A New Method of Wavelet Domain Watermark Embedding and Extraction Using Fractional Fourier Transform

Olcay Duman and Olcay Akay

Dokuz Eylül University, Dept. of Electrical and Electronics Eng., Kaynaklar Campus, 35130 Buca / İZMİR
olcay.duman@ozture.com, olcay.akay@deu.edu.tr

Abstract

In this paper, a new watermark embedding and detecting method for blind and robust digital watermarking of images are presented. A binary image is utilized as a watermark which is embedded using the Discrete Wavelet Transform (DWT) and the Fractional Fourier Transform (FrFT). We use DWT domain to embed the watermark into the original image in such a way that it is imperceptible by the human visual system. The FrFT orders are used as the encryption keys that allow the watermarking method to be more robust against various attacks. It is also shown that the watermark can be extracted from the watermarked image without needing the knowledge of the original image.

1. Introduction

Digital image watermarking is a technique of embedding hidden information in image data by making small modifications to the data. Image watermarking techniques can be broadly separated as spatial domain techniques and transform domain techniques. In spatial domain methods, watermark information is embedded into the pixels of an image [1], while in transform domain watermarking, first the original image is transformed into the underlying transform domain and then the transformed coefficients are modified. Discrete Cosine Transform, Fourier Transform (FT), Discrete Wavelet Transform (DWT) are examples of different transform domains [2-4]. Recently, the fractional Fourier transform (FrFT) has also been applied in watermarking as an alternative frequency domain technique [5,6]. In [5], white Gaussian noise is used as watermark. It is both embedded and detected in the FrFT domain. The transform orders of the FrFT and pixel positions where watermark is embedded are utilized together as encryption keys. In [6], a linear chirp signal, which produces a narrow peak in the FrFT domain if the correct transform order is used, is employed as the watermark and is embedded in the FrFT domain.

In this paper, we consider image watermarking by using a combination of DWT and FrFT. As the main advantage of applying watermarking in the FrFT domain, we can state that it is difficult to extract the watermark without knowing the correct transform orders. Furthermore, by changing the transform orders we can embed more watermarks. Employing DWT and FrFT together provides us with a more robust and visually imperceptible watermarking scheme which would not be possible to obtain by using the FrFT domain only.

2. Discrete Wavelet Transform (DWT)

DWT decomposes an image into its sub-bands. Each sub-band has such information as approximation (low-low sub-band), vertical (low-high sub-band), horizontal (high-low sub-band), and detail (high-high sub-band) components. Adding watermark to the high frequency sub-band provides better invisibility. However, low frequency sub-band is more robust to image processing attacks such as low-pass filtering and "jpeg" compression [7].

In this paper, we apply a 1-level DWT with the Haar mother wavelet. We embed the watermark in the high-low sub-band of the wavelet decomposition to provide the watermark with better invisibility.

3. Fractional Fourier Transform (FrFT)

The FrFT is a generalized form of the classical FT. It is a potentially applicable tool for processing especially non-stationary signals such as linear chirps. The FrFT domain can be considered as a type of combination of the time and frequency domains. In the time-frequency plane, the classical FT corresponds to a rotation angle $\pi/2$, which is a special case of all the FrFT domains [8,9]. The one-dimensional FrFT with a transformation angle, α, is defined [8,9] as

$$\mathrm{IF}^{\alpha}\{f(t)\}(u)=\int_{-\infty}^{\infty} f(t)K^{\alpha}(t,u)dt \tag{1}$$

with the transformation kernel given as

$$K^{\alpha}(t,u)=\sqrt{\frac{1-j\cot\alpha}{2\pi}}\,e^{j(t^2+u^2)\frac{\cot\alpha}{2}-jtu\csc\alpha}. \tag{2}$$

The inverse of the FrFT can be obtained by taking an FrFT with the negative transformation angle, -α. Thus, we can write

$$f(t)=\mathrm{IF}^{-\alpha}\left\{\mathrm{IF}^{\alpha}\left[f(t)\right]\right\}(t). \tag{3}$$

Two-dimensional FrFT is used for image analysis with a pair of transform orders[1] (a_1, a_2) which are applied to the rows and columns of an image, respectively [10]. It is a straightforward generalization of the one-dimensional FrFT in (1) for two-dimensional signals, namely images.

