Geometric correction code-based robust image watermarking

Zhili Zhou | Jianyu Zhu | Yuecheng Su | Meimin Wang | Xingming Sun

Jiangsu Engineering Center of Network Monitoring & School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing, China (Email: Zhu_jy_1996@163.com; syc1997@126.com; 15850720606@163.com; sunnudt@163.com)

Abstract
Digital image watermarking is one of the effective schemes to protect the copyrights of still images. However, the existing watermarking schemes are still not robust enough to the common geometric transformation attacks such as arbitrary rotation, scaling and shifting with desirable hiding capacity. To address this issue, we propose a robust watermarking scheme based on geometric correction codes (GCCs). In this scheme, the watermark and pre-set GCCs are combined and embedded into a cover image to obtain the watermarked image. At the stage of watermark extraction, the watermarked image, under a variety of geometric transformation attacks, can be geometrically corrected by minimising the difference between the extracted and the original GCCs, then the watermark is extracted from the watermarked image. The experiments demonstrate that, compared to the typical watermarking schemes, the proposed scheme achieves much higher robustness to the common geometric transformation attacks and comparable invisibility with the same embedding capacity.

1 | INTRODUCTION
Digital watermarking is popularly adopted to protect the copyright of multimedia content by invisibly embedding watermarks into digital media. However, in practice, the images may suffer a variety of intentional or unintentional geometric transformation and image manipulation attacks such as rotation, scaling and noise-like attacks [1–3], which will affect the correct extraction of watermarks from the watermarked images for the copyright protection. Thus, an ideal watermarking scheme should be robust to most of the common attacks with desirable hiding capacity.

According to the manners of watermark embedding, the existing watermarking schemes can be roughly categorised into two classes: Image-level and region-level watermarking schemes. Image-level watermarking schemes embed watermarks into whole image region, while region-level watermarking schemes embed watermarks into a set of local regions.

In early works, image-level watermarking schemes are proposed based on frequency domains such as discrete cosine transform (DCT) [4], discrete wavelet transform [5], discrete Fourier transform [6] and singular value decomposition [7]. These schemes generally show high robustness to noise-like attacks such as JPEG compression, Gaussian noise adding and blurring. Subsequently, some improved watermarking schemes based on frequency domains [8–11] have been proposed to further enhance the robustness to those noise-like attacks. Recently, some researchers applied neural networks in image-level watermarking [12–15]. Mei et al. [16] designed a neural network to model the human visual system to decide the watermark strength for DCT coefficients. Kandi et al. [17] trained an autoencoder convolutional neural network (CNN) and applied it in image watermarking tasks. However, it is a non-blind watermarking scheme, making it less appealing in practice. Zhong and Shih [18] viewed image watermarking as an image fusion task and adopted CNN to fuse watermark with a cover image.
However, those image-level watermarking schemes are generally vulnerable to the common geometric transformation attacks such as rotation, scaling and shifting, as those geometric transformation attacks usually desynchronise the watermark extractors and image blocks used for embedding the watermark.

To resist the geometric transformation attacks, instead of embedding a watermark into the whole image region, some region-level watermarking schemes [19–25] embedded watermark into a set of invariant local regions detected by region detectors such as scale-invariant feature transform [26] and speed-up robust feature detector [27]. It has been proven that these region-level watermarking schemes have shown high robustness to the common geometric transformations including rotation, scaling and shifting, since the content of detected local regions used for watermark extraction is invariant under these attacks. However, to ensure accurate extraction of the watermark, these schemes usually selected a set of non-overlapping local regions and embedded the same watermark into each of these regions. This causes the region-level watermarking schemes have limited hiding capacity.

To achieve high robustness and desirable hiding capacity simultaneously, some geometric correction-based watermarking schemes [28, 29] embedded watermark into the image frequency domain and adopted the fuzzy least squares support vector machine, the least squares support vector regression and Bessel K-form distribution to estimate parameters of possible geometric transformations to geometrically correct the watermarked image for watermark extraction. Unfortunately, these schemes cannot accurately correct the watermarked image under combinations of geometric transformations due to its limited ability of parameter estimation. In this study, we propose a novel geometric correction-based image watermarking scheme using geometric correction codes (GCCs). In this scheme, the GCCs are designed and used to geometrically correct the watermarked image for watermark extraction.

