Robust Digital Image Watermarking Algorithm against RST Attacks using Self-patch Correlation

Ruichen Jin
Dept. of Copyright Protection,
Sangmyung University
Seoul, Korea
Email: jinruichen@cclabs.kr

Jongweon Kim
Dept. of Contents and Copyright,
Sangmyung University
Seoul, Korea
Email: jwkim@smu.ac.kr

*Abstract***— In this paper, we propose an effective watermarking scheme using self-patch correlation based on Radon transform for image. The robustness against Rotation, Scaling, and Translation (RST) attacks is achieved using the translation property of the Radon transform and self-patch correlation. The Radon transform emphasizes and detects the linear characteristic to calculate the angle of image rotation. We insert random number blocks in the frequency domain to determine whether the image is scaled and predict the scale degree. The watermark is a hologram generated by quantization based on the cover image. We used hologram quantization to spread the watermark information and analyze the cover image in detail. The hologram is transformed by a discrete fractional random transform (DFRNT) with a random seed β. It makes the watermark security. We detect the watermark after restoring the image. The proposed method uses discrete wavelet transform (DWT) domain. DWT domain watermarking is robust against signal processing attacks. We have performed an intensive simulation to show the robustness in geometrical attacks.**

Keywords-image watermakring; radon transform; self-patch corrilation; digital wavelte transfotm; robust.

I. INTRODUCTION

As more and more people are interested in the intellectual property rights, extensive research has been done on copyright protection technology. With the improvement of science and copyright protection technology, many high-performance multimedia devices are produced, as well as high definition multimedia products. Thus, we have to develop and improve a corresponding technique for copyright protection.

Digital watermarking is an efficient solution for copyright protection, which inserts copyright information such as author name or ID into the contents [1]-[4]. The watermarking methods should be robust against various attacks. Geometric attack is known as one of the most difficult attacks to resist. It includes rotation, scaling and translation (RST). There are many research works dealing with geometric attacks, such as non-blind scheme [5], invariant domain embedding [6][7], template based synchronization [8][9] and feature-based synchronization [10]-[18].

We propose an algorithm to predict the geometrical attacks and automatically restore and then detect the watermark from the restored image.

First, we predict whether or not the image is rotated and calculate the degree of angle of rotation using image normalization [19]. Second, we predict whether or not the image is scaled and translated, and we calculate the degree of scaling and distance of translation. After this pre-processing, we extract the watermark.

II. RELATED WORKS

A. *Image normalization*

We use image normalization resistant against rotation attack. Figure 1. shows the process of image normalization. Through the image normalization, a rotated image can be corrected.

Step 1: Detect the edge of the original image using canny detect operator.

Step 2: Link the edge with thickening operation.

Step 3: Calculate the rotation angle and normalize image.

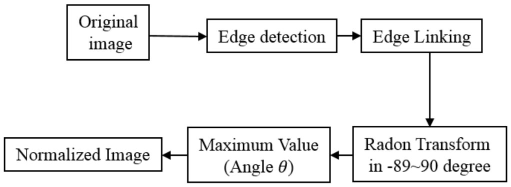

Original image
Edge detection
Edge Linking
Radon Transform in -89~90 degree
Maximum Value (Angle θ)
Normalized Image

Figure 1. The process of Image Normalization.

B. *Radon transform*

The Radon transform is the integral transform consisting of the integral of a function over straight lines. The transform was introduced in 1917 by Radon [20]. The Radon transform of image function f (x, y) is denoted by R (θ, r), which is defined as follows:

$$R(\theta, r) = \iint f(x,y)\delta(r - xcos\theta - ysin\theta)dxdy \quad (1)$$

where δ is the Dirac function. $\theta \in [0, \pi)$ denotes the angle between the beam and x-axis. $r \in (-\infty, \infty)$ is the perpendicular distance from the beam crossing the origin.

III. SELF-PATCH CORRILATION

For predicting whether or not the image is scaled and translated, and for calculating the degree of scaling and distance of translation, we used the self-patch correlation. It consists of the following steps:

Step 1: Transform the original image in frequency domain.

Step 2: Generate the n×n pseudo random number block. Arrange the random number blocks as same size of image transformed.

Step 3: Add the transformed image and random number blocks.

Step 4: After scaling and translating the image, transform the attacked image in frequency domain

Step 5: Split the block (n*n) as patch, and add with generate a blank block which size as same as attacked image.

