Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 2 (2010) 236–241

Procedia Computer Science

www.elsevier.com/locate/procedia

ICEBT 2010

A Blind Digital Watermark Technique for Color Image Based on Integer Wavelet Transform and SIFT

C.G. Thorat, B.D. Jadhav*

Pune Univ.R.S.C.O.E,Pune - 411033,India

Abstract

This paper presents an anti-geometric attacks algorithm of color image watermarking based on the scale-invariant feature transformation (SIFT). Firstly, the method detects SIFT feature points in the red component of a true color image and filters out the feature points information. Then three-level Discrete Integer Wavelet Transform (DIWT) is performed on the blue and green component of the color image to extract the low-frequency component coefficient. Finally, a binary watermark which has been scrambled is embedded in the low-frequency wavelet coefficients of the blue component. The simulation results show that the algorithm is robust against signal processing and geometric attacks.

Keywords— Digital watermarking; geometric attacks; scale-invariant feature transform; color images, discrete integer wavelet transform

1. Introduction

With the development of second-generation digital watermarking technology, digital watermarking algorithm's robustness against geometric attacks are growing. Especially the algorithm based on SIFT feature region is very robust against geometric attacks. Therefore, it has been studied extensively. Reference [1], [2], [3] have adopted the watermarking algorithm based on SIFT feature region. First of all, detect SIFT feature points on the carrier image, and then select each feature point as the center of a circle to construct circle area with different properties. At last, through the spatial domain quantify method to embed the binary watermarking into characteristic regions. As the watermarking information is embedded in the characteristics of the region, so this method ensures as much as possible the robustness against affine invariant. But in order to realize blind watermarking algorithm, the watermarking is usually embedded into the space domain, which makes such algorithm difficult to obtain a satisfactory robustness in the face of filtering attack, noise attack, JPEG compression attacks, and malicious attacks. In addition, with different carrier images extracted features are different, this may lead to a smaller characteristic region, which makes the watermark embedding capacity was extremely restricted. To solve the above problems, this paper proposes an improved color image watermarking algorithm based on SIFT features region. The algorithm embeds watermarking into DIWT domain to ensure the robustness in face of filtering attack, noise attack, JPEG compression attacks; At the same time, the algorithm separates color carrier image into three different color channels, the red component is used for feature point extraction and the blue component is used for watermark embedding and detecting. This method ensures that the maximum watermarking information can be embedded into carrier image and also uses the wavelet transform coefficients of the blue component and green component in a proper way. Without changing the green component, through comparing the value of both wavelet coefficients to achieve self-adaptive watermark embedding and blind watermarking detection watermark embedding and detecting.

2. Recovery of Geometric Attacks

David G. Lowe in 2004, proposed a new characterization operator called SIFT [4], that is scale-invariant feature transform [6]. Even the image suffers attacks like image zoom, rotate, pan, brightness change and affine transform, the local feature region

* Corresponding Author. Tel.: +091-09766122884
E-mail address:chandrama1684@gmail.com

1877-0509 © 2010 Published by Elsevier Ltd Open access under CC BY-NC-ND license.
doi:10.1016/j.procs.2010.11.030

based on SIFT will not be changed. According to the local image features, SIFT operator extract the image feature points and describe the position, scale and direction of each feature point. Firstly, SIFT operator implement feature detection in scale space; determine the location of feature points and the scale of the feature points. Then use the gradient's main direction of neighborhood point as the direction features of SIFT feature point. This way realize that the SIFT operator is independent on scale and direction.

2.1. Image scaling distortion correction

Scaling of the image will change the image scale directly, while SIFT feature points is achieved under different scales respectively, therefore the scale characteristics of feature points have a proportional relationship with image scaling. Assuming the scale of F feature points is δ_1 before zooming, after the scale operation, the scale of matched feature points is δ_2 . The scale operator on image is s, by the prosperity of scale space, there are $\delta_2 = s\ \delta_1$. Assuming image scaling factor is s, the match point of original image and scaled image constitute a set of M, the number of matching points are m. The scale factor of original image feature point *Pi* is *pi,* the corresponding feature point will become into *Qi* and the scale factor also become into q_i after the scaling operation.

That is:

$$s = \frac{\sum_{i=1}^{m} q_i / p_i}{m} \tag{1}$$

2.2. Image rotation distortion correction

Rotate the image distortion can be calculated based on the angle difference of matching feature points. Assuming image rotation angle is θ, the match points before and after rotating the image constitute a set of M, the number of matching points is m. The center of angle of the original image feature points P_i *is* θ_i. After being rotated, the corresponding feature point will become into *Qi* and the center angle of this point also become into θ_{i1}.