Specifically, at the stage of watermark embedding, the watermarked image and pre-set GCCs are combined to form a new watermark binary image, and the new watermark image is embedded into the DCT coefficients of a copyrighted image to obtain the watermarked image. At the stage of watermark extraction, the watermarked image under various geometric transformation attacks is geometrically corrected by minimising the difference between the extracted and the original GCCs, and then the watermark is extracted from the DCT coefficients of geometrically corrected watermarked image. By introducing GCCs in watermarking, the proposed scheme outperforms the typical watermarking schemes in the aspect of robustness to common geometric transformation attacks such as rotation, scaling, shifting and their combinations while it has comparable invisibility with the same embedding capacity.

This study is organised as follows. The proposed scheme is presented in Section 2. Experimental results and analysis are described in Section 3. Finally, the conclusion is drawn in Section 4.

## 2 | PROPOSED SCHEME

### 2.1 | Discrete cosine transform

Discrete cosine transform is the image transformation that converts an image from spatial to the frequency domain, and is widely adopted in image watermarking schemes because the low-frequency DCT coefficients are robust to noise-like attacks. We assume that an image \( f(i, j) \) with the size of \( N \times N \) and \( N \) is integer multiples of 8, and thus the image \( f(i, j) \) can be divided into \( N \times N / 64 \) non-overlapping blocks with a size of \( 8 \times 8 \). The transformation from the spatial to the frequency domain can be expressed by the following Equation (1).

\[
F(u, v) = \frac{c(u) c(v)}{N} \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} f(i, j) \cos \left(\frac{(2i + 1) u \pi}{2N}\right) \cos \left(\frac{(2j + 1) v \pi}{2N}\right)
\]

The inverse DCT that transforms the image from the frequency to the spatial domain can be expressed as follows:

\[
f(i, j) = \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} F(u, v) \cos \left(\frac{(2i + 1) u \pi}{2N}\right) \cos \left(\frac{(2j + 1) v \pi}{2N}\right)
\]

In Equations (1) and (2), \( u = 0, 1, ..., N-1, v = 0, 1, ..., N-1, \) and

\[
c(k) = \begin{cases} \frac{1}{\sqrt{N}}, & k = 0 \\ \frac{2}{\sqrt{N}}, & k \neq 0 \end{cases}
\]

### 2.2 | Geometric correction codes

As shown in Figure 1, the GCCs are arranged around the watermarked image to form the new watermark image. There are four GCCs in total, each of which is with the size of \( d' \times d' \). The pixel value of one code is set as 1 and those of the other three GCCs are set as 0. Note that the pixel values of GCCs are not symmetric, as we cannot geometrically correct the watermarked images undergoing 90° rotation transformation by the symmetric GCCs. The setting of the sizes of GCCs is discussed in Section 3.1.

The GCCs can not only geometrically correct the watermarked images undergoing geometric transformations but also locate the embedded watermark information in the watermark extraction stage. Then, after the geometric correction, the watermark can be accurately extracted from the watermarked images. More details are given as follows.
2.3 Framework of the proposed scheme

In practice, an ideal image watermarking scheme should have high robustness to most of the common image attacks with desirable hiding capacity so that the watermark can be accurately extracted under these attacks to prove the ownership if needed. However, it is still a challenge for the existing image watermarking schemes to resist geometric transformation attacks such as rotation, scaling and shifting, which are also called desynchronisation attacks. This is because the geometric transformation attacks would contribute to desynchronisation between embedded pixel blocks and watermark extractors [30, 31]. Therefore, the robustness against the geometric transformation attacks would be significantly improved as long as the watermark extractors are resynchronised with the embedded pixel blocks. To this end, we propose a GCC-based robust image watermarking scheme. Figure 2 shows the overall framework of the proposed watermarking scheme, which consists of watermark embedding and extraction stages.

