Proceedings of the World Congress on Engineering and Computer Science 2013 Vol I
WCECS 2013, 23-25 October, 2013, San Francisco, USA

A Robust and Invisible Digital Watermarking Algorithm based on Multiple Transform Method for Image Contents

M. Kim, D. Li*, and S. Hong

***Abstract*—Most of digital image watermarking techniques have focused on uncompressed images. However, compressed images more widely used than uncompressed images on the web due to its size. Joint Photographic Experts Group (JPEG) is well known and widely used digital format for compressing images. In this paper, we propose a new robust and invisible digital image watermarking algorithm for JPEG images based on the multiple transform method, discrete wavelet transform (DWT) and discrete fractional random transform (DFRNT). We generate a watermark through a two-dimensional (2D) barcode and scrambling method, and the generated watermark image is embedded into DWT-DFRNT transformed JPEG images using quantization technique in order to ensure the robustness and invisibility of the watermark. Experimental results present that our proposed method has improved the extraction performance of watermark from the compressed JPEG images and ensured the invisibility and robustness of the watermark against image signal processing such as image rotation and noise adding attacks.**

***Index Terms*—Watermarking, Discrete Wavelet Transform (DWT), Discrete Fractional Random Transform (DFRNT), 2D-barcode, Quantization, Joint Photographic Experts Group (JPEG)**

I. INTRODUCTION

DUE to advances in network and multimedia technologies, the Internet usage and number of digital media contents has continued to increase rapidly. Digital media contents can be used and distributed easily through the Internet. With the rise of digital contents, copyright infringement of digital content is also increasing constantly and it is now recognized as a serious problem. Digital watermarking [1], [2] may be used as an effective method for identifying the copyright ownership of digital content from unauthorized use and distribution. In digital watermarking, a watermark which contains the copyright information is embedded into the digital media content such as images, audio, and video, and may be extracted when the copyright ownership of the digital content needs to be verified [2], [3]. In the previous researches, many digital watermarking methods have been proposed for images, audio, and video. There are discrete cosine transform (DCT) [4], [5], DWT [6], [7], singular value decomposition (SVD) [8], and DFRNT [9] single domain based watermarking techniques. To complement the limitations of single transform based watermarking, dual transform domain based watermarking techniques such as DWT-DCT [10], [11] and DWT-SVD [12] have also been proposed.

In digital image watermarking, most of watermarking methods for images have been proposed based on uncompressed images. However, JPEG compressed images are more widely used on the web than uncompressed images like Bitmap (BMP) or Tagged Image File Format (TIFF). Therefore, some watermarking techniques have been proposed for JPEG images [13]-[15].

In this paper, we propose a robust and invisible digital image watermarking algorithm for JPEG images based on the multiple transform method which combines DWT and DFRNT domains using 2D barcode in order to improve the invisibility, extraction performance, and robustness of the watermark against image signal processing attacks such as noise addition and image rotation.

II. RELATED TECHNIQUES

A. Watermark Generation method

In the proposed watermarking algorithm, we use 2D barcodes which have various information capacities and the self-error correction function to create watermarks. 2D barcodes are a technique that contains information in the form of a rectangular or square box which is made up of black or white square dots or other shapes, like circles, hexagons. 2D barcodes can store information in both the horizontal and vertical directions, and thus they encode greater amount of data and take up smaller space than one-dimensional (1D) barcodes which encode information in the horizontal direction only according to the width of the bars and the spacing. 2D barcode can store usually up to thousands of characters by comparison to 20 to 25 characters in a 1D barcode. There are many types of 2D barcodes such as PDF417, DataMatrix, Maxicode, QR Code, Aztec Code, Data Code, Code 49, etc. These 2D barcodes have various information capacity and code size that are determined by the module size, error correction level, and type of encoding. Generally, the information capacity increases as the code size of the 2D barcode increases, but decreases as the error

Manuscript received July 23, 2013; revised August 14, 2013.

