Histogram Rotation-Based Image Watermarking with Reversibility

Youngseok Lee[1] and Jongweon Kim[2]

[1] *Dept.of Electronic Engineering, Chungwoon University,*
Daehak-Gil 25, Hongsung-Eup, Hongsung-Gun, Chungnam, 350-701, Korea
[2] *Dept.of Copyright Protection, Sangmyung University,*
7, Hongji-dong, Jongno-gu, Seoul 110-743, Korea
[1]*yslee@chungwoon.ac.kr,* [2]*jwkim@smu.ac.kr*

Abstract

This paper proposes a reversible blind image watermarking scheme for digital images based on discrete fractional random transform (DFRT). Based on a patchwork watermarking scheme, the proposed algorithm utilizes histogram rotation to embed a binary watermark in DFRT domain with strong information security. To evaluate the performance of the proposed scheme, several experiments are configured for block size, capacity (bits/pixel) as a function of embedding level. The results show the performances of proposed scheme are the same and/or the higher than the conventional histogram rotation scheme in [2]. But high security by DFRT is a unique in the proposed scheme while that is absent in the histogram rotation-based conventional scheme.

Keywords: *reversible watermarking, histogram rotation, discrete fractional random transform*

1. Introduction

Digital watermarking is a process in which digital contents such as image, video, audio, and even text are protected by embedding information such as a hidden copyright message into the content. Such a watermark should be imperceptible to others while being perceptible to the copyright holder who possesses the proper private information key [1].

In the case of image content, digital watermark signals are commonly embedded in the spectral or frequency domain for security and robustness. Most watermarking algorithm, called *lossy* watermarking, has resigned a loss of an original image quality in a watermarking process. But in some fields of the watermarking, a loss of an original image quality is not allowed to process the watermarking algorithm called *reversible* watermarking. In particular, it is the most important issue for security and a loss during transmission in the watermarking process of medical, remote sensing and legal enforcement images [2].

Recently, reversible watermarking algorithms without a loss of image quality have been reported in literatures [1, 2]. In [1], these algorithms are categorized into two types by the reversible data- hiding techniques. In the first type of algorithms, during encoding a spread spectrum signal corresponding to the watermark is superimposed on the host signal. During decoding the watermark is subtracted from the watermarked image in a restoration step. In the second type of algorithms, some features of the original image are replaced with the watermark. The original portions of the image that will be replaced by the watermark are compressed and passed. During the decoding process this compressed watermark-part is extracted and decompressed. Thus the original image is achieved by replacing the modified portions with the decompressed original features. The algorithms of first type offer visible artifacts and lower capacity. On the other hand, algorithms of second type offer better visible quality and higher capacity than the first type.

In this paper, we propose a DFRT-based reversible watermarking algorithm which is second type in the mentioned category. The basic principle of this scheme is based on the rotation of histogram that is a statistical property of a host image in DFRT domain with strong security. We have demonstrated that the proposed reversible watermarking scheme is highly secure on account of the inherent randomness of DFRT with reversible.

2. Security Analysis of Discrete Fractional Random Transform

It has been reported that a DFRT can essentially be derived from the discrete fractional random Fourier transform (DFRFT) [3]. The randomness is generated by using a random matrix. The overall process is quite similar to that by which the transform matrix of the DFRFT is obtained. The DFRT can be defined by a diagonal symmetric random matrix. The matrix Q is generated by an $N \times N$ real random matrix P that satisfies the following relation

$$Q = \left(P + P^T\right)/2 \tag{1}$$

where $Q_{lk} = Q_{kl}$. We define the kernel matrix of the DFRT R^α in such a way that Q commutes with R^α,

$$R^\alpha Q = QR^\alpha \tag{2}$$

In (2), these two matrices have the same eigenvectors. By the characteristic of a symmetric matrix, the eigenvectors of the matrix $\{V_{Rj}\}$ ($j = 1, 2, \cdots, N$) are real-orthonormal to each other. The eigenvector matrix $\{V_R\}$ is obtained by combining these column vectors:

$$V_R = [V_{R1}, V_{R2}, \cdots, V_{RN}] \tag{3}$$

Then, the kernel transform matrix of the DFRT can be expressed as

$$R^\alpha = V_R D_\alpha^R V_R^T \tag{4}$$

and the DFRT of a two-dimensional image X is expressed as

$$X_R = R^\alpha X (R^\alpha)^T \tag{5}$$

The DFRT is linear, unitary, index additive, and energy conserved. However, its kernel transform matrix is random, and this affords high security in information security applications such as digital watermarking.

3. Proposed Image Watermarking Scheme

The basic principle of our scheme is based on the randomness of DFRT in itself and histogram rotation of randomly selected two zones as patchwork scheme in [2]. The proposed method started from the assumption that the histogram property of the randomly selected two zones is most likely to that of the DFRTed version of the host image. This is the absolutely valid assumption because of the generation property of the real random matrix P in (1).

Similarly to the patchwork scheme, two pseudo-random zones of the host image are transformed in opposite directions. The pixel transformation is bijective to ensure reversibility. The proposed watermarking algorithm is blind in that it does not require a copy of the original image or any characteristic of the original image for extraction.