As following:

$$s = \frac{\sum_{i=1}^{m} q_i / p_i}{m} \tag{2}$$

3. Watermarking Scheme

3.1. Watermark Embedding Scheme

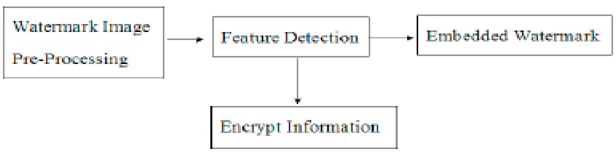

Figure 1. Watermark Embedding Scheme

a) Arnold transform is performed on the watermark image and save the times of Arnold transform as a private key to enhance water marking security.

b) Separate the color carrier image into three color channels. Extract red component for SIFT feature point detection, and save the SIFT feature points of red component as synchronous registration information while watermark detecting.

c) Three levels discrete integer wavelet transform is performed on the blue and green component of carrier image. After that, low-frequency sub-band information of three level wavelet transform will be extracted.

d) The watermark information W, the three level low-frequency integer wavelet transform coefficients B_cA3 of blue component and G_cA3 of green component are reshaped into one-dimensional vector. Watermark embedding scheme accords to the following processes:

```
for i=1:length(W)
       if W(i) = = 1
             if B_cA3(i) <= G_cA3(i)
             B_cA3(i) = G_cA3(i) + T;
            End
      elseif W(i) = = 0
             if B_cA3(i) >= G_cA3(i)
             B_cA3(i) = G_cA3(i) - T;
             End
        End
End
```

e) Implement reshape operation in B_cA3 and G_cA3.Transform them into two-dimensional vector and combine them with the red component. Finally, obtain the image with watermark embedded.

3.2. Watermark Detecting Scheme

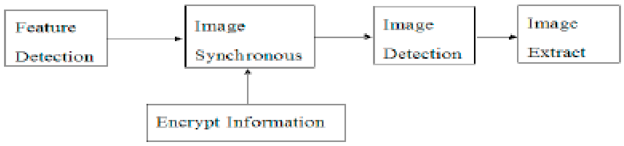

Figure 2. Watermark Detecting Scheme

a) Separate the image with watermark by color channel and extract red component. Then SIFT feature point detection is performed on red component.
b) Synchronize the SIFT feature points with encrypted file to correct geometry attack.
c) Three levels wavelet transform is performed on the blue and green component of image with watermark. After that, low-frequency sub-band information of three level discrete integer wavelet transform will be extracted.
d)The three level low-frequency wavelet transform coefficients B_cA3 of blue component and G_cA3 of green component are respectively reshaped into one-dimensional vector. The watermark detecting scheme are the following:

```
for i=1:length(B_cA3)
     if B_cA3(i) >= G_cA3(i)
         W(i) = 1;
     elseif B_cA3(i) < G_cA3(i)
         W(i) = 0;
      end
end
```

e) Transformed the extracted one-dimensional vector information W into two-dimensional matrix. According to the key information to implement Arnold inverse transform, then obtain the watermark image which has been attacked.

4. Experimental Results

4.1. Geometric distortion correction simulation results

Select Lena grey image as test image, implement rotate attack, scale attack, rotation and shear simultaneous attacks respectively. TABLE I, TABLE II and TABLE III are the simulation results:

- Rotation correction: counter-clockwise rotation, rotation angle is from 10°to 338°.

TABLE I. RESU LTS OF GEOMETRIC DISTORTION CORRECTION

Rotation Angle	Matched Point	Angle correction	Accuracy
10	317	9.9320	99.32%
30	370	30.1393	99.54%
90	690	89.9040	99.89%
136	369	135.8435	99.88%
181	558	180.3369	99.63%
258	327	258.0430	99.98%
272	513	270.9796	99.62%
295	368	294.9406	99.98%
338	345	337.9015	99.97%

- Scaling correction: scaling transform, scaling factor from 0.1 to 2.0

TABLE II. RESULTS OF SCALING CORRECTION

Scale Factor	Matched Point	Scaling correction	Accuracy
0.1	8	0.1001	99.90%
0.3	55	0.3366	87.80%
0.5	120	0.4908	98.16%
0.8	232	0.8179	97.76%
1.2	376	1.1975	99.79%
1.5	433	1.4940	99.60%
1.8	446	1.8193	98.93%
2.0	521	2.0498	97.51%

- Rotation and shear attack correction: the test image is sheared by half (shown in Fig.3) and rotation attack angle is from 1°to 237°

Figure 3. Sheared testing image

TABLE III. RESULTS OF ROTATION AND SHEAR ATTACK CORRECTION

Rotation Angle	Matched Point	Angle correction	Accuracy
30	127	30.1004	99.67%
45	108	48.4911	92.24%
90	284	89.8675	99.85%
237	328	237.4175	99.82%

4.2. Watermark embedding and detecting simulation results

- Carrier image: 512 X 512 RGB true color image, as shown in Fig.4

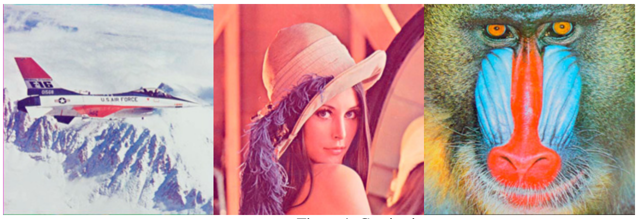

Figure4. Carrier image

- Watermark image: 64 X 64 binary image, as shown in Fig.5.

