COLOR IMAGE WATERMARKING USING LOCAL QUATERNION FOURIER SPECTRAL ANALYSIS

Xiaojun MA[1], Yi XU[1], Li SONG[1], Xiaokang YANG[1,2] and Hans Burkhardt[2]

[1]Institute of Image Communication and Information Processing, Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai 200240, China
[2]Institute for Computer Science, University of Freiburg, Germany
E-mail: {zxmhuailema27, xuyi, song_li, xkyang}@sjtu.edu.cn, Hans.Burkhardt@informatik.uni-freiburg.edu

ABSTRACT

We propose a watermarking scheme for color images based on local quaternion Fourier spectral analysis (LQFSA).The merits of the proposed scheme include: 1) Quaternion Fourier transform is defined in a 4D vector space and thus provides a larger embedding scope for watermark than conventional monochannel transformation techniques. 2) We improve the imperceptibility of watermark with regard to human color vision properties through LQFSA. 3) We introduce invariant feature transform (IFT) and geometric correction scheme so as to enhance the robustness to extensive attacks, which is another essential factor to evaluate a watermarking scheme. 4) We adopt the nearest-neighborhood search to ensure the correctness of watermark extraction. Extensive experiments on the Stirmark platform validate the aforementioned merits.

Index Terms— Color Image Watermarking, Local Quaternion Fourier Spectral Analysis

1. INTRODUCTION

Watermarking is an important technique to resolve the ownership protection problem of digital media. Each watermarking scheme can be described as two stages: mark embedding and mark extraction. It is known that the image mark should be placed in significant pixels without affecting the perceptual quality. On the other hand, mark extraction should be feasible even the external attacks have destroyed the synchronization in the watermarked bit stream. Significant progress has been made in watermarking of digital images. However, many challenging problems still remain in practical applications, e.g., the trade-off between imperceptibility and robustness of embedded mark and the resilience of watermarking to geometric attacks.

To determine the significance of each pixel, many watermarking schemes work in the transformed domain with the help of frequency analysis. However, these mono-channel transformation techniques cope with the channels of color images separately, which might reduce the capacity of information embedding. Recently, Bas *et al.* proposed a digital color image watermarking scheme in Quaternion Fourier Transform (QFT) domain [1]. It processes the channels of images coherently thus increases the information capacity, and gains the ability to project the image to the color axis along which the perceptual impact of data variations is minimal. The imperceptibility is emphasized in Bas' work but the robustness to extensive attacks is somehow overlooked. Later T.K.Tsui [2] proposed a new quaternion based watermarking. It interprets the QFT coefficients using spatio-chromatic Fourier analysis and robustness and invisibility is balanced by modifying both positive and negative coefficients. But this scheme only deals with most common attacks.

Many of the existing watermarking schemes become ineffective after geometric attacks. Examples of geometric attacks include rotation, scaling, translation, shearing, bending, and change of aspect ratio. To retain invariance under geometric distortions, recently the concept of invariant features is introduced into a series of watermarking schemes [3][4][5]. These features are composed of the most significant pixels or provide an invariant measure of the whole image, so that it is difficult to destroy them even if a variety of geometric attacks are enforced. However, geometric attacks would introduce local shift variance into images along with other signal processing attacks, which is generally ignored by the state-of-art watermark detection procedure. The resultant variance of embedding locations would lead to watermark extraction failure.

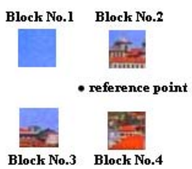
In this paper, we develop a robust watermark scheme for color image in order to resist a wide range of watermark attacks including geometric distortion and common image processing. It takes the merits of QFT to improve the imperceptibility, IFT to tackle geometric attacks, and nearest-neighborhood search strategy to increase the probability of correct watermark extraction.

2. WATERMARK EMBEDING BASED ON LQFSA

According to a fixed distance from each reference point, we select four 32×32 blocks around it to be the candidates for watermark embedding. The details of how to select reference points will be discussed in Section 2.2. Here we first focus on the selection of blocks and the execution of watermark embedding.