4. Watermark Embedding and Extraction

In this section, we outline our newly proposed watermark embedding and extraction method. Digital image watermarking consists of two parts as the embedding and extraction of the

[1] The FrFT order, a, and the corresponding transform angle, α, are related as $a=(2\alpha/\pi)$.

watermark. We embed the watermark into an image in the transform domain. This watermark can be detected or extracted later for various purposes.

The block diagram of our proposed watermark embedding method is shown in Fig. 1. For the embedding, the original image to be watermarked (such as a 512x512 image) is firstly decomposed into four wavelet sub-bands of different frequency bands. Subsequently, the high-low sub-band (a 256x256 image), where the watermark (a 32x32 image) is embedded, is divided into blocks of 8x8 (we also experimented with blocks of 16x16 and 32x32 with corresponding watermark images of 16x16 and 8x8, respectively). Then, an FrFT is applied to each block with transform orders (a_1, a_2) that are later used as encryption keys in the extraction process. The watermark image is a binary image of 0's and 1's (if it is not binary, it should be first converted into a binary image). To modify the FrFT coefficients of the high-low sub-band image, we initially generate two separate pseudorandom noise (PN) sequences of size 1x64, which are distributed according to standard normal (Gaussian) distribution. Then, we look at the first pixel at the upper left corner of the binary watermark image. If it is a 1, then we multiply the first PN sequence by a constant gain factor, c , and add the multiplied PN sequence to the FrFT coefficients in the first 8x8 block of the high-low sub-band image. If, otherwise, the considered pixel of the watermark is a 0, then the second PN sequence is multiplied by c and added. Repeating this procedure for all the binary-valued pixels of the 32x32 watermark image, all 1024 blocks in the high-low sub-band image are modified using either of the PN sequences and thus, the watermark information is encoded into the original image. To complete the embedding process, we need to go back to the spatial domain. For this purpose, we first take inverse FrFT (with order pair $(-a_1, -a_2)$) of all 1024 modified 8x8 blocks. Then, bringing together the modified high-low sub-band with the three unmodified sub-bands and applying an inverse DWT, we finally obtain the watermarked image.

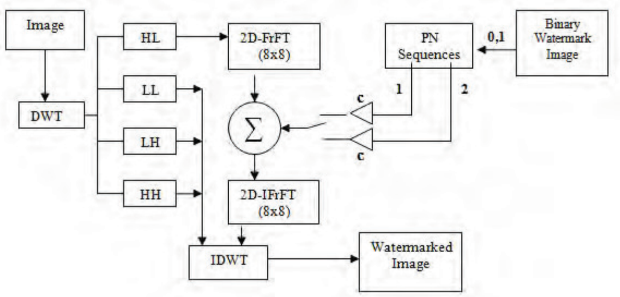


Figure 1: Block diagram of proposed watermark embedding method.

Watermark extraction process can be undertaken if the FrFT transform order pair and PN sequences are known. In fact, they are used for encryption keys to provide additional security. The block diagram of our proposed watermark extraction method is shown in Fig. 2. Applying DWT to the watermarked image, we obtain the high-low sub-band, which contains the watermark information, and the other unmodified sub-bands. Then, the high-low sub-band image is divided into 8x8 blocks. We apply a 2-dimensional FrFT to each block with the known transform order pair, (a_1, a_2) . Following that, data samples in each 8x8 block are correlated with the two 1x64 PN sequences separately. The output values of the two correlators are fed into a decision device that determines the larger one of these two values. If the correlation value with the first PN sequence is greater than the other, then the value of the corresponding pixel of the extracted watermark image is determined as 1. Otherwise, the value of 0 is assigned to the corresponding pixel of the watermark image. This process is repeated for all 1024 blocks in the high-low sub-band image and all pixel values of the 32x32 watermark image are determined either as 1 or 0.