This research project was supported by the National Natural Science Foundation of China (Grant No. 61262090)

M. Kim is with the Department of Computer and Information Sciences, Towson University, Maryland, USA (e-mail: mkim2@students.towson.edu)

* Corresponding author: De Li is with the Department of Computer Science, University of Yanbian, Yanji, China (e-mail: leader1223@ybu.edu.cn)

S. Hong is with the Department of Computer and Information Sciences, Towson University, Maryland, USA (e-mail: shong@towson.edu)

correction level rises.

2D barcodes have the self-error correction function along with the characteristics such as the information capacity maximization, code region minimization, and rapid code reading, and therefore can be applied to the technologies for copyright protection of digital contents such as watermarking.

(a) QR Code (b) Aztec Code (c) DataMatrix

(d) PDF417

Fig. 1. Types of 2D-barcode.

After creating a 2D barcode, we use the scrambling conversion for converting the 2D barcode. The process increases the hidden computational complexity of information.

B. *Multiple Transform Method*

The transform method used in the proposed system consists of a combination of DWT and DFRNT [16] dual domain in order to ensure the invisibility and robustness of the watermark due to the frequency decomposition ability of DWT that extracts robust coefficients and the unpredictable random characteristic of DFRNT.

Before doing multiple transformations, first we convert a host image to a JPEG compression image. For the dual transformation, we use 2D-DWT [3], [17], and the JPEG image is used as input signal to the 2D-DWT. Through the process of frequency decomposition based on 2D-DWT, the input image signal is converted in such a way that the filters of DWT decompose the signal into three frequency sub-bands H (LH), V (HL), and D (HH), which have different frequency characteristics from one another. One level of 2D-DWT allows at least three watermarks to be embedded. This not only robustly embeds watermarks into a specific frequency band, but also allows the information about the copyright holders and users, to be additionally embedded into the content circulated by the copyright owner. This shows the pathways by which the contents are circulated and thereby enables effective multi-stage circulation tracking.

Next, the frequency coefficients generated by the 2D-DWT are used as input data to the DFRNT, and are mixed randomly by effecting various changes through the parameter manipulation. By the inherent randomness of DFRNT, the computational complexity of data can be increased, and thus the security of the algorithm can also be improved. The DFRNT is generally performed in the method that follows.

First, the DFRNT and its randomness are represented by a random matrix, with which the form is diagonal symmetric. Matrix H is generated using P generated as a random seed value, which is one of the parameters shown in Equation (1):

$$H = \frac{P+P^T}{2} \tag{1}$$

To generate an eigenvector from matrix H, SVD matrix decomposition is performed with respect to H, as shown in Equation (2):

$$[V_R, S, U] = SVD(H) \tag{2}$$

Here, the generated V_R is the matrix composed of *N* orthogonal eigenvectors, as in Equation (3):

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

Next, the N×N diagonal matrix D_α^R is generated using α and m, other parameters of DFRNT, as in Equation (4):

$$D_\alpha^R = \mathrm{diag}[1, \exp\left(-i\frac{2\pi\alpha}{m}\right), \cdots, \exp\left(-i\frac{2(N-1)\pi\alpha}{m}\right)] \tag{4}$$

Then, R^α is calculated by Equation (5) using V_R and D_α^R. The calculated R^α and the DFRNT input signal X are substituted in Equation (6) to obtain X_R, the final output of the DRFNT:

$$R^\alpha = V_R D_\alpha^R V_R^T \tag{5}$$

$$X_R = R^\alpha X (R^\alpha)^T \tag{6}$$

As above, DFRNT can transform the input signals generated by the 2D-DWT into random unpredictable signals by using three parameters, and the output signals can be restored again by doing the inverse transformation.