At the stage of watermark embedding, we pre-set GCCs, which will be used to geometrically correct the watermarked image undergoing various geometric transformation attacks, and then combine GCCs with the original watermark image to form a new watermark image as shown in Figure 1. Then, the new watermark image is embedded into the frequency domain of a cover image by DCT.

At the stage of watermark extraction, to achieve high robustness against geometric transformation attacks, the watermarked image is geometrically corrected by minimising the difference between the original GCCs and the ones extracted from the watermarked image, and then the watermark is extracted from the synchronised watermarked image.

2.4 Watermark embedding

In this section, the watermarked image is embedded into the DCT coefficients of a cover image. The steps of the embedding process of the proposed scheme are detailed as follows. We suppose the information of GCCs is shared between the sender and receiver beforehand.

\[ B_k = \{B_k(i, j)\}_{i, j = 0, 1, \ldots, 7}; \]
\[ k = 0, 1, \ldots, (a + 2d') \times (a + 2d') - 1 \] (4)

Then, DCT technique is applied to transform the image blocks from spatial to frequency domain. The DCT coefficients...
of each image block, denoted as \( C_k(m, n) \), can be obtained by Equation (5):

\[
C_k(m, n) = c(m) \cdot c(n) \cdot \sum_{i=0}^{7} \sum_{j=0}^{7} B_k(i, j) \cos \left( \frac{\pi (2i + 1) m}{16} \right) \cos \left( \frac{\pi (2j + 1) n}{16} \right)
\]

(5)

where

\[
c(m) = \begin{cases} \sqrt{1/8} & m = 0 \\ \sqrt{1/2} & m = 1, 2, \ldots, 7 \end{cases}
\]

\[
c(n) = \begin{cases} \sqrt{1/8} & n = 0 \\ \sqrt{1/2} & n = 1, 2, \ldots, 7 \end{cases}
\]

Step (4): DCT coefficient modification. As shown in Figure 3, once a pair of reference bit \((i_1, j_1)\) and embedding bit \((i_2, j_2)\) in the same image block is selected, the watermark information is embedded by modifying the DCT coefficients of embedding bits using Equation (6):

\[
C_k(i_2, j_2) = \begin{cases} \max \left( C_k(i_2, j_2), C_k(i_1, j_1) + \rho \right), w_k = 1 \\ \min \left( C_k(i_2, j_2), C_k(i_1, j_1) - \rho \right), w_k = 0 \end{cases}
\]

(6)

where \( \rho \) represents the embedding strength, and \( w_k \) represents the watermark information to be embedded. \( C_k(i_1, j_1) \) and \( C_k(i_2, j_2) \) denote the DCT coefficients of reference and embedding bits, respectively. The low-frequency domain is usually used to embedding watermark, in this study, we set the reference bit to (2, 2) and the embedding bit to (3, 3).

Step (5): Watermarked image generation: After the above steps, the watermark information has been embedded into the frequency domain of the cover image. The inverse DCT transformation is performed on the coefficients of each block, and then YCrCb colour space is transformed to RGB colour space to generate the final watermarked image.

2.5 | Watermark extraction

It is a common phenomenon that watermarked images would undergo a variety of intentional or unintentional geometric transformation and noise-like attacks during transmission since the internet is open to all users. Especially, the geometric transformation attacks, that is, desynchronisation attacks, would make the accurate extraction of watermarks quite difficult.

To resist the geometric transformation attacks, image geometric correction using GCCs is introduced in this subsection. Although the geometric transformation attacks are usually unknown by the receiver, we assume the watermarked image has undergone some common types of geometric transformations, and denote the set of possible geometric transformations as \( \Omega \).

The steps of geometric correction are detailed as follows:

Step (1): GCCs extraction. For each geometric transformation \( \omega \) from \( \Omega \), we assume the watermarked image has undergone this transformation. Then, we attempt to geometrically correct the watermarked image under this assumption and extract embedded GCCs from geometrically corrected watermarked image by DCT transformation. The GCCs are marked in red as shown in Figure 4.