2.1. Selection of blocks and execution of watermarking based on LQFSA

It is known HVS is more insensitive to the changes in textured regions than the same amount of changes in the flat regions. LQFSA is utilized here to roughly estimate the richness of the color texture through comparing the non-DC QFT component magnitude, as referred to (1). Two blocks with more textures around each reference point are selected out for watermark embedding to improve the imperceptibility, as shown in Fig.1. It should be noted that we embed the same watermark sequence in the QFT domain around each reference point to enhance the robustness.



Block	Non-DC QFT magnitudes	Selected state
No.1	0.237	No
No.2	1.754	Yes
No.3	1.714	No
No.4	1.756	Yes

Fig.1. Selection of embedding blocks

Local QFT:

$$F^q(u,v) = \int_{-\frac{a}{2}}^{+\frac{a}{2}} \int_{-\frac{b}{2}}^{+\frac{b}{2}} e^{-i2\pi ux} f(x,y) e^{-j2\pi vy}\, dxdy \quad (1)$$

Non-DC QFT component magnitude:

$$S = \frac{1}{32\times 32} \sum_{u\neq 0, v\neq 0} |F^q(u,v)| \quad (2)$$

where *a*, *b* respectively denote the width and height of the embedding block and $i^2 = j^2 = -1, ij = -ji = k$. The general representation of a quaternion can be formulated as a hypercomplex number $q = a + b\cdot i + c\cdot j + d\cdot k$, $a, b, c, d \in \mathbb{R}$, where we indicate a, b, c, d as the R part, I part, J part and K part of the quaternion. Thus QFT domain is a 4D vector space and provides a larger embedding scope than the monochannel transformation techniques such as DCT and DWT. Due to the following two reasons, we implement the bit embedding only in the three imaginary parts of QFT coefficients. For a RGB color image, each pixel can be depicted as a pure quaternion, namely $q = b\cdot i + c\cdot j + d\cdot k$. It can be inferred that the important DC energy of the R part in tQFT domain takes zero value. Thus the watermark embedded in the non-DC components of the R part becomes fragile under filtering attacks. Moreover, it is convenient to extend this implementation to quaternion wavelet domain [6] and always preserve pure quaternion form during transformation to avoid color distortion.

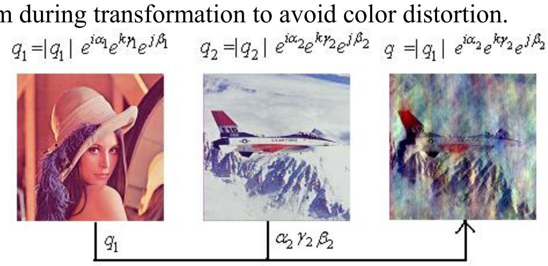


Fig.2. The perceptual impact of quaternion phases

To enhance the imperceptibility of our watermarking scheme, we should establish a measure to estimate the visual distortion caused by the bit embedding. It is well known that the phase spectrum takes larger information entropy than the amplitude spectrum and encodes the type and relative location of image structures. Thus quaternion Fourier phases dominantly determine the perceptual impact on human eyes, as shown in Fig.2.

Given the polar representation of a quaternion $q = |q|e^{i\alpha}e^{k\gamma}e^{j\beta}$, we set up the visual distortion measure based on phase deviations incurred by watermark embedding,

$$\mathrm{VD} = |\alpha_o - \alpha_w| + |\beta_o - \beta_w| + |\gamma_o - \gamma_w| \quad (3)$$

where the subscripts o and w respectively indicate the quaternion phase of the original image and the watermarking image. As for the same amount of embedding bits, we compute the VD value when the embedding happens respectively to the I part, J part and K part of QFT image around seven reference points, as shown in Table I. The perceptual results are correspondingly listed in Fig. 3(b), (c) and (d).

Table I. VD Analysis

Embedding Channel (70 bits)	I part	J part	K part
Sum of VD (rad)	136.8	103.3	94.1

(a) Original image (b)embedding in I part (c)embedding in J part (d)embedding in K part