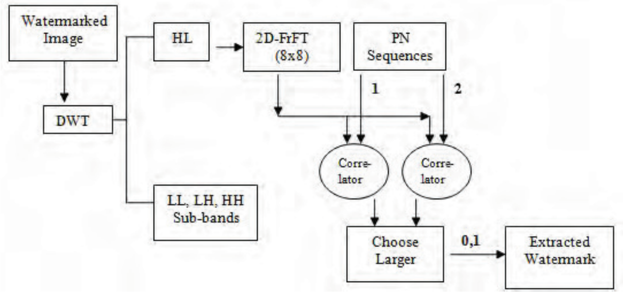


Figure 2: Block diagram of the proposed watermark extraction method.

We would like to note that it is important to use the exact negatives of the transform order pair (a_1, a_2) when performing the inverse FrFT during the embedding process. If we do not use the correct transform orders, we might end up with erroneous results. We demonstrate that using the Lena image in Fig. 3(a). Magnitude FrFT with (0.88, 1.06) of this image is shown in Fig. 3(b). If we take the inverse FrFT with the right orders of (-0.88, -1.06) we get back the original image. On the other hand, Figures 3(c) and (d) show the results of the inverse FrFT with order pairs of (-0.56, -1.55) and (-1.46, -0.45), respectively. Obviously, if we use wrong orders, we cannot recover the original signal.

5. Experimental Results

Several experiments are carried out to determine the performance of the proposed watermark embedding and extraction method. A standard Lena image (Fig. 4(a)) of dimension 512x512 is taken as the original image to be watermarked. The 32x32 binary image shown in Fig. 4(b) is used as the watermark. As explained in the previous section, we choose high-low sub-band image in DWT domain as the embedding sub-band, because this sub-band provides better imperceptibility. After dividing the high-low sub-band image into 8x8 blocks, we take the two-dimensional 8x8 FrFT of all the blocks using the FrFT order pair (1.21, 0.88). Based on the pixel values of the binary watermark image, we multiply and add the two PN sequences into the appropriate blocks of the DWT sub-band. The watermarked Lena image (obtained using the gain factor $c = 2$) is shown in Fig. 4(c).

Then, we used the watermarked image as the input of our proposed extraction method and performed the operations sketched in Fig. 2. After going through all the required steps as described in the previous section, we ended up with the extracted watermark image shown in Fig. 4(d).

To measure the image quality of a watermarked image (with 256 grayscale intensity values), the peak signal-to-noise ratio (PSNR) value (in *dB*) defined below can be used,

$$PSNR = 20\log_{10}\left(\frac{255}{\sqrt{MSE}}\right) \tag{4}$$

In (4), the mean squared error (MSE) between the *NxN* original, $p(x,y)$, and the watermarked, $p(x,y)'$, images is defined as

$$MSE = \frac{1}{N\times N}\sum_{x=1}^{N}\sum_{y=1}^{N}\left[p(x,y)-p(x,y)'\right]^2 . \tag{5}$$

On the other hand, to measure the similarity between the original and extracted watermarks, the normalized correlation (NC) value, ρ, defined below can be used,

$$\rho = \frac{\sum_{x=1}^{N}\sum_{y=1}^{N}(w(x,y)-\bar{w})(w_e(x,y)-\bar{w}_e)}{\sqrt{(\sum_{x=1}^{N}\sum_{y=1}^{N}(w(x,y)-\bar{w})^2)(\sum_{x=1}^{N}\sum_{y=1}^{N}(w_e(x,y)-\bar{w}_e)^2)}} . \tag{6}$$

In (6), $w(x,y)$ is the original watermark and $w_e(x,y)$ denotes the extracted watermark. $\bar{w}$ and $\bar{w}_e$ are the mean values of the watermark and the extracted watermark, respectively.