Step (2): Similarity calculation. The extracted GCCs are compared with the original GCCs and the similarity between them can be computed. When the maximum similarity reaches a preset threshold, it can be inferred that the watermarked image has been resynchronised, and the watermark is very likely to be extracted accurately. The geometric transformation that the watermarked image has undergone can be determined by Equation (7):

\[
\omega^* = \arg\min_{\omega \in \Omega} \{ \text{Ext}(T_\omega(I)) - C \}
\]

(7)

where \( I \) denotes the watermarked image, and \( T_\omega(I) \) means the watermarked image has undergone the geometric transformation \( \omega \), respectively. The possible transformation \( \omega \) may be one certain type of rotation, scaling, shifting or their combinations, and \( \text{Ext}(T_\omega(I)) \) and \( C \) denote the extracted GCCs and original ones, respectively. The geometric transformation set \( \Omega \) contains rotation angles varying from 1 to 360° in steps of 1° and the shifting varying from (1, 1) to (512, 512) in steps of 1 pixel. Scaling is not included because the proposed scheme...
resizes the watermarked image to a specific size before extraction to avoid desynchronisation error caused by scaling.

Step (3): Geometric correction. From the above, we have known the transformation type \( \omega^* \) that the watermarked image has undergone, and thus the distorted watermarked image can be geometrically corrected by Equation (8), where \( I \) and \( I^* \) denote the distorted image and recovered one, respectively:

\[
I^* = T_{\omega^*}(I), \quad \omega^* \in \Omega
\]

Step (4): Watermark extraction. The watermark extraction process can be implemented on the geometrically corrected watermarked image. The watermark extraction is the inverse process of watermark embedding. According to the stage of watermark embedding, in order to resynchronise the watermark extractor with the embedded image blocks, the restored image is first scaled to a specific size \( 8(a + 2d') \times 8(a + 2d') \) and then divided into non-overlapping image blocks with a size of \( 8 \times 8 \).

Subsequently, inverse DCT transformation is performed on each image block to construct the coefficient matrix \( C_k \), and watermark information can be extracted by comparing the values of the reference and the embedding bits in each block according to Equation (9).

\[
w_k = \begin{cases} 
1, & C_k(j_2, j_2) > C_k(i_1, j_1) \\
0, & C_k(j_2, j_2) \leq C_k(i_1, j_1)
\end{cases}
\]

\[
W' = \{w_k | w_k \in (0, 1), k = 0, 1, ..., a \times a + 4 \times d \times d - 1\}
\]

Finally, the extracted sequence of watermark information shown in Equation (10) is converted to a binary watermark image.

3 EXPERIMENTAL RESULTS AND ANALYSES

In this section, our parameter settings of the embedding strength, the sizes of GCCs and geometric transformation set \( \Omega \) are first discussed and determined in Section 3.1. Then, the performance test of the proposed scheme is shown in Section 3.2, and the comparison with other typical watermarking schemes is implemented in the aspects of invisibility and robustness in Section 3.3.

In order to evaluate the performances of the proposed watermarking scheme and the typical watermarking schemes [32, 33], the standard image dataset, that is, c512 [34] including 512 \( \times \) 512 sized images such as ‘Lena’, ‘peppers’, ‘baboon’ is adopted. Some test images are shown in Figure 5. Besides, the binary watermark image of size 64 \( \times \) 64 adopted in the scheme [32] is used as the watermarked image, which is shown in Figure 1. In our experiments, both structural similarity index measure (SSIM) and peak signal-to-noise ratio (PSNR) between the original cover and watermarked images are used to measure the invisibility, and the normalised correlation (NC) between the original watermark and recovered watermark is adopted to measure the robustness.

3.1 Parameter settings

In the proposed scheme, the selection of embedding strength \( \rho \) is critical, which will significantly affect the invisibility and robustness of the proposed scheme. Another parameter that needs to be noted is the size of GCCs. In general, the size of the original watermark image is fixed at 64 \( \times \) 64, and the size of the new watermark image is related to those of GCCs. The scheme is designed to enhance the robustness against geometric transformation attacks. Smaller sizes of GCCs mean they could provide less reference for geometric correction. On the contrary, larger sizes of GCCs mean the proposed scheme has.
As shown in Figures 6 and 7, the NC value increases but SSIM value decreases with the increase of the size of GCCs when the embedding strength $p$ is fixed. The GCCs with the small sizes of $2 \times 2$ are too weak to geometrically correct the watermarked image, as the GCCs with small sizes are easy to be lost after attacks. When the GCC sizes are set as $4 \times 4$, the robustness is satisfactory. Thus, there is no need to set the sizes of GCCs as $8 \times 8$ in which the improvement of NC is limited and the SSIM decreases significantly. Hence, it is suitable to set the size of GCCs as $4 \times 4$.