III. Proposed Watermarking Algorithm

A. *Watermarking Embedding Process*

The watermark embedding process is summarized as follows:

1) First, the original host image signal is compressed to a JPEG image.
2) Next, we generate the watermark image through the 2D barcode and scrambling.
3) The JPEG image is decomposed into three sub-bands, H, V, and D, through the two-level 2D-DWT. The 2D-DWT is performed by scanning the image signal in the 8 x 8 block unit, and some coefficients are chosen among the specified sub-band coefficients of each block according to the key table.
4) Next, the DFRNT is performed on the sub-band coefficients. And then, we embed the watermark image into the sub-band coefficient value using quantization technique.
5) Finally, we performed the inverse DFRNT (IDFRNT) and inverse DWT (IDWT).
6) As the final result, we obtain the watermarked JPEG image.

Fig. 2 shows the steps in the watermark embedding process.

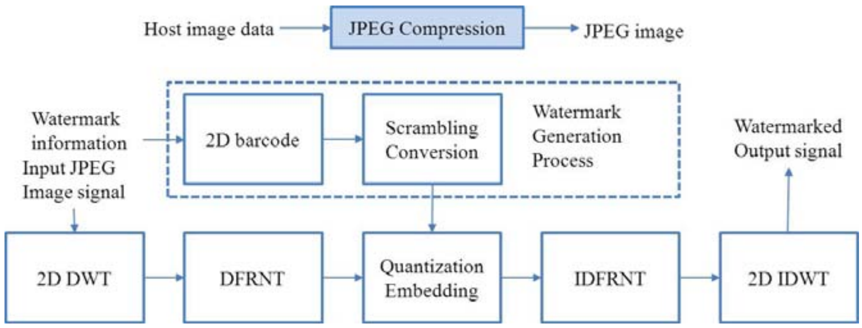


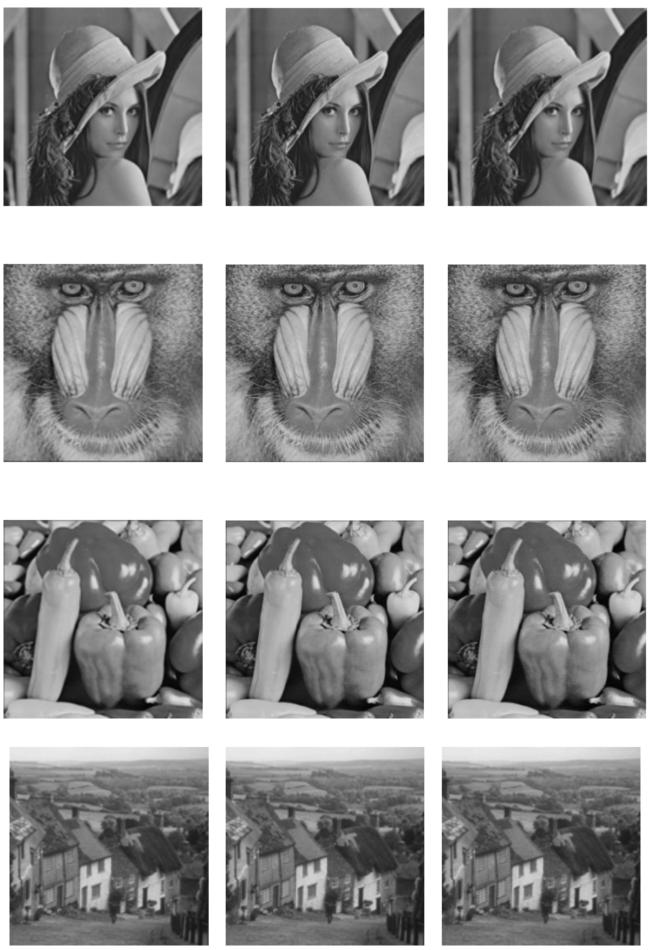
Fig. 2. Watermark embedding process.

B. *Watermark Extraction Process*

The watermark extraction process is performed in such a way that the embedding process is inversely applied to the watermarked JPEG image signal.

