A Dual-Watermarking Scheme Robust to Affine Transformation

Liu Feng12*

1 State key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou Science and Technology Institute, Zhengzhou City, Henan Province, 450000, China
2 College of Software Engineering, Zhengzhou University of Light Industry, Zhengzhou City, Henan Province, 450000, China
*Corresponding author’s e-mail: 2014018@zzuli.edu.cn

Abstract. This paper proposes a robust watermarking algorithm based on dual watermarking and robust affine transformation. First, the color image is divided into three channels, feature point extraction, watermark embedding, and location watermark extraction will be performed respectively. Feature points are used for image reconstruction when extracting watermarks. The watermark embedding needs to select a square area not at the edge of the image as the watermark embedding position, and then embed the watermark in the frequency domain of the corresponding area. According to the watermark embedding position, extract the zero watermark in another channel as the location watermark. Because the zero watermark does not modify the original image information, it has good robustness and can assist the attacked image to locate the watermark embedding position.

1. Introduction
With the popularization of portable digital devices and the rapid development of network transmission, remakes, screen shots, and piracy have become increasingly serious. Digital watermarking technology, which can provide copyright protection for digital media, has received increasing attention. Image robust watermark can resist attacks such as normal image processing operations, noise interference, and geometric deformation. Among them, the anti-affine transformation watermark that can resist attacks such as rotation, scaling, and stretching is the focus of robust watermark research. The problem to be solved is how to effectively resist the attack and extract the digital watermark smoothly when facing a combination of common geometric attacks such as rotation, scaling and translation.

The biggest impact of geometric attacks such as affine transformation on the carrier image is that the watermark is difficult to synchronize, which directly affects the watermark extraction effect. At present, watermarking schemes that can resist geometric attacks are mainly divided into three categories: The first category is to embed the watermark in the affine invariant subspace, and the more common ones are based on DFT transform [1-2], Fourier-Mellin transform [3-4] and image normalization, etc. [5-6]; the second type is a template-based watermarking technology [7-8], which uses the template hidden in the image to restore the synchronization of the watermark; the third type is the use of the important image Features [9-12], using feature point extraction algorithms to extract important features from the image, and repeatedly embed the watermark in the area around the feature points. The watermarking algorithm based on invariant points uses relatively stable feature points in...
the image to identify the location where the watermark is embedded, and embeds the watermark independently in the local area corresponding to each feature point.

This paper proposes a zero-watermark as location watermark and copyright watermark embedding scheme based on different channels of color images. After extracting the zero-watermark in specified area, combined with estimate the affine matrix parameters for image reconstruction, it can embed watermark in corresponding area. The watermarking algorithm in this paper can effectively synchronize the watermark embedded area while resisting the attack of affine transformation, and then extract the watermark correctly.

2. The scheme of location watermark
In the watermark embedding, assuming that the size of carrier image $I$ is $N \times N$, the embedding position used for watermark embedding in the image is a square area with a starting point of $(x, y)$ and size $M \times M$ where $M < N$. First, find a region $Area$ with starting point $(x, y)$ and size $M \times M$ on the R channel of carrier image $I$. Then perform first-order DWT transformation on $Area$ to obtain the low-frequency subband $LL$ and divide $LL$ into non-overlapping $m \times m$ sub-blocks. The size of subband $LL$ is $\frac{M}{2} \times \frac{M}{2}$, total number of subblocks is $K = \left(\frac{M}{2m}\right)^2$. Next perform SVD transformation on each sub-block, $L_i = U_i \Sigma_i V_i^T$, where $U_i$ and $V_i$ are orthogonal matrices, $\Sigma_i$ is a diagonal matrix, and $\sigma_i^k (k=1,2,\cdots,m)$ is its $m$ singular values. Finally judge the maximum singular value of each sub-block. For the parity of the highest digit, the watermark value of odd-numbered records is "0", and the watermark value of even-numbered records is "1", the final watermark sequence $w_{m}$ is obtained.

$$ w_{m_i} = \begin{cases} 0 & \sigma_i^j \text{ is odd number} \\ 1 & \sigma_i^j \text{ is even number} \end{cases} $$

The resulting zero-watermark information will be passed to the extractor as a key, and used as a location watermark to locate the embedded position of the watermark when extracting the watermark. When positioning, the similarity between different blocks and the watermark is calculated according to the window sliding method, and the block with the highest similarity is regarded as the starting block of the embedded position of the copyright watermark.