Then, we fix the size of GCCs at $4 \times 4$ to test the impact of parameter $p$ as shown in Figures 6(b) and 7(b). It can be observed that when $p$ increases, the NC value increases but the SSIM value decreases. It means invisibility is sacrificed for higher robustness. The NC increases rapidly when embedding strength is between 50 and 70. However, further increasing $p$ cannot improve robustness significantly. Therefore, we set the embedding strength $p$ to 70. We discuss the definitions of geometric transformation set $\Omega$, as it directly decides the accuracy of watermark extraction and the time consumption. We give three definitions of set $\Omega$ denoted as $\Omega_1$, $\Omega_2$ and $\Omega_3$; where $\Omega_1$ contains rotation angles ranging from 1 to $360^\circ$, $\Omega_2$ contains the shifting transformations with the offset $(1,1)$ to $(512,512)$ in a step of 1 pixel; and $\Omega_3$ denotes the set that include both $\Omega_1$ and $\Omega_2$. We randomly select 10 geometric attack samples from each set and perform those attacks on the dataset. The results shown in Table 1 are the time consumption of a given image under the 10 different attacks from each set, and the right-most column named ‘average’ represents the average value of different test images in the dataset.

It can be clearly observed that time required for watermark extraction is acceptable even under complicated attacks. Thus, to resist multiple geometric transformation attacks, the geometric transformation set $\Omega_3$ is more appropriate for our scheme.

### 3.2 Performance test

According to the above, the size of GCCs is set as $4 \times 4$ and embedding strength is set as 70 in this experiment. To

| Table 1 Time consumed for watermark extraction under different transformation set |
|-----------------|-----------------|-----------------|-----------------|-----------------|
|                 | Baboon          | Lena            | Peppers         | Average         |
| $\Omega_1$      | 0.881 s         | 0.854 s         | 0.865 s         | 0.859 s         |
| $\Omega_2$      | 8.174 s         | 7.893 s         | 8.011 s         | 7.997 s         |
| $\Omega_3$      | 8.745 s         | 8.434 s         | 8.627 s         | 8.592 s         |
investigate the robustness of the proposed scheme, filtering attacks (including Gaussian filtering, median filtering), image enhancement attacks (including histogram equalisation, sharpen), noise-adding attacks (including Gaussian noise, salt & pepper noise), compression attacks (including JPEG compression with different quality factors) and geometric transformation attacks (including rotation, scaling, shifting, cropping and their combinations) are applied on the watermarked images. Then, the watermarks are extracted from these watermarked images by the proposed scheme. The toy examples of watermarked images distorted by these attacks are shown in Figure 8. The corresponding watermarks extracted from these distorted watermarked images are shown in Figure 9.

Since the proposed scheme is designed to resist geometric transformation attacks, to further verify the robustness of this scheme against geometric transformation attacks, not only the Gaussian noise, salt and pepper noise, JPEG compression but also the rotation, scaling, shifting, cropping and their combinations are performed on the watermarked image. It can be observed from Tables 2 and 3 that the proposed scheme shows high robustness on these attacks, especially for JPEG compression, rotation and scaling.

The three cover images and their corresponding watermarked images are shown in Figure wwwww10. There is almost no visual difference between the cover images and the corresponding watermarked images.