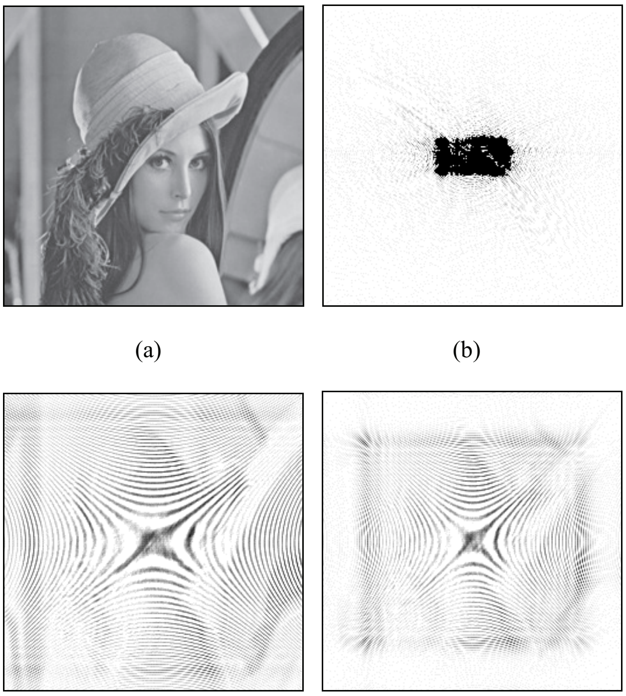


Figure 3: a) Lena image, b) magnitude FrFT of the Lena image with order pair (0.88, 1.06), c) inverse transformed image with order pair (-0.56, -1.55), d) inverse transformed image with order pair (-1.46, -0.45).

The watermarked image in Fig. 4(c) (obtained using the gain factor $c = 2$) has a PSNR value of 50.33 *dB* and the extracted watermark image in Fig. 4(d) has an NC value of 0.92 (note that in case of perfect recovery the NC value becomes 1).

For the embedding of the watermark, as an alternative to PN sequences, employment of deterministic linear chirp signals is also possible. The instantaneous frequency of a linear chirp signal changes linearly with time. A unit amplitude complex chirp signal with initial frequency, f_o, and sweep rate, m, parameters is defined [9] as

$$s(n) = e^{j2\pi(f_o n + \frac{1}{2}mn^2)} \tag{7}$$

with n denoting the sample number. If the sweep rate parameter, m, of a chirp signal matches the order of the FrFT, it produces a compact impulse in that matching FrFT domain. This is a result of the fact that chirp signals with different sweep rates form the underlying basis functions of the FrFTs with different orders [9]. Generation of an impulse in the FrFT domain can be exploited for efficient extraction of the watermark. Thus, replacing the PN sequences, we also experimented with two chirp signals with different sweep rate, m, parameters for embedding the watermark. The sweep rate parameters m_1 and m_2 can also serve as encryption keys for the extraction of the watermark. In the extraction phase, correlations are performed with the known chirp signals, instead of PN sequences.

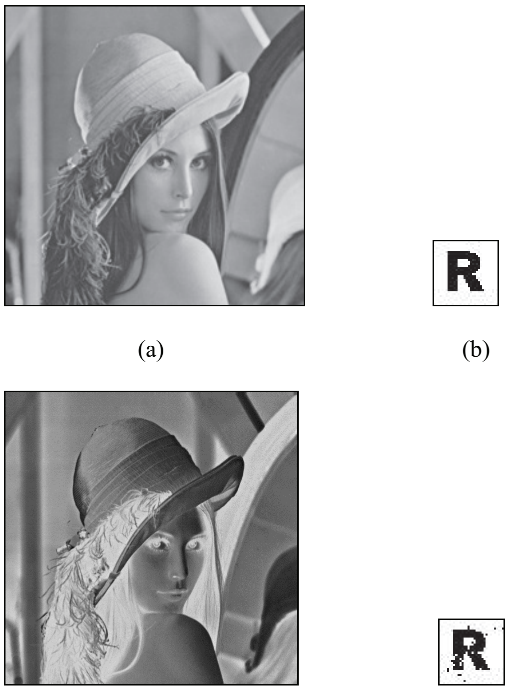
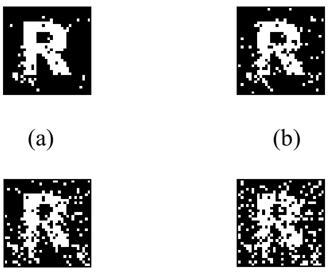


