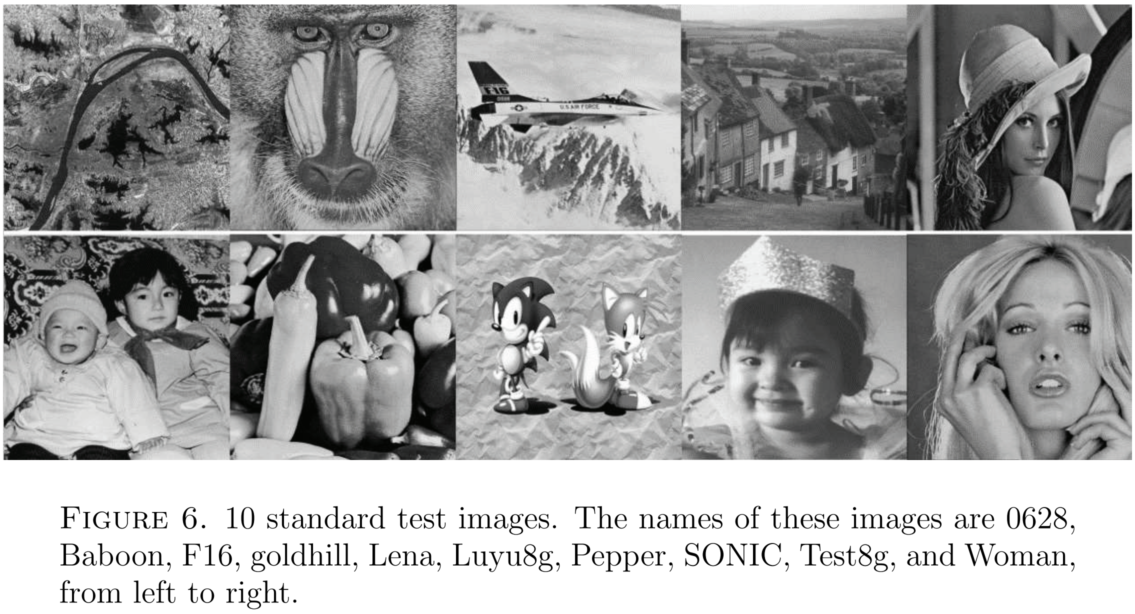


FIGURE 6. 10 standard test images. The names of these images are 0628, Baboon, F16, goldhill, Lena, Luyu8g, Pepper, SONIC, Test8g, and Woman, from left to right.

4.2. **Robustness to Special Attacks Including Collage and Cutout.** Because our scheme is designed for resisting attacks such as collage, cutout, cropping, etc. We simulate the attacks and then detect the watermark in the attacked images. We generate 1000 images with attack of collage. In each of them, the watermarked image stack on one

Table 1. PSNR values of ten images.

Image	1	2	3	4	5
PSNR	38.714	37.984	35.953	35.587	34.971
Image	6	7	8	9	10
PSNR	36.548	35.108	35.743	36.296	35.511

Table 2. Watermark detection results of ten images under different attacks.

Image	1	2	3	4	5	6	7	8	9	10
JPEG90	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
JPEG70	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Cropping25%	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Rotation0.5^o	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Scaling 1.2	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Scaling 0.8	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Guassian 1%	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Median3×3	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

background image, one example is shown in Fig.1(b). Also, we generate 1000 images which are cutouts of the watermarked images, one example is shown in Fig.1(c). Also, we generate 1000 images which are flipped watermarked images, one example is shown in Fig.1(d). And also, we generate 1000 synthetic images, one example is shown in Fig.1(f). Here,1000 images with watermark and 1000 images without watermark are also used for watermark detection test. The experimental results are shown in Table 3. From the results, we can find that our scheme has a strong robustness. Some images have periodicity, and these images can be detected as watermarked. And this problem can be solved by using joint watermarking schemes.

Table 3. The experiments results on robustness to special attacks.