### 3.3 Performance comparison

As mentioned above, Gaussian noise, salt and pepper noise, JPEG compression, rotation, scaling and so on are applied to the watermarked images. Tables 2 and 3 summarise robustness test of the proposed scheme and the typical watermarking schemes under different attacks. The proposed scheme demonstrates that it achieves desirable robustness against these attacks, especially the common geometric transformations. On the contrary, the scheme [32] is not robust enough to the geometric transformation attacks, as it is based on the correlation between different channels of colour spaces such as RGB, YCrCb, HSI,
TABLE 2  Normalised correlation (NC) values of extracted watermarks under noise-like attacks between the proposed scheme and the schemes in [32, 33]

| Attacks       | Gaussian noise | Salt and pepper noise | Gaussian filter 3 × 3 | Gaussian filter 5 × 5 | Median filter 3 × 3 | Median filter 5 × 5 | Histogram equalisation | Sharpening | JPEG (90%) |
|---------------|----------------|-----------------------|-----------------------|-----------------------|---------------------|---------------------|------------------------|-------------|------------|
| Baboon Proposed | 0.9495 | 0.9917 | 0.9734 | 0.9459 | 0.9385 | 0.5303 | 0.9991 | 1 | 1 |
| [32] | 0.8883 | 0.9450 | 0.8441 | / | 0.7647 | / | 0.9802 | 0.9532 | 0.9555 |
| [33] | 0.9429 | 0.8286 | 1 | 1 | 0.9232 | 0.2775 | 1 | 1 | 1 |
| Lena Proposed | 0.9596 | 0.9899 | 0.9771 | 0.9615 | 0.9541 | 0.5073 | 0.9972 | 0.9991 | 0.9991 |
| [32] | 0.9063 | 0.9396 | 0.9243 | / | 0.8811 | / | 0.9991 | 0.9991 | 0.9604 |
| [33] | 0.9548 | 0.8672 | 1 | 1 | 0.9842 | 0.8857 | 1 | 1 | 1 |
| Peppers Proposed | 0.9615 | 0.9881 | 0.9798 | 0.9688 | 0.9752 | 0.5294 | 0.9982 | 0.9984 | 0.9982 |
| [32] | 0.8541 | 0.9228 | 0.8613 | / | 0.8162 | / | 0.9865 | 0.9874 | 0.9775 |
| [33] | 0.9763 | 0.8073 | 1 | 1 | 0.9862 | 0.9015 | 1 | 1 | 1 |
| Average Proposed | 0.9564 | 0.9889 | 0.9747 | 0.9581 | 0.9544 | 0.5229 | 0.9982 | 0.9991 | 0.9991 |
| [32] | 0.8829 | 0.9358 | 0.8766 | / | 0.8207 | / | 0.9886 | 0.9799 | 0.9778 |
| [33] | 0.9553 | 0.7810 | 1 | 1 | 0.9650 | 0.7394 | 0.9925 | 1 | 1 |

Note: “/” indicate that the result is not provided.

TABLE 3  NC values of extracted watermarks under geometric attacks between the proposed scheme and the schemes in [32, 33]

| Attacks     | Rotation (1°) | Rotation (10°) | Rotation (75°) | Scaling (0.5) | Scaling (1.6) | Crop (25%) | Shifting (0.50) | Shifting (50.0) | Rotation (20°)+ Scaling (1.5) |
|-------------|---------------|----------------|---------------|---------------|---------------|------------|-----------------|-----------------|-----------------------------|
| Baboon       | 0.9901 | 0.9897 | 0.9862 | 0.9101 | 0.9972 | 0.8570 | 0.9689 | 0.9607 | 0.9989 |
| [32] | / | 0.9333 | / | / | 0.8964 | / | / | / | 0.7854 |
| [33] | 0.9429 | / | 0.7509 | 0.9291 | / | 0.8379 | / | / | / |
| Lena Proposed | 0.9889 | 0.9899 | 0.9927 | 0.9321 | 0.9963 | 0.8432 | 0.9717 | 0.97 | 0.9990 |
| [32] | / | 0.9596 | / | / | 0.9640 | / | / | / | 0.8667 |
| [33] | 0.9548 | / | 0.9448 | 0.9862 | / | 0.7778 | / | / | / |
| Peppers Proposed | 0.9914 | 0.9911 | 0.9899 | 0.9486 | 0.9963 | 0.8761 | 0.9750 | 0.9782 | 0.9972 |
| [32] | / | 0.9491 | / | / | 0.9258 | / | / | / | 0.8604 |
| [33] | 0.9763 | / | 0.9252 | 0.9901 | / | 0.8193 | / | / | / |
| Average Proposed | 0.9901 | 0.9902 | 0.9891 | 0.9312 | 0.9971 | 0.8587 | 0.972 | 0.9702 | 0.9982 |
| [32] | / | 0.9473 | / | / | 0.9287 | / | / | / | 0.8375 |
| [33] | 0.9553 | / | 0.7688 | 0.9348 | / | 0.7675 | / | / | / |