3. The scheme of dual-watermark
The location watermark method proposed in Section 2 can help the image before and after the attack to match the watermark embedding position. But the copyright watermark still needs to be embedded in the carrier image. Extract feature points on G channel for image reconstruction during extraction; extract location watermark on R channel to match the embedding start position of the copyright watermark; embed a robust watermark on B channel for copyright protection. As shown in Figure 1, the blue area on the image indicates the watermark embedding position. The green, red and blue shade indicates the use of the green, red and blue channel respectively. The different channels need merged to obtain the final watermark image in the final restoration.

3.1. Embedding copyright watermark
The copyright watermark needs to be embedded on B channel. Assuming the $n$th DWT transformation is used, corresponding $LL_n$ low-frequency subbands obtained after the transformation are divided into non-overlapping sub-blocks of size $k \times k$, and DCT transformation is performed on each block. $q$ bits are embedded in each sub-block, then the total number of bits that need to be embedded is $Q$. From this, the minimum required embedded area length is $\text{len} = \sqrt{\frac{Q}{q} \times k^2 \times 4n}$. 

2
Figure 1. Watermark embedding process

Watermark sequence is a set $W_m$ of "0" and "1" bits. First, we use ASIFT algorithm extract robust feature points set $F_k(x,y)$ on G channel. Watermark embedding Area has been select with starting point $(x,y)$ and side length $M$ > len. Then $n$th DWT transformation has perform on Area to get $LL_n$. And divide $LL_n$ into $k \times k$ non-overlapping sub-blocks with DCT transformation. Each sub-blocks can embed $m$ bits and $f'_i(j)$ is the watermarked $i$ sub-block coefficients, where $j = 1,2,\cdots,m$:

$$f'_i(j) = (1-\gamma) \times \text{sign}(f_i(j)) \times Q(\lfloor f_i(j) \rfloor) + \gamma \times f_i(j)$$ (2)

$$Q(x) = \begin{cases} 2 \times \left| \frac{x}{2} + 0.5 \right| & W_{mk} = 0 \\ 2 \times \left| \frac{x}{2} + 1 \right| & W_{mk} = 1 \end{cases}$$ (3)

$\gamma$ controls embedding strength, $Q(\bullet)$ is the rule for modifying the corresponding sub-block coefficients according to the watermark bit value, and $mk = 1,2,\cdots,M$ is the sequence of watermark.

After embedded, IDCT transformation is performed to obtain the embedded sub-blocks. Combine the area with $LH_n$, $HL_n$, and $HH_n$ to perform IDWT transformation, and finally obtain a new B channel, which is combined with other channels to obtain a watermarked color image.

3.2. Extract location watermark

The extraction of the location watermark needs to extract the regional watermark size on the received carrier image for matching. Calculate the watermark value of each designated size area and compare it with the location watermark in the key transmission. The area position corresponding to the watermark with the highest similarity is the embedding position of the watermark. The steps are as follows:

Step 1: Use R channel on image $I'$, calculate the watermark value of the square area $Area$, with the side length of the sliding window as $M$, current starting position starting $(x,y)$;
Step 2: Perform the DWT transformation on Area to obtain low frequency subband LL. Divide the LL into m x m non-overlapping sub-blocks. Perform SVD transformation on each sub-block.

Step 3: Determine the parity of the highest digit of the largest singular value of each sub-block, and get one watermark value of $w_{m}'$ for each sub-block:

$$w_{m}' = \begin{cases} 
0 & \text{if } \sigma_i \text{ is even number} \\
1 & \text{if } \sigma_i \text{ is odd number}
\end{cases}$$  \hspace{2cm} (4)

Step 4: Obtain the watermark sequence $w_{m}'$, calculate the BER value between the current $w_{m}'$ and the original watermark $w_{m}$ and record it as $\frac{BER(x',y')}{\sigma}$.

Step 5: Slide the sliding window to the right and down in units of one pixel, repeat Step 2, and record $\frac{BER(x',y')}{\sigma}$, the lowest corresponding point coordinate $(x_{be}'', y_{be}'')$.

The point coordinate $(x_{be}', y_{be}'')$ is the point where watermark embedding position starts.