IV. Experimental Result

In order to evaluate the performance of our proposed algorithm, we have performed the experiments with respect to the invisibility, extraction performance, and robustness of the watermark in various conditions including noise adding and image rotation attacks.



(a) (b) (c)

Fig. 3. Image signals (a) Original host image (b) Compressed JPEG image (c) Watermarked JPEG image.

We used 512×512 size standard gray level images, including Lena, Baboon, Pepper, and Goldhill, as the sample host images and a 21×21 cell QR code. For the experiments, the host image is converted to JPEG format with Quality Factor (QF) 65, and 2D-DWT is applied to the JPEG image. While 2D-DWT is performed, the image signal is scanned in 8×8 block unit. In order to evaluate the imperceptibility and robustness, we compute the peak signal to noise ratio (PSNR) and Bit Error Rate (BER). BER value is calculated as follows:

$$BER = \frac{\sum_{i=1}^{P\times P} \omega_i \oplus \omega_i^*}{P \times P} \times 100\%$$

The comparison of the original image with the compressed JPEG image and watermarked JPEG image without being attacked is shown in Fig. 3. The value of the quantization coefficient Q value was set to 25 and the acquired PSNR are 40.22 dB, 40.73 dB, 39.64 dB, and 40.51 dB for Lena, Baboon, Pepper, and Goldhill JPEG images. This indicates that the proposed algorithm ensures good invisibility of watermark.

We evaluated the extraction performance of the proposed watermarking algorithm by computing BER and the experimental results are shown in Fig. 4. Fig. 4 shows (a) the extracted watermark image from the watermarked Lena JPEG image, (b) the restored 2D barcode. In the experimental result, the restored 2D barcode gave that BER=0.18%, 0.18%, 0.37%, and 0.37% for Lena, Baboon, Pepper, and Goldhill. This indicates that the 2D barcode was correctly restored.

(a) Extracted watermark (b) Restored QR code

Fig. 4. Image signals (a) Original host image (b) Compressed JPEG image (c) Watermarked JPEG image.

We performed the experiments by carrying out noise adding and rotation attacks, and the extracted and restored QR codes from the JPEG images after being attacked are shown in Table 1.

In the case of noise attack, Noise(g) denotes the Gaussian noise with mean set to 0 and variance set to 0.001, and

ISBN: 978-988-19252-3-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Noise(s) denotes the Salt & Pepper noise with density set to 0.01. In the case of rotation attack, the angle of rotation was set to 15°.

In addition, we evaluated the extraction performance of the proposed algorithm with reference to BER. In the performed experiment, we computed the BER values of the extracted watermark images fixing the PSNR at 40 dB after being attacked.

TABLE I
EXPERIMENTAL RESULTS BY VARIOUS ATTACKS

Images	Attacks		
	Noise(g)	Noise(s)	Rotation
Lena	BER=2.11%	BER=1.74%	BER=1.65%
Baboon	BER=1.74%	BER=1.29%	BER=2.48%
Pepper	BER=1.65%	BER=2.20%	BER=1.74%
Goldhill	BER=1.65%	BER=1.38%	BER=1.56%

As given in Table 1, the experimental results verify that the DWT-DFRNT dual domain ensures the extraction and robustness of the watermark, and the 2D barcodes could be restored.

V. CONCLUSIONS

In this paper, we have proposed a robust and invisible watermarking scheme for JPEG images, which are widely used on the web due to its size, based on DWT-DFRNT multiple transform method for protecting digital content from copyright infringement. We compressed the host images into JPEG images which are used as input signals to DWT-DFRNT multiple transform, and used a 2D barcode which contains watermark information and the scrambling conversion to generate watermarks. We performed various experiments to evaluate the performance of the proposed algorithm. The experimental results presented that the proposed algorithm has good invisibility and extraction performance, and ensure robustness of watermark against Gaussian noise, Salt & Pepper noise, and image rotation attacks.