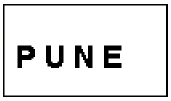

Figure5. Watermark image

To verify the analysis above, simulations are carried out using standard 512·512 RGB color images as the carrier image, 64·64 binary image as watermark image, the threshold T = 50. The simulation results shown in TABLE IV:

TABLE IV. THE NC UNDER SIGNAL PROCESS AND GEOMETRIC ATTACK

Attack Type	Parameter	Mandrill NC	Lena NC	Airplane NC
JPEG	50	0.9726	0.9709	0.9582
	60	0.9797	0.9789	0.9724
	70	0.9875	0.9831	0.9744
	80	0.9939	0.9904	0.9782
SHEAR	Upper Left 1/4	0.9894	0.9830	0.9896
	Center 1/4	0.9926	0.9879	0.9917
	Right Down 1/4	0.9864	0.9838	0.9863
MEDIAN FILTER	3*3	0.9712	0.9965	0.9899
	5*5	0.9534	0.9838	0.9758
SCALE	50%	0.9999	0.9992	0.9985
	75%	0.9950	0.9966	0.9948
	150%	0.9903	0.9947	0.9908
	200%	0.9971	0.9967	0.9933
ROTATE	10%	0.9954	0.9915	0.9824
	30%	0.9635	0.9931	0.9824
	45%	0.9887	0.9950	0.9876
	90%	0.9829	0.9924	0.9874
ROTATE + SHEAR	-2,75%	0.9682	0.9141	0.9206
	+2,75%	0.9897	0.9458	0.9446
ROTATE + SCALE	-2,75%	0.9643	0.9110	0.9184
	+2,75%	0.9883	0.9429	0.9339

As we can see from TABLE Ⅳ, the algorithm presented in this paper compared with the results in [5], not only greatly enhanced the general robustness of the signal processing operations, but also significantly increased the geometric attack robustness.

4.3. Experimental analysis

Based on the above simulation results, we analysis the robustness of algorithm in the following:

a) Robustness under signal process: Since DIWT has advantage on time-frequency analysis and also for the reason that human eye is insensitivity to the blue color, we choose the low frequency coefficient of blue component to embed the watermark image. Even the image with watermark suffers attacks such as JEPG compressed, median filtering and other signal process, we can still detect and recover the watermark image.

b) Robustness under geometric attack : We make good use of the property of color image to embed watermark image. In the first, the R channel is used for SIFT feature point detection and synchronization. After this being done, even the image is attacked in the way of rotation, scale, shear and other geometric transform, the watermark still keeps a high value of NC with original watermark image. Meanwhile, we through the way of comparing the low frequency coefficient in both B and G channel to embed the watermark information. Not only it ensures that the watermark embedding channels and SIFT feature point detection channel are separated and gets the maximum the amount of watermark embedding, but also it uses color images features to make this algorithm as blind watermarking algorithm. Therefore, we don't need original image while detecting the watermark image.

5. Conclusions

In this paper, we propose an improved color image algorithm based on SIFT feature point. Our contributions can be summarized as follows:

(a)The watermark embedded channel and SIFT feature points detection channel are separated, we can embed much more watermark information into same carrier image than the method in [1], [2], [3].

(b)By comparing the value of DIWT coefficient of B channel with the value of G channel, we can detect watermark without need original image. Simulation results and comparisons have demonstrated the advantages of the proposed scheme.

References

[1] Seo J. S. ,Yoo,C. D. " Image watermarking based on invariant regions of scale-space representation[J]," IEEE Transaction on Signal Processing, 2006, 54(4), pp. 1537~1549.

[2] Lee. H. Y, Lee. C. H, Lee. H. K, " Geometrically invariant watermarking: synchronization through circular Hough transform" in Multimedia Tools and Applications, 2007, 34(3), pp.337-353.

[3] H. Y. Lee, C. Lee, H. K. Lee, "Evaluation of feature extraction techniques for robust watermarking," Proceedings 4th International Workshop on Digital Watermarking (IWDW), 2005, pp. 418~431.

[4] Bas. P. Chassery, J-M, Macq. B, "Geometrically invariant watermarking using feature points," IEEE Transactions on Image Processing, 2002, 11(9), pp. 1014~1028.

[5] H. Y. Lee, H. S. Kim, and H. K. Lee, "Robust image watermarking using local invariant features," Opt.Eng., vol.45, no.3, 2006, pp.1-11.

[6] Marr D, Hildreth E, "Theory of edge detection," Proc. Royal Society of London, 1980, B-207, pp. 187-217.