3.3. Extract copyright watermark

When extracting watermark, needs feature point set $F_{x,y}(x,y)$, watermark embedding position side length $M$, and location watermark $w_{m}$. First, use the feature point set information $F_{x,y}(x,y)$ to reconstruct the image under attack. During image reconstruction, the original feature point set is matched with the extracted feature point set, and the affine transformation inverse matrix is calculated to reconstruct the image. After image is reconstructed to the original position, extract the location watermark to find the embedding position of copyright watermark. Here, the watermark embedding position side length $M$ and the zero watermark information $w_{m}$ are needed. Then, take $(x_{be}', y_{be}')$ as the starting point, side length $M$ as the side length of the area corresponding to the watermark embedding position, and extract the watermark in the corresponding square area $Area_{be}$. Perform DWT transformation on $Area_{be}$ to get $LL_{n}$ layers. Divide $LL_{n}$ layer into $k \times k$ size non-overlapping blocks, and extract $m$ bits from each block.

$$W_{m_{be}'} = \begin{cases} 
0, & \text{if } \text{round}\left(f'\left(j\right)\right) \text{ is even number} \\
1, & \text{if } \text{round}\left(f'\left(j\right)\right) \text{ is odd number}
\end{cases}$$  \hspace{2cm} (5)

4. Experimental results and analysis

The simulation experiment is implemented in the MatlabR2014a environment of the Windows 7 operating system. A total of 50 test images are used in the experiment, all of which are 512 x 512 color images, with pixel values between [0,255]. The average PSNR values is around 42, and the average SSIM values is around 0.997.

Figure 2. The extraction results of zero watermark after images are attacked by different
Figure 2 shows the results of matching zero watermarks after different image attacks. The two horizontal axes represent x and y axis. The vertical direction is the BER of zero watermark matching. It can be seen that there is a unique point closest to 0, through the position of the robust watermark can be accurately located, which provides a guarantee for the accurate extraction of the watermark.

The results in Table 1 show that our scheme has good robustness to different image processing attacks. The accuracy of watermark extraction is above 0.95, and some can reach above 0.99. From the results, it can be seen that our scheme is relatively stable compared with other schemes.

Table 1. Watermark bit accuracy performance under common image processing attacks

| Attacks                | Our    | Pun[11] | Thanh[12] | Zhang[8] |
|------------------------|--------|---------|-----------|----------|
| Gaussian filter 3×3    | 0.995  | 0.990   | 0.853     | 0.996    |
| Median filter 4×4      | 0.994  | 1       | 0.851     | 0.993    |
| Gaussian noise 0.03    | 0.989  | 0.825   | 0.984     | 0.987    |
| JPEG 40                | 0.951  | 1       | 0.923     | 0.938    |

Table 2 is about the results of common geometric attacks. Our method in this paper maintains the accuracy rate of 0.82 or more in the rotation correlation experiment. The results related to the scaling attack show that although the accuracy rate performance is different under different scaling conditions, the overall accuracy rate is maintained above 0.92.

Table 2. Watermark bit accuracy performance under common geometric attacks

| Attacks       | Our    | Pun[11] | Thanh[12] | Zhang[8] |
|---------------|--------|---------|-----------|----------|
| Rotation 5°   | 0.901  | 0.937   | 0.923     | 0.895    |
| Rotation 45°  | 0.821  | 0.752   | 0.801     | 0.762    |
| Scaling 2.0   | 0.981  | 1       | 0.946     | 0.811    |
| Scaling 1.5   | 0.982  | 1       | 0.947     | 0.891    |
| Scaling 0.6   | 0.929  | 0.887   | 0.913     | 0.841    |

In the affine transformation attack experiment, different affine matrices are used. The matrices are respectively (a)\[ \begin{bmatrix} 1.15 & 0.1 & 0 \\ 0 & 1.13 & 0 \\ 0 & 0 & 1 \end{bmatrix} \], (b)\[ \begin{bmatrix} 0.15 & 1.13 & 0 \\ -0.15 & 1.1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \], (c)\[ \begin{bmatrix} 0.9 & -0.12 & 3 \\ -0.1 & 1.09 & 5 \\ 0 & 0 & 1 \end{bmatrix} \], corresponding images are shown in Figure 3.