REFERENCES

[1] I. J. Cox, M.L. Miller, J. M. G. Linnartz, and T. Kalker, "A Review of of Watermarking Principles and Practices", *Digital Signal Processing for Multimedia Systems*, Marcel Dekker, Inc., 1999, pp. 461-485.

[2] I. J. Cox and M. L. Miller, "The first 50 years of electronic watermarking", *Journal on Applied Signal Processing*, vol. 2002, no 2, pp. 126-132, 2002.

[3] V. M. Potdar, S. Han, and E. Chang, "A Survey of Digital Image Watermarking Techniques", in *Proceedings of the 3rd IEEE International Conference on Industrial Informatics*, Aug. 2005, pp. 709-716.

[4] S. P. Mohanty, K. R. Ramakrishnan, and M. S. Kankanhalli, "A DCT domain visible watermarking technique for images", in *IEEE International Conference on Multimedia and Expo 2*, 2000, pp. 1029-1032.

[5] H. Lu, X. Shi, Y.Q. Shi, A.C. Kot, and L. Chen, "Watermark embedding in DC components of DCT for binary images", in *Proceedings of IEEE Workshop on Multimedia Signal Processing*, 2002, pp.300-303.

[6] N. Kashyap and G. R. SINHA "Image Watermarking Using 3-Level Discrete Wavelet Transform (DWT)", *International Journal of Modern Education and Computer Science*, vol. 3, pp. 50-56, Apr. 2012.

[7] W. Lu, W. Sun, and H. Lu, "Novel robust image watermarking based on subsampling and DWT", *Multimedia Tools and Applications*, vol. 60, no. 1, pp. 31-46, 2012.

[8] C. Chang, P. Tsai, and C. Lin, "SVD-based digital image watermarking scheme", *Pattern Recognition Letters*, vol. 26, no. 10, pp. 1577-158615, Jul. 2005.

[9] H. Luo, F. Yu, Z. Huang, and Z. Lu, "Blind image watermarking based on discrete fractional random transform and subsampling", *Optik - International Journal for Light and Electron Optics*, vol. 122, no. 4, pp. 311-316, Feb. 2011.

[10] M. A. Mohamed, and A.M. El-Mohandes, "Hybrid DCT-DWT Watermarking and IDEA Encryption of Internet Contents", *IJCSI International Journal of Computer Science Issues*, vol. 9, no 2, Jan. 2012.

[11] M. Jiansheng, L. Sukang, and T. Xiaomei, "A Digital Watermarking Algorithm Based On DCT and DWT", in *Proceedings of the 2009 International Symposium on Web Information Systems and Applications*, China, May. 2009, pp. 104-107.

[12] Q. Li, C. Yuan, and Y.Z. Zong, "Adaptive DWT-SVD domain image watermarking using human visual model", in *Proceedings of 9th International Conference on Advanced Communication Technology*, vol. 3, 1997, pp. 1947-1951

[13] W. Luo and G. L. Heileman, "A Fast and Robust Watermarking Method for JPEG Images", *Computer Modeling & New Technologies*, vol. 8, no. 1, pp. 39-47, 2004.

[14] V. Saxena and J. P. Gupta, "A Novel Watermarking Scheme for JPEG Images", *WSEAS Transactions on Signal Processing archive*, vol. 5, no. 2, pp. 74-84, 2009.

[15] Q. Sun and S. Chang, "A Robust and Secure Media Signature Scheme for JPEG Images", *Journal of VLSI signal processing systems for signal, image and video technology*, vol. 41, no. 3, pp. 305-317, 2005.

[16] Z. Liu, H. Zhao, and S. Liu, "A discrete fractional random transform", *Optics Communications*, vol. 255, no. 4, pp. 357-365, Nov. 2005.

[17] M. J. Shensa, "The Discrete Wavelet Transform: Wedding the A Trous and Mallat Algorithms", *IEEE Transactions on Signal Processing*, vol. 40, no. 10, pp. 2464-2482, Oct. 1992.