FIGURE 10  Invisibility comparison. First column: The new watermark image, which consists of the original watermark image (64 × 64) and the GCCs; second and third columns: The cover and the watermarked images; fourth and fifth columns: The SSIM and peak signal-to-noise ratio values between the cover and the watermarked images.
In summary, compared to the typical watermarking scheme, the proposed scheme achieves much higher robustness to the common attacks, especially the common geometric transformations, while it has comparable invisibility.

4 | CONCLUSION

In this study, we have presented a robust image watermarking scheme. Due to the introduction of the GCCs, the proposed scheme is robust to geometric transformation attacks such as rotation and scaling, which are difficult to resist with desirable high capacity. However, the proposed scheme is still not robust enough to cropping attack. Our further work is to enhance the robustness against cropping attacks while maintaining desirable hiding capacity.

ACKNOWLEDGEMENTS

This work is supported in part by the National Natural Science Foundation of China under Grant 61972205, U1836208, U1836110, in part by the National Key R&D Program of China under Grant 2018YFB1003205, in part by the Priority Academic Program Development of Jiangsu Higher Education Institutions (PAPD) fund, in part by the Collaborative Innovation Center of Atmospheric Environment and Equipment Technology (CICAET) fund, China, in part by Ministry of Science and Technology under Grant MOST 108-2221-E-259-009-MY2 and 109-2221-E-259-010, Taiwan.