Figure 3. Transformed images corresponding to different affine matrices

In the affine transformation attack experiment, different affine matrices are used. The matrices are respectively (a)\[ \begin{bmatrix} 1.15 & 0.1 & 0 \\ 0 & 1.13 & 0 \\ 0 & 0 & 1 \end{bmatrix} \], (b)\[ \begin{bmatrix} 0.15 & 1.13 & 0 \\ -0.15 & 1.1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \], (c)\[ \begin{bmatrix} 0.9 & -0.12 & 3 \\ -0.1 & 1.09 & 5 \\ 0 & 0 & 1 \end{bmatrix} \], corresponding images are shown in Figure 3.

Figure 4. Extraction results of zero watermark after different affine transformations

Geometrically attacked image needs image reconstruction before match zero watermark. The interpolation and sampling generated by this process will interfere with the pixels near the embedded
position of the watermark. But there is still a unique point closest to 0 in the image, through which the position of the robust watermark can be accurately located. Table 3 is about the result of affine transformation attack, the result shows that the method in this paper is robust to affine transformation.

| Attacks | Ours | Thanh[12] | Zhang[8] |
|---------|------|-----------|---------|
| (a)     | 0.84 | 0.52      | 0.836   |
| (b)     | 0.82 | 0.51      | 0.732   |
| (c)     | 0.81 | 0.47      | 0.711   |

5. Summary
In order to avoid the effect of feature point extraction on the synchronization of watermark embedding position, this paper proposes a method based on zero watermark to synchronize the watermark embedding position with double watermarks. This method takes advantage of the feature that the zero watermark does not change the image, takes the embedding position as a sub-image of the carrier image, and extracts the zero watermark. The received image is divided into all possible sub-images, and the watermark contrast similarity is extracted. The starting position of the sub-image with the highest similarity is the embedding position of the watermark.

The experimental results show that the similarity of watermarks extracted from different sub-images by zero watermarking shows that the method in this paper has a good performance in the simultaneous watermark embedding position; compared with the existing methods, the method in this paper is not only effective in general single attacks such as rotation. It performs well under zooming conditions, and also performs well when affine transformation attacks occur.

References
[1] Yuan, W., Ling, H., Lu, Z., Zou, F., Yu, Y. (2006) Image Content-based Watermarking Resistant against Geometrical Distortions. In: Signal Processing, 2006 8th International Conference on Guilin.
[2] Urvoy, M., Goudia, D., Autrusseau, F. (2014) Perceptual DFT watermarking with improved detection and robustness to geometrical distortions. IEEE Transactions on Information Forensics and Security 9, 1108-1119.
[3] Shao, Z., Shang, Y., Zhang, Y., Liu, X., Guo, G. (2016) Robust watermarking using orthogonal Fourier–Mellin moments and chaotic map for double images. Signal Processing 120, 522-531.
[4] Kim, B.-S., Choi, J.-G., Park, K.-H. (2003) RST-resistant image watermarking using invariant centroid and reordered Fourier-Mellin transform. In: International Workshop on Digital Watermarking, pp. 370-381.
[5] Yang, C.-Y. (2017) Robust high-capacity watermarking scheme based on Euclidean norms and quick coefficient alignment. Multimedia Tools and Applications 76, 1455-1477.
[6] Xiaolin, J., Zhou, Y., Yanli, Q., Liping, S. (2016) The anti-geometric attack digital watermarking algorithm based on image normalization of local information. In: Information Technology, Networking, Electronic and Automation Control Conference, pp. 1120-1124.
[7] Wang, X.-y., Liu, Y.-n., Li, S., Yang, H.-y., Niu, P.-p. (2016) Robust image watermarking approach using polar harmonic transforms based geometric correction. 174, 627-642.
[8] Zhang, X., Cao, X., Li, J. (2013) Geometric attack resistant image watermarking based on MSER. Frontiers of Computer Science 7, 145-156.
[9] Wang C, Zhang Y, Zhou X. (2018) Robust image watermarking algorithm based on ASIFT against geometric attacks. Applied Sciences, 8(3): 410-428.
[10] Lin L, Deng W. (2019) Research on digital watermarking algorithm for anti-geometric attack. Matec Web of Conferences, 267:1-4.
[11] Pun, C.-M., Yuan, X.-C. (2015) Histogram modification based image watermarking resistant to geometric distortions. Multimedia Tools and Applications 74, 7821-7842.

[12] Thanh, T.M., Tanaka, K., Dung, L.H., Tai, N.T., Nam, H.N. (2018) Performance analysis of robust watermarking using linear and nonlinear feature matching. Multimedia Tools and Applications 77, 2901-2920.