All embedding and extraction processes are simply carried out in the DFRT domain. For the same random number β, a change in the value of fractional order α produces an entirely different transformed image and can make the watermark undetectable. The fractional order α of the DFRT and the random seed β used to generate the random kernel matrix are used as secret keys. In our watermarking scheme, the embedding process was started from the DFRT of the host image and following as:

Step 1: The host image X is transformed by the DFRT, where the fractional order α of the DFRT and the random seed β used for the generation of the random kernel matrix are used as secret keys.

Step 2: Choose the two non-overlapping $M \times M$ random blocks, zones A and B from the DFRT pair of the host image. And according to the distribution of the weights, the centers of the mass of zones A and B, denoted as M_a and M_b, are computed.

Step 3: Let V_a and V_b represent the vectors pointing from the center of the circle to M_a and M_b, the watermarks embedding is thus achieved by slightly rotating them. To embed the message *bit 0* (*bit 1*), V_a and V_b are rotated counter-clockwise (clockwise) and clockwise (counter-clockwise) by the same angle as shown in Fig. 2 [4].

Step. 4: After embedding all the bits of the watermark, inverse DFRT is applied to the watermarked coefficients of the DFRTed image to obtain the final watermarked image.

In the extraction process, the sign of the difference between the rotated pair is used to extract the watermark bits and the magnitude of it indicates the rotated angles, that is, the changed amount of the grayscale values of the block as in [2]. After the watermark bits are extracted, the rotated centers of the mass, denoted as $M_{a'}$ and $M_{b'}$ in Fig. 2, can be rotated back to their original ones, M_a and M_b. That is, the host images can be recovered without any distortion and thus the reversibility is achieved.

Because of the randomness of DFRT, the proposed algorithm provides very strong security. Even though a very small error occurs in the fractional order α used in the DFRT, a meaningful image cannot be retrieved from the transformed image. Although the value of α is known, it remains difficult to retrieve the watermark. Because the kernel matrix of DFRT has $N(N + 1)/2$ independent elements, more than $2^{N(N + 1)/2}$ steps are required to try and find the right matrix.

4. Experimental Results

To test the performance of the proposed algorithm, we configured the test conditions; as host images, standard images such as *Lena*, *Mandrill*, *Gold hill* and *Harbor* (256 × 256 pixels, 8-bit grey level) in Fig. 3, were used to demonstrate the performance of the proposed algorithm. The values of the other parameters are as follows: the value of fractional order α is *4.42*.

Table 1. Capacities *($\times 10^{-2}$)*, as a Function of Embedding Depth for the Test Image, *Lena*

	Embedding depth			
Block size	1	2	4	8
16×16	0.1	0.2	0.2	0.2
8×8	0.8	1.1	1.2	1.3
4×4	2.6	4.1	4.9	5.2

The capacity (bits/pixel) is measures the number of bits transmitted by the watermark. Table 1 shows the capacities as a function of embedding depth for the test image, *Lena*. Increasing with block size, capacity tends to decrease and also it is not linearly increasing in proportion to the increase of embedding depth for the same block size. It is shown that they have not a significant correlation.

The invisibility, which is utilized to measure the transparence of the watermarked image, depends on the embedding depth. When the embedding depth was given a fixed value, 5, the invisibilities are approximately same, even though different block sizes are employed in our experiment. In summary, the proposed scheme achieves the high security and the high capacities while the acceptable visual quality of the watermarked image.

5. Conclusions

Based on the rotation of the image’s histogram in DFRT domain, a reversible blind watermarking scheme for digital images has been proposed. The fractional order α and random seed β, parameters of DFRT are used as the secret keys required to access the watermarked image in the proposed scheme.

To evaluate the performance of the proposed scheme, several experiments are configured for block size, capacity (bits/pixel) as a function of embedding level and invisibility. The results show the overall performance of the proposed scheme is the same or the higher than the conventional histogram rotation- based watermarking scheme in [2]. But high security in the proposed scheme is a unique property that is absent in the conventional scheme.

Acknowledgements

This research project was supported by Ministry of Culture, Sports and Tourism (MCST) and from Korea Copyright Commission in 2011.

References

[1] M. Awrangjeb, “An overview of reversible data hiding”, Proc. of ICCIT-2003, Bangladesh **(2003)**.

[2] A.Umaamaheshvari and K.Thanushkodi, IJCSNS 11, 4 **(2011)**.

[3] Z. Liu, H. Zhao and S. Liu, Optics Communications 255, 4 **(2005)**.

[4] J. Natarajan and V. R. Rathod, MIT International Journal of Electrical and Instrumentation Engineering 1, 1 **(2011)**.

Authors

Youngseok Lee is a currently Professor in Microprocessor and Signal processing with Electronic Department at the Chungwoon University, Korea. He received his PhD degree in Electronic Engineering at University of Seoul in 2000. His current research interests include Mathematical Analysis of Human Sensory System, Signal Processing, Pattern Recognition and Embedded System.

Jongweon Kim received the Ph.D. degree from University of Seoul, major in signal processing in 1995. He is currently a Professor of Dept. of Copyright Protection at Sangmyung University in Korea. He has a lot of practical experiences in the digital signal processing and copyright protection technology at the institute, the industry, and College. His research interests are in the areas of copyright protection technology, digital rights management, digital watermarking, and digital forensic marking.