Step 6: Based on the peaks position and inserted random number block size, we can calculate the scale proportion and the distance of translation.

Figure 2. shows the process of predicting the scale degree using self-patch correlation

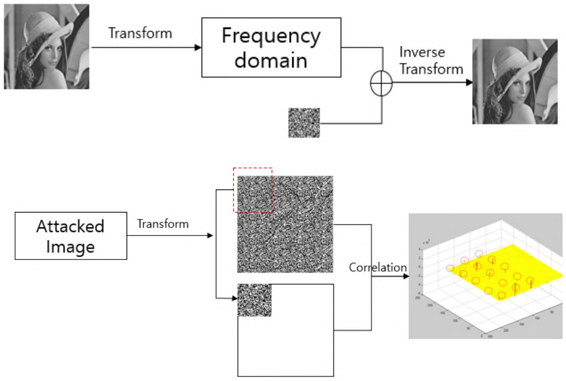


Figure 2. The process of predicting the scale degree using self-patch correlation.

IV. PROPOSED ALGORITHM

A. Embedding Scheme

Step 1: Insert the random number blocks into the transformed image on frequency domain.

Step 2: Encode the watermark message by quick response (QR) code encoder.

Step 3: Transform the QR code using a discrete fractional random transform (DFRNT) with seed β, and generate the hologram.

Step 4: Normalize the original image and get angle value by radon transform.

Step 5: Rotate the hologram by angle θ and get the new matrix.

Step 6: Transform them by two-depth, two- dimension Inverse DWT.

Step 6: Add the matrixes that gained in Step1 and Step 6.

B. Eslimate attatcks and restore

First, we predict whether or not the image is rotated and calculate the degree of angle of rotation using image normalization. Next, we predict whether or not the image is scaled and translated, calculate the degree of scaling and distance of translation.

Through the normalization algorithm and self-patch correlation, we can get the degree of rotation angle and the scale proportion. Based on these values, we restore the image and execute subsequent processing.

C. Extraction Scheme

The extraction process is the reverse of the embedding process, as follows:

Step 1: Transform the matrix using a two-depth, two-dimension discrete wavelet transform (DWT), and select the subbands.

Step 2: Add the subbands and transform them by DFRNT with seed β.

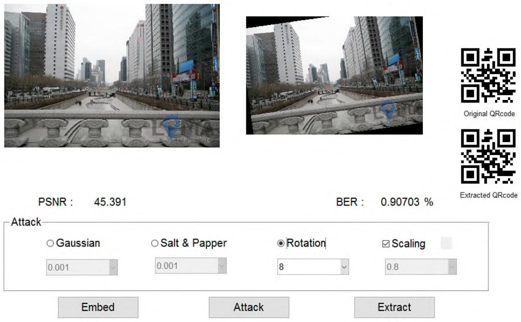
Step 3: Restore them with ReHologram and decode with QR decoder.

Step 4: If the QR decoder cannot decode the message, then distort the image. Loop from Step 1 to Step 4 until the decoder can read the QR code.

V. EXPERIMENTAL RESULTS

In this paper, we used a QR code for the watermark message. QR codes consisted of black modules arranged in a square pattern on a white background. The size of the QR code was 21×21 and its payload was from 72 to 152bits. It used Reed–Solomon error correction algorithm with four error correction levels. The higher the error correction level, the lower the storage capacity. According to the level, from 7% to 30% damaged QR Code can be restored.

Each 0.23% means that the QR code has the 1pixcel point error in 21×21. According to the QR code attribution that can be restored from 7 to 30%, the results with the values of BER are enough to restore the watermark information. In rotation attack 0~20 degree scale 0.8~1.4, we detect the watermark with 0.7~4.3% BER. We used the QR code as watermark which can restore the damaged QR code.



PSNR : 45.391

BER : 0.90703 %

Attack

○ Gaussian 0.001

○ Salt & Papper 0.001

● Rotation 8

☑ Scaling 0.8

Figure 3. The performace of the expriment.

VI. Conclusion and Future Work

In this paper, we propose a watermarking scheme using self-patch correlation based on Radon transform for image. The robustness against geometrical attacks is achieved using the translation property of the Radon transform and self-patch correlation. To evaluate the performance of the proposed method, watermark information was embedded in the wavelet-transformed domain. The experimental results showed that the proposed method gives robustness under RST attacks. In rotation attack 0~20 degree scale 0.8~1.4, we detect the watermark with 0.7~4.3% BER. We proposed an algorithm is robust to limited scale and angle degree. In many previous watermarking technology researches, they extract the watermark after rotation attack means that it is robust to the interpolation between rotate the image and re-rotate the image. In this paper, we predict the rotate the degree of rotating attack and restore. In the future work, we need more research to overcome the limitations.