ORCID

Zhili Zhou https://orcid.org/0000-0002-5641-7169

REFERENCES

1. Zhou, Z.L., Mu, Y., Wu, Q.M.J.: Coverless image steganography using partial-duplicate image retrieval. Soft Comput. 23(13), 4927–4938 (2019)
2. Zhou, Z.L., et al.: Near-duplicate image detection system using coarse-to-fine matching scheme based on global and local CNN features. Mathematics 8(4), 1–16 (2020)
3. Zhou, Z.L., et al.: Region-level visual consistency verification for large-scale partial-duplicate image search. ACM Trans. Multimedia Comput. Commun. Appl. 16(2), 1–25 (2020)
4. Barni, M., et al.: A DCT-domain system for robust image watermarking. Signal Process. 66(66), 357–372 (1998)
5. Al-Haj, A.: Combined DWT-DCT digital image watermarking. J. Comput. Sci. 3(9), 740–746 (2007)
6. Cedillo-Hernández, M., et al.: Robust hybrid color image watermarking scheme based on DFT domain and 2D histogram modification. Signal Image Video Process. 8(1), 49–63 (2014)
7. Singh, D., Singh, S.K.: DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection. Multimedia Tools Appl. 76(11), 13001–13024 (2017)
8. Chu, W.C.: DCT-based image watermarking using subsampling. IEEE Trans. Multimedia 5(1), 34–38 (2003)
9. Lin, S.D., et al.: Improving the robustness of DCT-based image watermarking against JPEG compression. Comput. Stand. Interfaces 32(1–2), 54–60 (2010)
10. Singh, A.K., Dave, M., Mohan, A.: Hybrid technique for robust and imperceptible image watermarking in DWT–DCT–SVD domain. National Acad. Sci. Lett. 37(4), 351–358 (2014)
11. Fang, H., et al.: A robust image watermarking scheme in DCT domain based on adaptive texture direction quantization. Multimedia Tools Appl. 78(7), 8075–8089 (2019)
12. Sun, L., et al.: A robust image watermarking scheme using Arnold transform and BP neural network. Neural Computing Appl. 30(8), 2425–2440 (2018)
13. Li, D., et al.: A novel CNN based security guaranteed image watermarking generation scenario for smart city applications. Inf. Sci. 479, 432–447 (2019)
14. Mun, S., et al.: Finding robust domain from attacks: A learning framework for blind watermarking. Neurocomputing 337, 191–202 (2019)
15. Liu, Y., et al.: A novel two-stage separable deep learning framework for practical blind watermarking. In: Proceedings of the 27th ACM International Conference on Multimedia, Nice, France, pp. 1509–1517 (2019)
16. Mei, S., et al.: Decision of image watermarking strength based on artificial neural networks. In: Proceedings of the 9th International Conference on Neural Information Processing, Singapore, pp. 2430–2434 (2002)
17. Kandi, H., et al.: Exploring the learning capabilities of convolutional neural networks for robust image watermarking. Comput. Secur. 65, 247–268 (2017)
18. Zhong, X., Shih, F.Y.: A robust image watermarking system based on deep neural networks. 201–210 (2019), arXiv:1908.11331
19. Gao, X., et al.: Geometric distortion insensitive image watermarking in affine covariant regions. IEEE Trans. Syst. Man Cybern. Part C Appl. Rev. 40(3), 278–286 (2010)
20. Nam, S.H., et al.: A SIFT features based blind watermarking for DIBR 3D images. Multimedia Tools Appl. 77(7), 7811–7850 (2018)
21. Yu, Y., et al.: Robust localized image watermarking based on invariant regions. Digital Signal Process. 22(1), 170–180 (2012)
22. Wang, X., Wu, J., Niu, P.: A new digital image watermarking algorithm resilient to desynchronization attacks. IEEE Trans. Inf. Forensics Secur. 2(4), 655–663 (2007)
23. Wang, X., et al.: Geometrically invariant colour image watermarking scheme using feature points. Sci. China Ser. F: Inf. Sci. 52(9), 1605–1616 (2009)
24. Wang, C., Zhang, Y., Zhou, X.: Robust image watermarking algorithm based on ASIFT against geometric attacks. Appl. Sci. 8(3), 410 (2018)
25. Wang, X., et al.: A new robust digital watermarking using local polar harmonic transform. Comput. Electr. Eng. 46, 403–418 (2015)
26. Lowe, D.G.: Object recognition from local scale-invariant features. In: Proceedings of the Seventh IEEE International Conference on Computer Vision, Kerkyra, Greece, vol. 2, pp. 1150–1157 (1999)
27. Bay, H., et al.: Speeded-up robust features (SURF). Comput. Vision Understanding 110(3), 346–359 (2008)
28. Wang, C., et al.: Geometric correction based color image watermarking using fuzzy least squares support vector machine and Bessel K form distribution. Signal Process. 134, 197–208 (2017)
29. Wang, X., et al.: Synchronization correction-based robust digital image watermarking approach using Bessel K-form PDF. Pattern Anal. Appl. 23(2), 933–951 (2020)
30. Yan, B., et al.: Structure compliant local warping of images with applications to watermarking attack. Multimedia Tools Appl. 75(21), 13451–13479 (2016)

31. D’angelo, A., Barni, M., Merhav, N.: Stochastic image warping for improved watermark desynchronization. EURASIP J. Inf. Secur. 2008(1), pp. 1–14 (2008)

32. Li, J., et al.: Color image watermarking scheme based on quaternion Hadamard transform and Schur decomposition. Multimedia Tools Appl. 77(4), 4545–4561 (2018)

33. Moosazadeh, M., Ekhatanifard, G.: A new DCT-based robust image watermarking method using teaching-learning-based optimization. J. Inf. Secur. Appl. 47, 28–38 (2019)

34. Rodriguez-Sanchez, R., et al.: Computer Vision Group. University of Granada, Granada, Spain (2002). http://decsai.ugr.es/cvg/dbimagenes/c512.php

How to cite this article: Zhou Z, Zhu J, Su Y, Wang M, Sun X. Geometric correction code-based robust image watermarking. IET Image Processing 2021;1–10. https://doi.org/10.1049/ipr2.12143