Figure 4: a) Lena image, b) binary watermark, c) watermarked Lena image, d) extracted watermark.

In simulations, we experimented with two unit amplitude chirp signals of length 64 with sweep rates of m_1=0.81 and

$m_2 = 0.67$, respectively. In Table 1, PSNR values showing quality of watermarked images obtained by using either PN sequences or chirp signals, with different block sizes (8x8, 16x16, or 32x32), and different constant gain factor, c , values are presented.

Our proposed watermark extraction method was also tested against some common attacks. In these experiments, the constant gain factor, c , is assigned the value of 10. Additive white Gaussian noise (WGN) has a variance of $\sigma^2 = 0.005$. "jpeg" compressions with different percentage quality factors, Q, are tried out. Cropping operation is applied as 32x32 central cropping. The other two simulated attacks are unsharp image and histogram equalization. NC is used to measure the similarity of the original and extracted watermark images. Again, different block sizes of 8x8, 16x16, and 32x32 (and the corresponding watermark image sizes of 32x32, 16x16, and 8x8) are experimented with. Note that these three different block sizes correspond to PN sequences (or chirp signals) of length 64, 256, and 1024, respectively. In Table 2, we present the NC values of attacked images watermarked using chirp signals with different block sizes. Similarly, In Table 3, NC values of attacked images watermarked using PN sequences with different block sizes can be seen. In addition, using the gain factor of $c = 15$ with chirp signals and blocks of 8x8, the extracted watermark images after "jpeg" compression attacks with percentage quality, Q, factors of 80%, 70%, 60%, and 50% can be seen in Fig. 5.



(a) (b) (c) (d)

Figure 5: Extracted watermark images after applying "jpeg" compression with different percentage quality factor, Q, values. a) 80%, b) 70%, c) 60%, d) 50%.

Table 1. PSNR values of watermarked images (using either PN sequences or chirp signals, different block sizes (8x8, 16x16, 32x32), and different gain factor values, c).

Gain factor c	Chirp Signal 8x8 PSNR (dB)	Chirp Signal 16x16 PSNR (dB)	Chirp Signal 32x32 PSNR (dB)	PN Seqn. 8x8 PSNR (dB)	PN Seqn. 16x16 PSNR (dB)	PN Seqn. 32x32 PSNR (dB)
1	58.24	59.08	59.19	55.39	56.06	56.34
2	40.78	53.35	53.46	50.33	50.74	50.38
3	53.15	49.97	50.29	47.93	46.35	47.32
5	44.90	45.53	46.06	44.48	42.96	43.08
8	40.78	41.47	41.89	36.44	39.16	39.03
10	38.85	39.60	39.98	38.76	36.89	37.22
12	37.35	38.00	38.43	35.37	36.00	35.76
15	35.36	36.11	36.48	32.84	32.75	33.84
20	32.89	33.61	33.97	30.17	31.56	31.22

Table 2. NC values of attacked images watermarked using chirp signals with different block sizes.

Attack on watermarked image	Chirp Signal 8x8 Normalized Correlation (NC)	Chirp Signal 16x16 Normalized Correlation (NC)	Chirp Signal 32x32 Normalized Correlation (NC)
Additive WGN $\sigma^2 = 0.005$	0.76	0.97	1
Cropping	0.98	1	1
"jpeg" (Q=80%)	0.88	0.95	1
"jpeg" (Q=70%)	0.77	0.92	1
"jpeg" (Q=30%)	0.32	0.23	0.87
Unsharp Image	1	1	1
Histogram Equalization	0.98	1	1

Table 3. NC values of attacked images watermarked using PN sequences with different block sizes.