Acknowledgment

This research is supported by Ministry of Culture, Sports and Tourism (MCST) and Korea Creative Content Agency (KOCCA) in the Culture Technology (CT) Research & Development Program 2016.

References

[1] J. Kim, N. Kim, D. Lee, S. Park, and S. Lee, “Watermarking two dimensional data object identifier for authenticated distribution of digital multimedia contents,” Signal Processing: Image Communication 25, pp. 559–576 (2010)

[2] Y. Lee and J. Kim, “Robust Blind Watermarking scheme for Digital Images Based on Discrete Fractional Random Transform,” Communications in Computer and Information Science 263, pp. 139-145 (2011)

[3] R. Jin and J. Kim, “Rotation-Invariant Image Watermarking Scheme Based on Radon Transform”, Advanced Science and Technology Letters, vol. 120(DCA2015), pp753-758, 2015

[4] J. Nah, J. Kim, and J. Kim, “Video Forensic Marking Algorithm Using Peak Position Modulation,” Applied Mathematics & Information Sciences (AMIS) 6(6S) , pp. 2391-2396, 2012

[5] J. Seo and C. Yoo, “Localized image watermarking based on feature points of scale-space representation,” Pattern Recognition ,Volume 37, Issue 7, July 2004, pp.1365–1375, 2004

[6] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, “Attacks on copyright marking systems,” in Proc. Int. Workshop on Information Hiding, pp. 218–238, Springer-Verlag, 1998.

[7] M. Kutter, “Watermarking resisting to translation, rotation and scaling,” Proc. SPIE 3528, pp. 423–431, 1998.

[8] S. Pereira and T. Pun, “Robust template matching for affine resistant image watermark,” IEEE Trans. Image Process. 9(6), pp. 1123–1129, 2000.

[9] C. Lin and I. Cox, “Rotation, scale and translation resilient watermarking for images,” IEEE Trans. Image Process. 10(5), pp. 767– 782, 2001.

[10] J. Ruanaidh and T. Pun, “Rotation, scale and translation invariant spread spectrum digital image watermarking,” Signal Process. 66(3), pp. 303–317, 1998.

[11] P. Bas, J. Chassery, and B. Macq, “Geometrically invariant watermarking using feature points,” IEEE Trans. Image Process. 11(9), pp. 1014–1028, 2002.

[12] M. Kutter, S. K. Bhattacharjee, and T. Ebrahimi, “Toward second generation watermarking schemes,” in IEEE Int. Conf. on Image Processing,Vol. 1, pp. 320–323 , 1999.

[13] A. Nikolaidis and I. Pitas, “Region-based image watermarking,” IEEE Trans. Image Process. 10(11), pp. 1726–1740, 2001.

[14] C. Tang and H. Hang, “A feature-based robust digital image watermarking scheme,” IEEE Trans. Signal Process. 51(4), pp. 950–959, 2003.

[15] D. Lowe, “Distinctive image features from scale-invariant keypoints,” Int. J. Comput. Vis. 60(2), pp. 91–110, 2004.

[16] K. Mikolajczyk and C. Schmid, “Scale and affine invariant interest point detectors,” Int. J. Comput. Vis. 60(1), pp. 63–86, 2004.

[17] T. Tuytelaars and L. V. Gool, “Matching widely separated views based on affine invariant regions,” Int. J. Comput. Vis. 59(1), pp. 61–85, 2004.

[18] S. Voloshynovskiy, A. Herrigel, N. Baumgartner, and T. Pun, “A stochastic approach to content adaptive digital image watermarking,” in Proc. Int. Workshop on Information Hiding, pp. 212–236, Springer-Verlag, 1999.

[19] J. Kim and J. Jin, “A Robust Watermarking Scheme for City Image,” International Journal of Security and Its Applications, Vol. 10, No. 1 (2016), pp.303-314, 2016

[20] A. Paplinski, “Rotation invariant categorization of visual objects using Radon transform and self-organizing modules,” in Lect. Notes in Comp. Sci. vol. 6444. Springer, pp. 360–366, 2010.