Fig.3. Perceptual comparison

It is observed that data embedding in I part causes the largest visual distortion while the one in K part takes the smallest one. It is known imperceptibility and robustness of watermark are the two sides of one thing. To make a trade-off, we embed more bits in J part. For example, we embed 10 bits in J part and 6 bits both in I part and K part. As a result, 22 bits are embedded in each block and thus 44 bits around each reference point. The pseudocode of the embedding procedure for one bit is written as below,

```
Let K = mod2(Round(C/α))
If w = 0 and K = 0, Then C = Round(C/α) × α
If w = 0 and K = 1, Then
  If C > Round(C/α) × α, Then C = (Round(C/α) + 1) × α
  Else C = (Round(C/α) − 1) × α
If w = 1 and K = 1, Then C = Round(C/α) × α
If w = 1 and K = 0, Then
  If C > Round(C/α) × α, Then C = (Round(C/α) + 1) × α
  Else C = (Round(C/α) − 1) × α
```

where *C* denotes the QFT coefficient of a given imaginary part, *α* is the watermark strength, *w* is the binary watermark bit generated by the secret key. In essence, the basic idea behind the code is to quantize coefficient *C*, where *α* acts as the quantization step. Given the QFT coefficient at frequency $(u_0, v_0)^T$, the embedding procedure should follow the conjugate symmetry rule of QFT, namely

$$F^q(u_0, -v_0) = -i \cdot F^q(u_0, v_0) \cdot i \tag{4}$$

$$F^q(-u_0, v_0) = -j \cdot F^q(u_0, v_0) \cdot j \tag{5}$$

$$F^q(-u_0, -v_0) = -k \cdot QF^q(u_0, v_0) \cdot k \tag{6}$$

Finally, inverse QFT is applied to the embedding blocks to obtain the watermarked image.

2.2. Selection of reference points using IFT

We adopt invariant feature transform (IFT) to get significant reference points. Here quaternion phase congruency model (QPCM) in our previous work is first used to extract a large number of reliable feature points, which has been proved as a quite effective IFT method [6]. Then fifteen points with the largest characteristic scale are selected as reference points because they present themselves in a more global sense in an image. If some of them are neighbors, we only retain the point with the largest characteristic scale to avoid the interference between features. The computation of characteristic scale can be referred to [6]. Until now, we could outline the flowchart of our watermark embedding procedure, as shown in Fig.4.

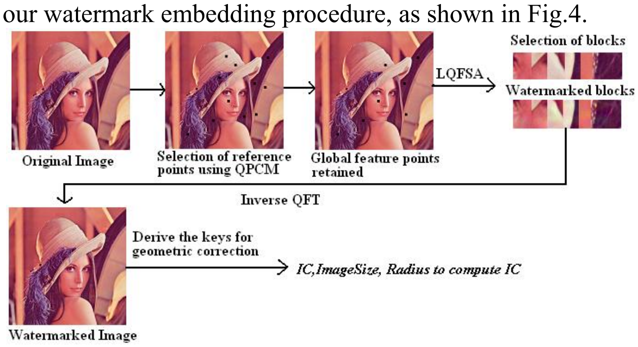


Fig.4. Watermark embedding Scheme

3. WATERMARK EXTRACTION

When geometric attacks happened to the watermarked images, the QPCM feature points would change their positions. To recover the reference points correctly under geometric attacks, another IFT method-invariant centroid (IC) [7] is adopted to obtain resistance to geometric distortions as well as low computational complexity.

The common geometric distortions include affine variations, under which the IC feature is changed with covariant properties. Thus we can perform geometric corrections on the attacked image according to the changes of IC feature as shown in Fig.5.

However, the IC feature is highly sensitive to the value of radius R [7] used to calculate the IC. We alleviate this problem by a rough estimation of suitable R choice in the attacked image. Let L' and L respectively denote the size of the attacked image and the non-attacked one, a modified value of R under geometric attacks is calculated as follows,

$$R' = R \times L'/L \tag{7}$$

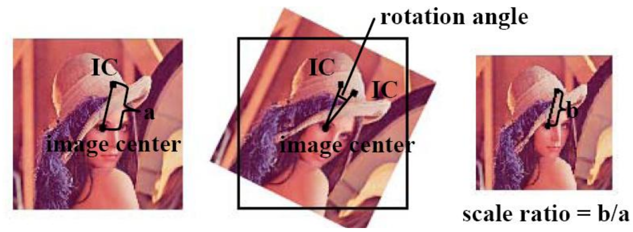


Fig.5. Geometric Correction

Moreover, the nearest-neighborhood search strategy is applied to the attacked image to further increase the probability of correct mark detection under inconsistent shift variations of reference points. We first recover the reference points using QPCM method in the attacked image and then watermark detection is performed both in the reference points and their neighbors. The embedded watermark bit is determined by the following formula:

$$w' = \text{mod2}\big(\text{Round}(C/\alpha)\big) \tag{8}$$

The bit w' is compared with the original watermark bit w. A copy of watermark is claimed correctly reconstructed if the number of matching bits exceeds a given threshold T for any two of the four blocks around a reference point. If three or more copies are correctly reconstructed, we claim the image watermarked. To reduce the computational complexity, geometric corrections are only considered when the above mentioned extraction scheme fails. If all the attempts fail, we conclude no existence of watermark in the image. The watermark extraction scheme is illustrated in Fig.6.

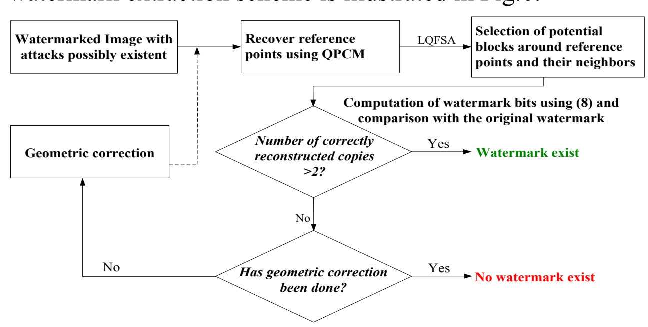


Fig.6. Watermark Detection Scheme

We can adjust the threshold T to assure the false positive rate less than a given value, e.g. 1×10^{-5}. Assuming the matching probability of each extracted bit to be $1/2$ and 3×3 neighborhood of each reference point are checked, the false positive rate around one reference point can be estimated as

$$P_{point} = \sum_{i+j \geq T}^{i=n, j=n} \left(\frac{1}{2}\right)^{2n} \times C_n^i \times C_n^j \times C_4^2 \tag{9}$$

$$P_{ref\ point} = \sum_{i=1}^{9} P_{point} \times (1 - P_{point})^{9-i} \times C_9^i \tag{10}$$

$$C_n^r = \frac{n!}{r!(n-r)!} \tag{11}$$

where n is the number of bits embedded in one block, i and j respectively denotes the matching bit number in two embedding blocks. For one-round extraction of watermark without geometric correction, the false positive rate is

$$P_{round} = \sum_{i=k}^{N} P_{ref\ point} \times \left(1 - P_{ref\ point}\right)^{N-i} \times C_N^i \quad (12)$$

where N is the number of the reference points, i starts from k means over k copies should be extracted to claim the watermark existence. For one-round watermark extraction with geometric correction, the false positive rate is

$$P_{image+G.C} = \sum_{i=1}^{M+1} P_{round} \times (1 - P_{round})^{M+1-i} \times C_{M+1}^i \quad (13)$$

where M denotes the number of potential geometric corrections throughout the whole image. This is a multivariate function. In this paper, we select $k = 3, n = 22, N = 8, M = 5$ as constant, and set $T = 35$ to make false positive rate equal to $7.8 \times 10^{-6} < 1 \times 10^{-5}$.

4. EXPERIMENTAL RESULTS

We test the robustness of our watermark scheme on the StirMark platform [8] and select five 512×512 standard test images to perform the experiments. The watermarked Lena and Peppers are shown in Fig.7.


Fig.7. Watermarked Images

We present in Table II the watermark extraction rate of our scheme under various attacks, where the formation N/A denotes N copies of watermark are correctly extracted when there are actually A copies in a marked image. A successful extraction is claimed when $N \geq 3$ as shown in section 3. Table III gives the comparison results with the work of Tang [4] and Jonathan [5], both of which have been proved to possess a relatively balanced robustness to a larger range of attacks as compared with other popular watermarking schemes.