Type	Number of images	Detected watermarks	Accuracy
Watermarked	1000	1000	100%
Without watermark	1000	54	94.6%
Collage	1000	1000	100%
Cutout	1000	1000	100%
Flip	1000	1000	100%
Multiple image synthesis	1000	1000	100%

4.3. **Algorithm Comparisons Under Collage and Cutout Attacks.** In order to demonstrate the superiority of our scheme, in this experiment, we compare our scheme with resent eight watermarking schemes[1-8] in terms of resisting to collage and cutout attacks, the comparison results are shown in Table 4. Here, we use above 1000 images with attack of collage and above 1000 images which are cutouts of the corresponding watermarked images. From these results, we can see that our scheme is superior to all other schemes under collage and cutout attacks.

5. **Conclusions and Future Work.** We propose a blind watermarking scheme for content protection. By embedding the watermark into the image, the watermark can be easily detected if part of the watermarked image still exists. Our scheme has a very high

Table 4. Comparison of robustness to collage and cutout attacks among nine algorithms.

Scheme	Accuracy under collage	Accuracy under cutout
2015[1]	0%	0%
2016[2]	0%	0%
2017[3]	0%	0%
2018[4]	0%	0%
2018[5]	0%	0%
2019[6]	0%	0%
2019[7]	0%	0%
2020[8]	0%	0%
our	100%	100%

robustness, and can resist attacks such as collage, cutout, etc. In addition, due to the improved weight template, the imperceptibility of the watermark is greatly improved. In some application scenarios, the only need is to detect the presence or absence of the watermark in the image, so the proposed embedding and detection schemes in this paper are completely applicable. This shceme can be combined with other watermarking scheme, thus this noise template watermarking can get the scale rate and rotation angle for image synchronization. In the future, combining with another suitable watermarking algorithm which contain the editable watermark information will be very useful.

REFERENCES

[1] T. Zong, Y. Xiang, I. Natgunanathan, S. Guo, W. Zhou and G. Beliakov, Robust histogram shape-based method for image watermarking, *IEEE Transactions on Circuits Systems for Video Technology*, vol.25, no.5, pp. 717–729, 2015.

[2] C.-P. Wang, X.-Y. Wang, Z.-Q. Xia, Geometrically invariant image watermarking based on fast radial harmonic Fourier moments, *Signal Processing: Image Communication*, vol. 45, pp.10–23, July 2016.

[3] S. Liu, Z. Pan, H. Song, Digital image watermarking method based on DCT and fractal encoding, *IET image Processing*, vol.11, no.10, pp. 815–821 2017.

[4] F. Liu, L.-H. Ma, C. Liu, M. Xu, Z.-M. Lu, Optimal blind watermarking for color images based on the U matrix of quaternion singular value decomposition, *Multimedia Tools and Applications*, vol. 77, no.18, pp.23483–23500, 2018.

[5] H. Y. Xu, G. Y. Jiang, M. Yu, T. Luo, A color image watermarking based on tensor analysis, *IEEE Access*, vol.6, pp. 51500–51514, 2018.

[6] H. Sadreazami, M. Amini,A robust image watermarking scheme using local statistical distribution in the contourlet domain, *IEEE Transactions on Circuits and Systems II: Express Briefs*,vol. 66, no.1, pp.151–155, 2019.

[7] J. Wang, Z. Du, A method of processing color image watermarking based on the Haar wavelet, *Journal of Visual Communication and Image Representation*, vol. 64, Article 102627, October 2019.

[8] H.-Y. Fan, Z.-M. Lu, Y.-L. Liu, A low-frequency construction watermarking based on histogram, *Multimedia Tools and Applications*, vol. 79, no.9-10, pp.5693–5717, 2020.

[9] A. M. Alattar, J. Meyer, Watermark re-synchronization using log-polar mapping of image autocorrelation, *Proceedings of the 2003 International Symposium on Circuits and Systems*, vol.2, 2003.

[10] C.-H. Lai, J.-L. Wu, Robust image watermarking against local geometric attacks using multiscale block matching method, *Journal of Visual Communication Image Representation*, vol.20, no.6, pp. 377–388, 2009.

[11] X. Xu, R. Zhang, X. Niu, Image synchronization using watermark as RST invariant descriptors, *IEEE International Conference on Information Theory and Information Security*, pp. 831–836, 2010.