Attack on watermarked Image	PN Sequence 8x8 Normalized Correlation (NC)	PN Sequence 16x16 Normalized Correlation (NC)	PN Sequence 32x32 Normalized Correlation (NC)
Additive WGN $\sigma^2 = 0.005$	0.98	1	1
Cropping	0.59	0.60	1
"jpeg" (Q=80%)	0.84	0.98	1
"jpeg" (Q=70%)	0.48	0.66	1
Jpeg (Q=30%)	0.01	0.10	0.39
Unsharp Image	1	1	1
Histogram Equalization	1	1	1

As can be seen from Tables 2 and 3, using chirp signals provides better robustness against most of the image processing attacks as compared to PN sequences. Only against additive WGN, PN sequences perform better than chirp signals. On the other hand, especially for the 30% "jpeg" compression, watermarking using PN sequences perform very poorly. Furthermore, it can be seen from Tables 2 and 3 that as the block size increases, NC performance of our proposed method improves at the expense of more computational cost.

6. Conclusions

A new transform domain watermark embedding and extraction method employing a combination of DWT and the FrFT is proposed. In this method, we do not need the original image to extract the watermark. Hence, it can be considered as a blind watermarking method. The FrFT order and PN sequences are used as encryption keys making watermarking scheme more robust against outside attacks. Experimental results show that this algorithm creates a watermark which is perceptually invisible and robust to various image processing attacks.

As for the computational complexity of the proposed method, using a PC having Intel Core 2 Duo 2.2 GHz processor and 4 GB memory and with Matlab (R2009b), it takes 3.46 and 1.99 seconds, respectively, to embed and extract a watermark image of 32x32 (using block size of 8x8) into a 512x512 original image.

7. References

[1] N. Nikolaidis and I. Pitas, "Robust image watermarking in the spatial domain", Signal Processing, vol. 66, pp. 385-403, May 1998.

[2] I. Cox, J. Killian, F. T. Leighton and T. Shamoon, "Secure spread spectrum watermarking for multimedia", IEEE Trans. on Image Proc., vol. 6, pp. 1673 – 1687, December 1997.

[3] V. Solachidis and I. Pitas, "Circularly symmetric watermark embedding in 2D-DFT domain", IEEE Trans. on Image Proc., vol. 10, pp. 1741 - 1753, November 2001.

[4] D. Kundur and D. Hatzinakos, "A robust digital image watermarking method using wavelet based fusion", Int. Conf. on Image Proc., vol. 3, pp. 544 - 547, October 1997.

[5] I. Djurovic, S. Stankovic and I. Pitas, "Digital watermarking in the fractional Fourier transformation domain", Journal of Network and Computer Applications, vol. 24, pp. 167-173, 2001.

[6] F. Q. Yu, Z. K. Zang and M. H. Xu, "A digital watermarking algorithm for image based on fractional Fourier transform", Proceedings of 1st IEEE Int. Conf. on Industrial Electronics and Appls., Singapore, pp. 1 - 5, May 2006.

[7] R. Dugad, K. Ratakonda and N. Ahuja, "A new wavelet-based scheme for watermarking images", IEEE Int. Conf. on Image Proc., Chicago, vol. 2, pp. 419-423, October 1998.

[8] L. B. Almedia, "The fractional Fourier transform and time-frequency representations", IEEE Trans. Sig. Proc., vol. 42, pp. 3084 - 3091, November 1994.

[9] H. M. Ozaktas, Z. Zalevsky and M. A. Kutay. *The Fractional Fourier Transform with Applications in Optics and Signal Processing*. John Wiley and Sons, 2001.

[10] A. Bultheel and H. Martinez-Sulbaran, "Computation of the fractional Fourier transform", Applied and Computational Harmonic Analysis, vol. 16, pp. 182-202, May 2004.