Table II. Extraction rate under various attacks

ATTACKS	Lena α=3.91 R=128	Peppers α=3.91 R=128	Airplane α=3.91 R=128	Baboon α=4.88 R=64	Sailboat α=4.88 R=128
Watermarked image without attacks	7/7	8/8	6/7	8/8	7/8
Median filter 3x3	6/7	6/8	6/7	3/8	6/8
Sharpening 3x3	4/7	7/8	5/7	5/8	6/8
Gaussian filter 3x3	7/7	8/8	6/7	7/8	7/8
JPEG30	3/7	7/8	5/7	6/8	5/8
Cropping 5%	4/7	3/8	6/7	4/8	3/8
Cropping 10%	3/7	3/8	4/7	5/8	3/8
Removed 5 row and 17 columns	4/7	4/8	4/7	5/8	4/8
Linear Geometric Transform (1.007,0.01,0.01,1.012)	3/7	3/8	5/7	3/8	3/8
Shearing-x-1%-y-1%	3/7	3/8	7/7	3/8	3/8
Rotation 60°	4/7	5/8	6/7	3/8	4/8
Rotation 90°	7/7	7/8	6/7	7/8	7/8
Scaling 0.9	4/7	5/8	5/7	5/8	5/8
Scaling 0.6	6/7	4/8	4/7	3/8	6/8
Rotation 60+cropping 5%	6/7	6/8	7/7	6/8	5/8
Scaling 0.8+cropping 5%	4/7	3/8	3/8	3/8	3/8
Cropping 5% off+JPEG70	5/7	3/8	5/7	4/8	3/8
Shearing +JPEG70	4/7	3/8	5/7	4/8	4/8
Linear Geometric Transform +JPEG70	3/7	4/8	6/7	5/8	3/8
Rotation 5+JPEG70	4/7	4/8	6/7	3/8	3/8
Median filter 3x3+JPEG40	5/7	4/8	5/7	3/8	7/8
sharpening 3x3+JPEG40	3/7	5/8	4/7	3/8	4/8
Gaussian filter 3x3+JPEG40	5/7	6/8	4/7	4/8	5/8

Table III. Comparison of Watermark Reconstruction Rate (%)

Attacks	Ours	Tang's	Jonathan's
JPEG compression(quality factor Q = 90,80,70,60,50,40,30)	100%	78%	100% when Q=90,80
Filters(median, Gaussian, sharpening)	100%	50%	100%
Rotation attacks (rotation angle:1,2,4,5,10,15,20,30,60,90)	100%	generally failed	92.5%
Scale attack(scale rate 0.9,0.8,0.7,0.6)	100%	generally failed	75% under scaling 0.9
Rotation cropping attack	100%	about 33%	75%
Scale cropping attack	75%	about 33%	unavailable

From the experimental analysis, we can find that the proposed watermarking scheme is robust to a broad combination of non-geometric attacks, various rotation operations and the scaling down to a factor of 0.6.

5. ACKNOWLEDGEMENT

This work was supported in part by Shanghai Postdoctoral Foundation (06R214138), 863 (2006AA01Z124), NSFC (60502034, 60702044), the Cultivation Fund of the Key Scientific and Technical Innovation Project of MOE (706022), and the 111 Project.

6. REFERENCE

[1] P. Bas, N. L. Bihan and J. M. Chassery, "Color image watermarking using quaternion Fourier transform," IEEE ICASSP2003, vol.3, pp. 521-524, April 2003.

[2] T.K. Tsui, X.P. Zhang, and D. Androutsos, "Quaternion image watermarking using the spatio-chromatic Fourier coefficients analysis", ACM Multimedia, Oct. 2006

[3] M. Kutter, S. K. Bhattacharjee and T. Ebrahimi, "Toward second generation watermarking schemes," IEEE ICIP1999, vol. 1, pp. 320-323, 1999.

[4] C.W. Tang and H.M. Hang, "A feature-based robust digital image watermarking Scheme," IEEE Trans. signal processing, vol. 51, pp. 950-959, April 2003.

[5] J. Weinheimer, X. J. Qi and J. Qi, "Towards a robust feature-based watermarking scheme," IEEE ICIP2006, pp. 1401-1404, Oct. 2006.

[6] Y. Xu, X. K. Yang, et al., "QWT: Retrospective and new applications," The Fourth International Conference on Multivariate Approximation: Theory and Applications, invited paper, pp.70, Cancun, Mexico, April 2007.

[7] M. Awrangjeb, M. Murshed and G. Lu, "Global geometric distortion correction in images," IEEE MMSP2006, pp.435- 440, Oct. 2006.

[8] www.petitcolas.net/fabien/watermarking/stirmark/